DEFENSE ACQUISITION GUIDEBOOK
FOREWORD

The Defense Acquisition System exists to manage the Nation's investments in technologies, programs, and product support necessary to achieve the National Security Strategy and support the United States Armed Forces. In that context, our continued objective is to rapidly acquire quality products that satisfy user needs with measurable improvements to mission capability at a fair and reasonable price. The fundamental principles and procedures that the Department follows in achieving those objectives are described in DoD Directive 5000.1 and DoD Instruction 5000.2. The Defense Acquisition Guidebook is designed to complement those policy documents by providing the acquisition workforce with discretionary best practice that should be tailored to the needs of each program.

Acquisition professionals should use this Guidebook as a reference source supporting their management responsibilities. As an “on-line” resource, the information is limited only by the user’s interest or need. Some chapters contain general content; they provide individual topic discussions and describe processes and considerations that will improve the effectiveness of program planning. Some chapters may provide a tutorial on the application of these topics to the acquisition framework. Depending on the subject matter, a chapter may contain general background information, tutorial discussions, and/or discussions of the detailed requirements for each milestone decision and phase. All chapters contain non-mandatory staff expectations for satisfying the mandatory requirements in DoD Instruction 5000.2.

Each chapter is designed to improve understanding of the acquisition process and ensure adequate knowledge of the statutory and regulatory requirements associated with the process. Discussions, explanations, and electronic links to related information enable the “reader” to be efficient, effective, innovative, and disciplined, and to responsively provide warfighting capability. Each chapter lists potential ways the program manager or assigned manager can satisfy mandatory process requirements and meet staff expectations for other activities. Differences of view regarding discretionary practice will be resolved by the Milestone Decision Authority.

The Guidebook should be viewed as an electronic resource rather than a “book.” The “reader” “navigates” the information instead of “leafing” through hundreds of physical, collated pages. Navigation is electronic movement through the reference system. There are three ways to view the information:

- Select the Document View tab to review Guidebook information page-by-page.
- Select the Lifecycle Framework tab to review statutory and regulatory requirements and related best practice for each Milestone and acquisition phase. And
- Select the Functional/Topic View tab to review comprehensive discussions of key acquisition topics.

(There is also an on-line tutorial available that goes into greater detail and describes the full capability provided by the Guidebook.)

At the chapter level, you may scroll up and down through the text, and jump between previous and next paragraphs. Throughout the text, hyperlinks let you electronically jump to related information. Many times, the links take you to another paragraph in the Guidebook. Some links take you to related text in either acquisition policy documents or the Joint Capabilities Integration and Development System documents. Other links will take you to external references, such as United States Code, the Federal Acquisition Regulation, or other formal DoD publications. Still others will take you to related, informal sources that are rich in information, such as the various Defense Acquisition University Communities of Practice.

To maximize the utility of this system, we recommend you use a computer that has Internet Explorer 6.x or higher, and is JavaScript enabled. The hardware requirement is whatever is necessary to support Internet Explorer 6.

Overview of the Defense Acquisition Guidebook

This Guidebook contains the following 11 chapters:

Chapter 1, Department of Defense Decision Support Systems, presents an overview of the Defense Department's decision support systems for strategic planning and resource allocation, the determination of capability needs, and the acquisition of systems.

Chapter 2, Defense Acquisition Program Goals and Strategy, discusses acquisition program goals and the topics the program manager should consider in developing a strategy for the acquisition program. It addresses the required information associated with the Acquisition Program Baseline and the program's Acquisition Strategy

Chapter 3, Affordability and Lifecycle Resource Estimates, addresses acquisition program affordability and resource estimation.

Chapter 4, Systems Engineering, covers the system design issues facing a program manager, and details the systems engineering processes that aid the program manager in designing an integrated system that results in a balanced capability solution.

Chapter 5, Lifecycle Logistics, provides the program manager with a description of Lifecycle Logistics and its application throughout the system life cycle, from concept to disposal.

Chapter 6, Human Systems Integration, addresses the human systems elements of the systems engineering process. It will help the program manager design and develop systems that effectively and affordably integrate with human capabilities and limitations; and it makes the program manager aware of the staff resources available to assist in this endeavor.

Chapter 7, Acquiring Information Technology and National Security Systems, explains how the Department of Defense complies with statutory and regulatory requirements for acquiring IT and NSS systems and is using a network-centric strategy to transform DoD warfighting, business, and intelligence capabilities. The chapter also provides descriptions and explanations of the Clinger-Cohen Act, the Business Management

Modernization Program and many other associated topics and concepts, and discusses many of the activities that enable the development of net-centric systems.

Chapter 8, Intelligence, Counterintelligence, and Security Support, describes program manager responsibilities regarding research and technology protection to prevent inadvertent technology transfer, and provides guidance for and describes the support available for protecting those technologies.

Chapter 9, Integrated Test and Evaluation, discusses many of the topics associated with test and evaluation, to include oversight, Developmental Test and Evaluation, Operational Test and Evaluation, and Live Fire Test and Evaluation. The chapter enables the program manager to develop a robust, integrated test and evaluation strategy to assess operational effectiveness and suitability, and to support program decisions.

Chapter 10, Decisions, Assessments, and Periodic Reporting, prepares the program manager and Milestone Decision Authority to execute their respective oversight responsibilities.

Chapter 11, Program Management Activities, explains the additional activities and decisions required of the program manager, not otherwise discussed in earlier chapters of this Guidebook.

CHAPTER 1

Department of Defense Decision Support Systems

1.0. Overview

1.0.1. Purpose

This chapter provides background information about the environment in which the Department of Defense must operate to acquire new or modified materiel or services.

1.0.2. Contents

Section 1.1 presents an overview of each of the three, principal, decision support systems used in the Department of Defense to acquire materiel and services, and describes the integration of those systems. Sections 1.2 through 1.4 provide details of each of these systems: Section 1.2 discusses the Planning, Programming, Budgeting, and Execution process, employed by the Department of Defense to conduct strategic planning and make resource allocation decisions; Section 1.3 discusses the Joint Capabilities Integration and Development System used to determine military capability needs; and Section 1.4 discusses the formal Defense Acquisition System used to acquire that capability.

1.1. Integration of the DoD Decision Support System

The Department of Defense has three principal decision-making support systems, all of which were significantly revised in 2003. These systems are the following:

Planning, Programming, Budgeting and Execution (PPBE) Process - The Department's strategic planning, program development, and resource determination process. The PPBE process is used to craft plans and programs that satisfy the demands of the National Security Strategy within resource constraints.

Joint Capabilities Integration and Development System - The systematic method established by the Joint Chiefs of Staff for assessing gaps in military joint warfighting capabilities and recommending solutions to resolve these gaps. To ensure effective integration of the capabilities identification and acquisition processes, the Joint Capabilities Integration and Development System guidance (CJCS Instruction 3170.01 and Manual 3170.01) was developed in close coordination with the revision to the acquisition regulations (DoD 5000 series).

Defense Acquisition System - The management process by which the Department acquires weapon systems and automated information systems. Although the system is based on centralized policies and principles, it allows for decentralized and streamlined execution of acquisition activities. This approach provides flexibility and encourages innovation, while maintaining strict emphasis on discipline and accountability.

Together, illustrated in Figure 1.1.1, the three systems provide an integrated approach to strategic planning, identification of needs for military capabilities,

systems acquisition, and program and budget development. The next three sections provide brief introduction to each of these decision support systems.

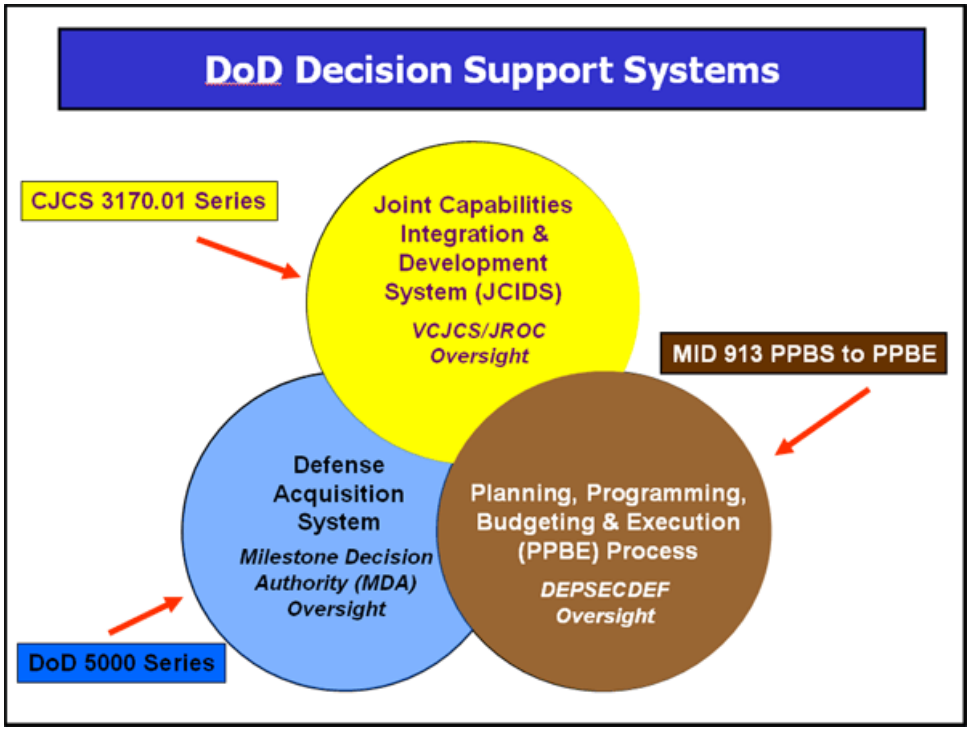

Figure 1.1.1 DoD Decision Support System

1.2. Planning, Programming, Budgeting and Execution (PPBE) Process

The purpose of the PPBE process is to allocate resources within the Department of Defense. It is important for program managers and their staffs to be aware of the nature and timing of each of the events in the PPBE process, since they may be called upon to provide critical information that could be important to program funding and success.

In the PPBE process, the Secretary of Defense establishes policies, strategy, and prioritized goals for the Department, which are subsequently used to guide resource allocation decisions that balance the guidance with fiscal constraints. The PPBE process consists of four distinct but overlapping phases:

Planning. The planning phase of PPBE, which is a collaborative effort by the Office of the Secretary of Defense and the Joint Staff, begins with a resource informed articulation of national defense policies and military strategy known as the Strategic Planning Guidance. The Strategic Planning Guidance is used to lead the planning process, now known as the Enhanced Planning Process. This

process results in fiscally constrained guidance and priorities - for military forces, modernization, readiness and sustainability, and supporting business processes and infrastructure activities - for program development in a document known as the Joint Programming Guidance. The Joint Programming Guidance is the link between planning and programming, and it provides guidance to the DoD Components (military departments and defense agencies) for the development of their program proposal, known as the Program Objective Memorandum (POM).

Programming. The programming phase begins with the development of a POM by each DoD Component. This development seeks to construct a balanced set of programs that respond to the guidance and priorities of the Joint Programming Guidance within fiscal constraints. When completed, the POM provides a fairly detailed and comprehensive description of the proposed programs, including a time-phased allocation of resources (forces, funding, and manpower) by program projected six years into the future. In addition, the DoD Component may describe important programs not fully funded (or not funded at all) in the POM, and assess the risks associated with the shortfalls. The senior leadership in OSD and the Joint Staff review each POM to help integrate the DoD Component POMs into an overall coherent defense program. In addition, the OSD staff and the Joint Staff can raise issues with selected portions of any POM, or any funding shortfalls in the POM, and propose alternatives with marginal adjustments to resources. Issues not resolved at lower levels are forwarded to the Secretary for decision, and the resulting decisions are documented in the Program Decision Memorandum.

Budgeting. The budgeting phase of PPBE occurs concurrently with the programming phase; each DoD Component submits its proposed budget estimate simultaneously with its POM. The budget converts the programmatic view into the format of the Congressional appropriation structure, along with associated budget justification documents. The budget projects resources only two years into the future, but with considerably more financial details than the POM. Upon submission, each budget estimate is reviewed by analysts from the office of the Under Secretary of Defense (Comptroller) and the Office of Management and Budget (OMB). The purpose of their review is to ensure that programs are funded in accordance with current financial policies, and are properly and reasonably priced. The review also ensures that the budget documentation is adequate to justify the programs presented to the Congress. Typically, the analysts provide the DoD Components with written questions in advance of formal hearings where the analysts review and discuss the budget details. After the hearings, each analyst prepares a decision document (known as a Program Budget Decision, or PBD) for the programs and/or appropriations under his or her area of responsibility. The PBD proposes financial adjustments to address any issues or problems identified during the associated budget hearing. The PBDs are staffed for comment and forwarded to the Deputy Secretary of Defense for decisions. These decisions are then reflected in an updated budget submission provided to the OMB. After that, the overall DoD budget is provided as part of the President's Budget request to the Congress.

Execution. The execution review occurs simultaneously with the program and budget reviews. The purpose of the execution review is to provide feedback to the senior leadership concerning the effectiveness of current and prior resource allocations. Over time, metrics are being developed to support the execution review that will measure actual output versus planned performance for defense programs. To the extent performance goals of an existing program are not being met, the execution review may lead to recommendations to adjust resources and/or restructure programs to achieve desired performance goals.

PPBE Biennial Cycles. In 2003, the Department adjusted its planning, programming and budgeting procedures to support a two-year cycle that results in two-year budgets. The revised process is described in Management Initiative Decision (MID) 913, dated May 22, 2003. The concept in MID 913 is consistent with submission of a biennial DoD budget that is part of the President's Budget request to Congress for even-numbered fiscal years (FY) (e.g., the FY 2004 President's Budget, submitted to Congress in March 2003, contained justification material for both FY 2004 and FY 2005). In this cycle, the even-numbered years are called on-years, while the odd-numbered years are called off-years. Figure 1. 2.1 displays a nominal timeline for the PPBE phases in an on-year.

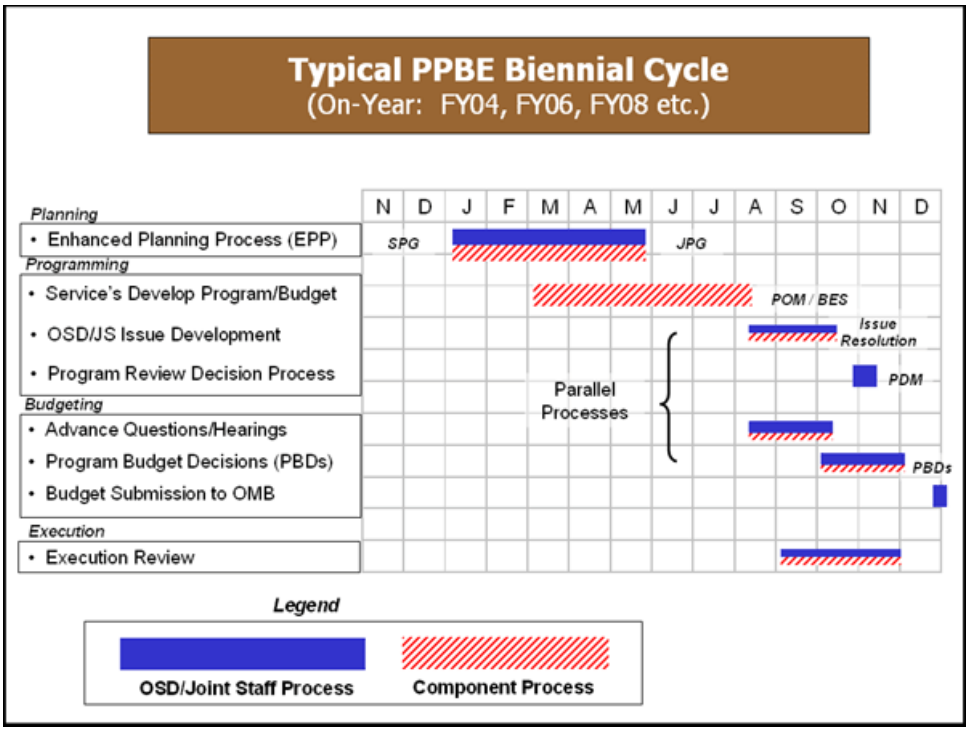

Figure 1.2.1. Typical PPBE Biennial Cycle, "On-Year"

In practice, Congress does not actually provide the Department with biennial appropriations. An amended budget justification must be submitted for the second year of the original biennial request so that Congress will appropriate funds for that second year. The Department uses a restricted process in the off-year to develop an amended budget that allows for only modest program or budget adjustments. Figure 1.2.2. displays a nominal timeline for the limited off-year process.

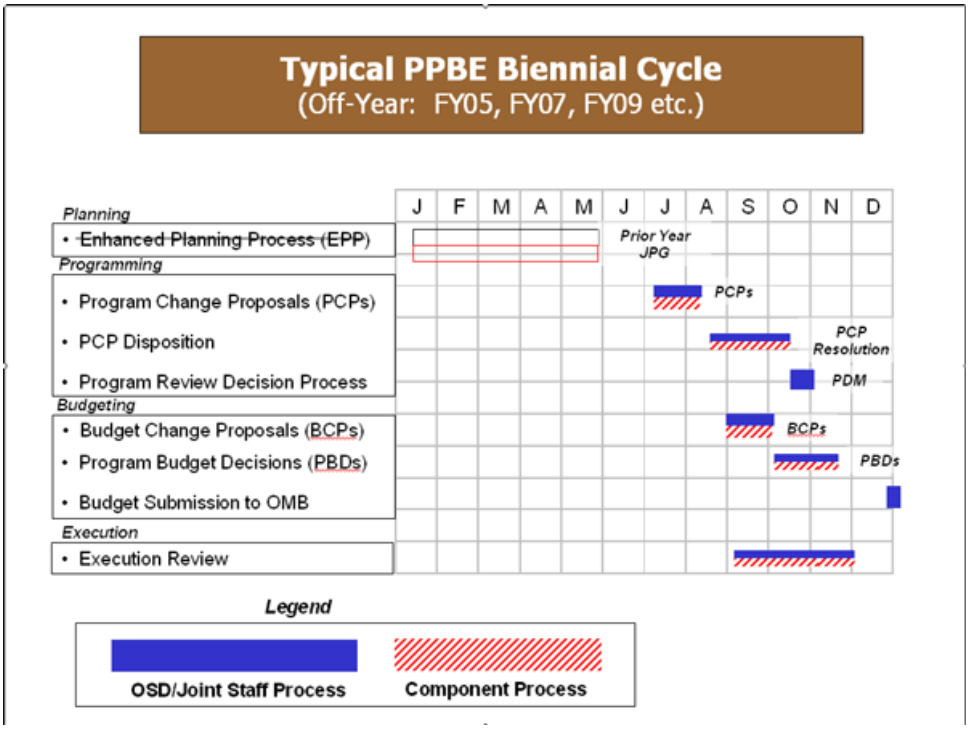

Figure 1.2.2. Typical PPBE Biennial Cycle, "Off-Year"

In the off-year, there are no significant changes to policy, strategy, or fiscal guidance. In fact, there may be no issuance of revised Joint Programming Guidance. If revised Joint Programming Guidance is provided, it would only contain minor revisions (although it could direct studies to support major decisions on strategy or program choices for the following Strategic Planning Guidance or Joint Programming Guidance). In addition, in the off-year, the DoD Components do not provide revised POMs or budget estimates. Instead, the DoD Components are allowed to submit Program Change Proposals (PCPs) and/or Budget Change Proposals (BCPs) to account for fact-of-life changes (e.g., program cost increases or schedule delays). BCPs and PCPs are limited to a single issue and must identify resource reductions to offset any program or budget cost growth. PCPs address issues over a multi-year period, whereas BCPs address issues focused on the upcoming budget year. PCPs are reviewed

in a manner similar to on-year program issues, and BCPs are resolved through the issuance and staffing of PBDs.

From a larger perspective, the biennial PPBE cycle is designed to support and implement policy and strategy initiatives for each new four-year Presidential administration. Figure 1.2.3. depicts alignment of the biennial PPBE cycle over a four-year term.

PPBE Two-Year Cycles Corresponding to Four-Year Presidential Terms

Year 1 (Review and Refinement):
- New National Security Strategy
- Off-year JPG as required (at discretion of SECDEF)
- Limited Changes to Baseline Program

Year 2 (Formalize the Agenda):
- Quadrennial Defense Review (QDR)
  - Aligned with PB submission in second year of an administration
- On-year SPG/JPG (implementing QDR)
- Fiscal Guidance Issued
- POM/BES Submissions

Year 3 (Execution of Guidance):
- Off-year JPG as required (at discretion of SECDEF)
- Limited Changes to Baseline Program

Year 4 (Ensuring the Legacy):
- On-year SPG/JPG (refining alignment of strategy and programs)
- Fiscal Guidance Issued
- POM/BES Submissions

Figure 1.2.3. . PPBE Two-Year Cycles Corresponding to Four-Year Presidential Terms

In the first year of the administration, the President approves a new National Security Strategy, which establishes (1) the worldwide interests, goals, and objectives that are vital to the national security, and (2) the foreign policy, worldwide commitments, and national defense capabilities necessary to implement the national security goals and objectives. Once the new administration's National Security Strategy is established, the Secretary of Defense, in consultation with the Chairman of the Joint Chiefs of Staff, leads the Quadrennial Defense Review (QDR). The QDR is a comprehensive review of all elements of defense policy and strategy needed to support the national security strategy. The defense strategy is then used to establish the plans for military force structure, force modernization, business processes and supporting infrastructure, and required resources (funding and manpower). The QDR final report is provided to Congress in the second year of the administration. In the PPBE process, the QDR final report serves as the foundation document for defense strategy and business policy. Since this document is not

available until the second year, the first year of the administration is treated as an off-year, using the President's Budget inherited from the previous administration as a baseline. In the second year, which is treated as an on-year, the Strategic Planning Guidance and Joint Programming Guidance are rewritten to implement the QDR of the new administration.

1.3. Joint Capabilities Integration and Development System

The Joint Capabilities Integration and Development System (JCIDS) is a joint-concepts-centric capabilities identification process that allows joint forces to meet future military challenges. The Joint Capabilities Integration and Development System process assesses existing and proposed capabilities in light of their contribution to future joint concepts. Joint Capabilities Integration and Development System, supported by robust analytic processes, identifies capability gaps and potential solutions. While Joint Capabilities Integration and Development System considers the full range of doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) solutions, for purposes of this Guidebook, the focus remains on the pursuit of "materiel" solutions.

Joint Capabilities Integration and Development System acknowledges the need to project and sustain joint forces and to conduct flexible, distributed, and highly-networked operations. Joint Capabilities Integration and Development System is consistent with the DoD Directive 5000.1 charge for early and continuous collaboration throughout the Department of Defense. Joint Capabilities Integration and Development System implements a capabilities-based approach that leverages the expertise of government agencies, industry, and academia. Joint Capabilities Integration and Development System encourages collaboration between operators and materiel providers early in the process, and enhances the ability of organizations to influence proposed solutions to capability shortfalls. Joint Capabilities Integration and Development System defines interoperable, joint capabilities that will best meet the future needs. The broader DoD acquisition community must then deliver these technologically sound, sustainable, and affordable increments of militarily useful capability to the warfighters.

The revolutionary transformation to Joint Capabilities Integration and Development System, coupled with the evolutionary emergence of a more flexible, responsive, and innovative acquisition process should produce better integrated and more supportable military solutions; a better prioritized and logically-sequenced delivery of capability to the warfighters, despite multiple sponsors and materiel developers; and an improved Science and Technology-community focus on future warfighting capability needs.

Joint Capabilities Integration and Development System informs the acquisition process by identifying, assessing, and prioritizing joint military capability needs; these identified capability needs then serve as the basis for the development and production of acquisition programs. Joint Capabilities Integration and Development System is fully described in an instruction (CJCS Instruction 3170.01) signed by the Chairman of the Joint Chiefs of Staff. This instruction establishes the policies for Joint Capabilities Integration and Development System, and provides a top-level description of the process. A supplementary manual (CJCS Manual 3170.01) provides the details necessary for the day-to-day work in identifying, describing, and justifying joint warfighting capabilities.

The manual also includes the formats that describe the content required for each Joint Capabilities Integration and Development System document.

For major defense acquisition programs or major automated information systems subject to OSD oversight, the products of the Joint Capabilities Integration and Development System process directly support the Defense Acquisition Board and Information Technology Acquisition Board in advising the Milestone Decision Authority for major milestone decisions. Figure 5 is a simplified portrayal of the nature of this support. Joint Capabilities Integration and Development System provides similar support to other acquisition programs, regardless of the milestone decision authority. Where appropriate, the Joint Capabilities Integration and Development System process and its products may be tailored when applied to automated information systems

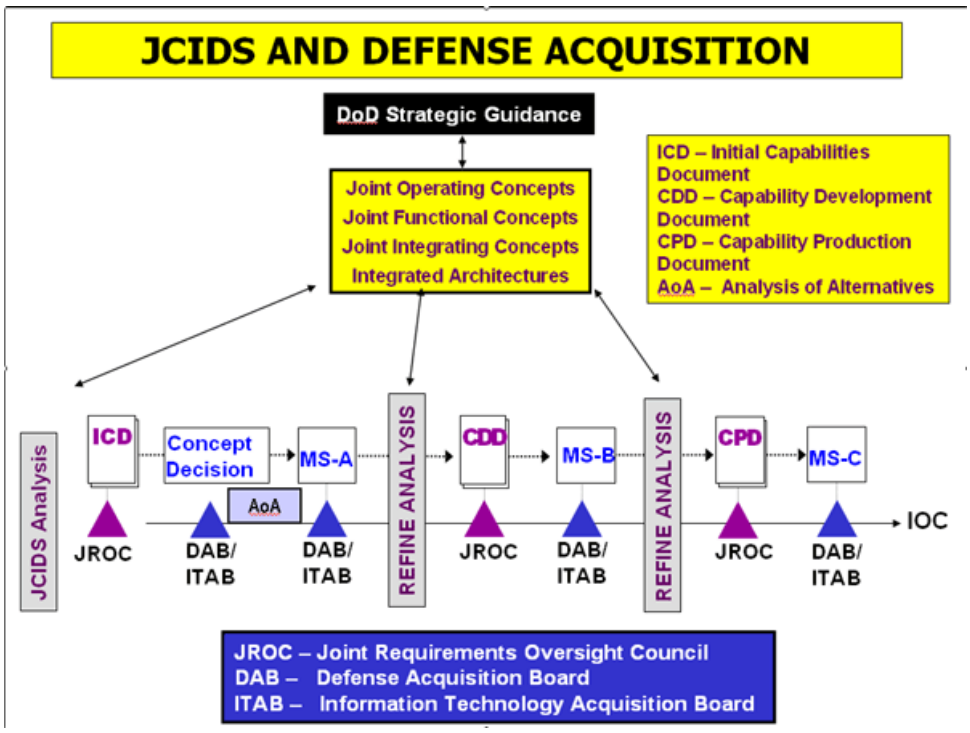

Figure 1.3.1. Joint Capabilities Integration and Development System and Defense Acquisition

There are several key points portrayed in Figure 1.3.1.. First, Joint Capabilities Integration and Development System is based on a series of top-down analyses ultimately derived from formal strategic-level guidance, including the National Security Strategy, National Military Strategy, Joint Vision 2020, and the report of the Quadrennial Defense Review. Second, these analyses assess existing and proposed capabilities in terms of their contribution to emerging joint warfighting concepts. Moreover, rather than focusing on the capabilities of individual weapon systems in isolation, the analyses assess capabilities

in the context of integrated architectures of multiple interoperable systems. Third, from these overarching concepts, the Joint Capabilities Integration and Development System analysis process identifies capability gaps or shortcomings, and assesses the risks associated with these gaps. These gaps may be addressed by a combination of materiel and/or non-materiel solutions (non-materiel solutions would be changes to doctrine, organization, training, leadership and education, personnel, and facilities). Fourth, recommended materiel solutions, once approved, lead to acquisition programs. For such programs, at each acquisition milestone, Joint Capabilities Integration and Development System documents are provided that will guide the subsequent development, production and testing of the program. Further information on the Joint Capabilities Integration and Development System analysis process, as well as the nature and role of each of the Joint Capabilities Integration and Development System documents, can be found in CJCS Instruction 3170.01, Enclosure A.

For Acquisition Category I and IA programs, and other programs designated as high-interest, the Joint Requirements Oversight Council (JROC) reviews and validates all Joint Capabilities Integration and Development System documents under its purview. For Acquisition Category ID and IAM programs, the JROC makes recommendations to the Defense Acquisition Board or Information Technology Acquisition Board, based on such reviews. JROC responsibilities are established by law (10 U.S.C. 181). The JROC is chaired by the Vice Chairman of the Joint Chiefs of Staff, who importantly also serves as the co-chair of the Defense Acquisition Board. The other JROC members are the Vice Chiefs of each military service.

1.4. Defense Acquisition System

The Defense Acquisition System is the management process that guides all DoD acquisition programs. DoD Directive 5000.1, *The Defense Acquisition System*, provides the policies and principles that govern the defense acquisition system. DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, in turn establishes the management framework that implements these policies and principles. The Defense Acquisition Management Framework provides an event-based process where acquisition programs proceed through a series of milestones associated with significant program phases. Details on the milestones and program phases are found in section 3 of the instruction. The instruction also identifies the specific statutory and regulatory reports and other information requirements for each milestone and decision point.

One key principle of the defense acquisition system is the use of acquisition program categories, where programs of increasing dollar value and management interest are subject to more stringent oversight. Specific dollar and other thresholds for these acquisition categories are contained in DoD Instruction 5000.2, Enclosure 2. The most expensive programs are known as Major Defense Acquisition Programs (MDAPs) or as Major Automated Information Systems (MAISs). These major programs have the most extensive statutory and regulatory reporting requirements. In addition, some elements of the defense acquisition system are applicable only to weapon systems, some are applicable only to automated information systems, and some are applicable to both. Specific details are found in DoD Instruction 5000.2, Enclosure 3.

An MDAP or a MAIS is subject to review by specific senior officials in the Office of the Secretary of Defense, unless delegated to a lower level of review (usually the DoD Component Head or Acquisition Executive). For the programs reviewed at the OSD level, MDAPs are denoted as Acquisition Category ID and are subject to review by the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); MAISs are denoted as Acquisition Category IAM and are subject to review by the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO). These individuals are each the Milestone Decision Authority for their respective programs. Both individuals are supported by a senior advisory group, either the Defense Acquisition Board for MDAPs, or the Information Technology Acquisition Board for MAISs. Senior officials from the Joint Staff, the Military Departments, and staff offices within OSD comprise these boards.

Both Boards are further supported by a subordinate group in OSD known as an Overarching Integrated Product Team (OIPT). Each OIPT facilitates communication and vets issues before the Defense Acquisition Board or Information Technology Acquisition Board meets. In this facilitator's role, the OIPT charters Working-level Integrated Product Teams for each review and manages their activities. At the Milestone Decision Point, the OIPT leader provides the Defense Acquisition Board or Information Technology Acquisition Board members with an integrated assessment of program issues gathered through the Integrated Product Team process as well as various independent assessments.

CHAPTER 2

Defense Acquisition Program Goals and Strategy

2.0. Overview

2.0.1. Purpose

The purpose of this chapter is to assist Program Managers in formulating the goals and developing the strategies required to manage their programs. Program goals serve as control objectives. The Acquisition Strategy describes the program managers plan to achieve these goals and summarizes the program planning and resulting program structure.

This chapter addresses the information required to comply with DoD Instruction 5000.2 Utilizing the capabilities of this "on-line" Guidebook, many topics are electronically linked to the related detailed discussions and explanations appearing elsewhere in this Guidebook or on the Internet.

2.0.2. Contents

Section 2.1 discusses program goals. An acquisition program and associated program goals result from the Joint Capabilities Integration and Development System determination to pursue a materiel solution to satisfy an identified capability need. Section 2.2 discusses the Technology Development Strategy, and Section 2.3 discusses the Acquisition Strategy leading to the achievement of the program goals.

2.1. Program Goals

Program goals are the minimum number of cost, schedule, and performance parameters necessary to describe program objectives. The discussion of program goals in this Guidebook is "*hot-linked*" to the discussion of Joint Capabilities Integration and Development System documentation in CJCS Instruction 3170.01, *Joint Capabilities Integration and Development System*, and CJCS Manual 3170.01, *Operation of the Joint Capabilities Integration and Development System.*

2.1.1. The Acquisition Program Baseline (APB)

To comply with 10 USC 2435 and 10 USC 2220, DoD Instruction 5000.2 requires every program manager to document program goals prior to program initiation. The Acquisition Program Baseline satisfies this requirement.

Program goals consist of an objective value and a threshold value for each parameter.

Objective values represent what the user desires and expects. The program manager manages the program to the objective value of each parameter.

Thresholds represent the acceptable limits to the parameter values that, in the user's judgment, still provide the needed capability. For performance, a threshold represents either a minimum or maximum acceptable value, while for schedule and cost parameters, thresholds would normally represent maximum allowable values. The failure to attain

program thresholds may degrade system performance, delay the program (possibly impacting related programs or systems), or make the program too costly. The failure to attain program thresholds, therefore, places the overall affordability of the program and/or the capability provided by the system into question.

For each parameter, if no objective is specified, the threshold value should also serve as the objective value. As a general rule, if no threshold is specified, the performance objective value should also serve as the performance threshold value; the schedule objective value plus 6 months for Acquisition Category (ACAT) I or 3 months for ACAT IA should serve as the schedule threshold value; or the cost objective value plus 10 percent should serve as the cost threshold value. Despite these guidelines, if no threshold is specified, the PM may propose an appropriate threshold value to optimize program trade-space, subject to Milestone Decision Authority (MDA) and user approval.

The program manager derives the Acquisition Program Baseline from the users' performance requirements, schedule requirements, and best estimates of total program cost consistent with projected funding. The sponsor of a capability needs document (i.e., Capability Development Document or Capability Production Document) provides a threshold and an objective value for each attribute that describes an aspect of a system or capability to be developed or acquired. The program manager will use this information to develop an optimal product within the available trade space. If the objective and the threshold values are the same, the sponsor indicates this in the capability needs document by including the statement, "Threshold = Objective"

Acquisition Program Baseline parameter values should represent the program as it is expected to be developed, produced and/or deployed, and funded. The baseline should only contain those parameters that, if thresholds are not met, will require the Milestone Decision Authority to re-evaluate the program and consider alternative program concepts or design approaches. The number of performance parameters should be limited to provide maximum trade space.

Per 10 USC 2435, the Department of Defense may not obligate funds for major defense acquisition programs after entry into System Development and Demonstration without a Milestone Decision Authority-approved baseline unless the Under Secretary of Defense for Acquisition, Technology, and Logistics specifically approves the obligation. DoD Instruction 5000.2 extends this policy to Acquisition Category IA programs. For an Acquisition Category IA program, the Assistant Secretary of Defense for Networks and Information Integration must approve the obligation.

2.1.1.1. APB Management and Content

The Joint Staff (J-8) will review the cost, schedule, and key performance parameter objective and threshold values in the Acquisition Program Baseline for Joint Requirements Oversight Council (JROC) Interest programs, and any other programs of significant joint interest (as determined by the J-8). The J-8 review will ensure that the objective and threshold values are consistent with the JROC-approved Capability Development Document, the Capability Production Document, and prior JROC decision(s). The review will also ensure that the baseline provides the necessary

warfighting capabilities affordably and within required time frames. (See also CJCS Instruction 3170.01.)

Performance. The total number of performance parameters should be the minimum number needed to characterize the major drivers of operational performance. Performance parameters should include the key performance parameters identified in the capability needs document(s) (i.e., Capability Development Document and Capability Production Document), and the values and meanings of thresholds and objectives should be consistent. (See also CJCS Instruction 3170.01D.)

The number and specificity of performance parameters may change over time. Early in a program, the Acquisition Program Baseline should reflect broadly defined, operational-level measures of effectiveness or measures of performance to describe needed capabilities. As a program matures, system-level requirements become better defined. The Milestone Decision Authority may also add performance parameters to the Acquisition Program Baseline other than the JROC-validated key performance parameters.

Schedule. Schedule parameters should include, as a minimum, the projected dates for program initiation, other major decision points, and initial operating capability. The Capability Development Document and Capability Production Document program summaries describe the overall program strategy for reaching full capability, and the timing of the delivery of each increment. The program manager may propose, and the Milestone Decision Authority may approve, other, specific, critical, system events.

Cost. Cost figures should reflect realistic cost estimates of the total program and/or increment. The Capability Development Document and Capability Production Document include a program affordability determination identified as life-cycle cost or, if available, total ownership cost. Budgeted amounts should never exceed the total cost thresholds (i.e., maximum costs) in the Acquisition Program Baseline. As the program progresses, the program manager can refine procurement costs based on contractor actual (return) costs from Technology Development, System Integration, System Demonstration, and Low-Rate Initial Production. The program manager should provide the refined estimates whenever updating the Acquisition Program Baseline.

For Acquisition Category IA programs, Acquisition Category I cost parameters apply with the addition of military pay and the cost of acquisition items procured with Defense Working Capital Funds.

The Acquisition Program Baseline should contain cost parameters (objectives and thresholds) for major elements of program life-cycle costs (or total ownership costs, if available), as defined in section 3.1. These elements include:

(1) Research, development, test, and evaluation costs;

(2) Procurement costs;

(3) Military construction costs;

(4) Acquisition-related operations and maintenance costs (that support the production and deployment phase), if any;

(5) Total system quantity (to include both fully configured development and production units);

(6) Average unit procurement cost (defined as total procurement cost divided by total procurement quantity); (Note: This item and number 7 below do not usually apply to business IT systems.)

(7) Program acquisition unit cost (defined as the total of all acquisition-related appropriations divided by the total quantity of fully configured end items); and

(8) Any other cost objectives established by the milestone decision authority. If system operating and support costs are included, they are normally expressed as annual operating and support costs per deployable unit (e.g., squadron or battalion) or individual system (e.g., ship), as appropriate.

The cost parameters are presented in base year dollars.

2.1.1.2. Acquisition Program Baseline in an Evolutionary Acquisition

Programs using an evolutionary acquisition strategy should design the Acquisition Program Baseline consistent with the sponsor's capability document(s) and the applicable approach outlined in Table 2.1.1.2.1.

Capability Development Document (CDD) or Capability Production Document (CPD)	**Acquisition Program Baseline (APB)**
CDD defines multiple increments of capability	APB contains multiple sets of parameter values, each set defining an increment
CDD incrementally updated and revalidated	APB values incrementally updated
Separate CDDs for each increment	Separate APBs for each increment
There is one CPD for each production increment	The corresponding APB should be updated to reflect the parameters in the CPD for that production increment

Table 2.1.1.2.1. APB Parameters under an Evolutionary Acquisition Strategy.

DoD Instruction 5000.2 requires the Milestone Decision Authority to formally initiate each increment of an evolutionary acquisition program. Program initiation may occur at Milestone B or C. Therefore, the program manager should develop goals for each program increment. Planned program goals (parameters and their values) for any program may be refined, according to the actual results demonstrated by the program.

2.1.1.3. APB Approval

The program manager, in coordination with the user/sponsor, prepares the Acquisition Program Baseline for program initiation. The program manager revises the Acquisition Program Baseline for each milestone review, and in the event of program restructurings or unrecoverable program deviations.

The Acquisition Program Baseline requires the concurrence of the Program Executive Officer for all acquisition category programs, and the concurrence of the Component Acquisition Executive for Acquisition Category ID and IAM programs.

For Acquisition Category I and IA programs, the Acquisition Program Baseline will be coordinated with the Under Secretary of Defense (Comptroller) (10 USC 2220 and DoD Instruction 5000.2) prior to Milestone Decision Authority approval. For Joint Requirements Oversight Council Interest Programs, the Acquisition Program Baseline must also be coordinated with the Joint Staff (J-8 or designee) prior to Milestone Decision Authority approval (CJCSI 3170.01).

2.1.2. Trade-Offs

Maximizing program manager and contractor flexibility to make cost/performance trade-offs is essential to achieving cost objectives. The program manager may treat the difference between an objective and its associated threshold as a "trade space," subject to agreement by the user.

The best time to reduce total ownership cost and program schedule is early in the acquisition process. Continuous cost/schedule/performance trade-off analyses can help attain cost and schedule reductions.

Cost, schedule, and performance may be traded within the "trade space" between the objective and the threshold without obtaining Milestone Decision Authority approval. Trade-offs outside the trade space (i.e., decisions that result in acquisition program parameter changes) require approval of both the Milestone Decision Authority and the capability needs approval authority. Validated key performance parameters may not be traded-off without approval by the validation authority. The program manager and the user should work together on all trade-off decisions.

2.2. Pre-Systems Acquisition: Technology Development Strategy

2.2.1. Technology Development

The acquisition framework incorporates a Technology Development Phase focused on the development, maturation, and evaluation of the technologies needed for the capability under consideration. Phase activities concentrate on maturing those technologies (consistent with recommended Technology Readiness Levels) and demonstrating readiness to proceed with program initiation. The Technology Development Phase ends when the Milestone Decision Authority determines that technologies are sufficiently mature. This determination, along with the satisfaction of other statutory and regulatory requirements, supports program initiation.

2.2.2. Required Information

The Technology Development Strategy focuses specifically on the activities of the Technology Development Phase. Where feasible, the Technology Development Strategy should also discuss activities associated with the post-program-initiation phases of the planned acquisition.

The Technology Development Strategy precedes the formal Acquisition Strategy and is required for Milestone A. The Technology Development Strategy is updated at subsequent milestones and subsumed into the Acquisition Strategy. If the Acquisition Strategy is approved at Milestone A, the Technology Development Strategy may be included in the Acquisition Strategy. While there is no mandatory format for the Technology Development Strategy, Public Law 107-314, Section 803, requires the following minimum content:

- A discussion of the planned acquisition approach, including a summary of the considerations and rationale supporting the chosen approach. For the preferred, evolutionary acquisition approach, whether spiral or incremental, DoD Instruction 5000.2 requires the following details:
    - A preliminary description of how the program will be divided into technology spirals and development increments;
    - The limitation on the number of prototype units that may be produced and deployed during technology development;
    - How prototype units will be supported; and
    - Specific performance goals and exit criteria that must be met before exceeding the number of prototypes that may be produced under the research and development program.
- A discussion of the planned strategy to manage research and development. This discussion must include and briefly describe the overall cost, schedule, and performance goals for the total research and development program. To the extent practicable, the total research and development program should include all planned technology spirals or increments.
- A complete description of the first technology demonstration. The description must contain specific cost, schedule, and performance goals, including exit criteria, for the first technology spiral demonstration.
- A test plan. The program manager must describe how the first technology spiral demonstration will be evaluated to determine whether the goals and exit criteria for the Technology Development phase have been achieved. The test plan is focused on the evaluation of the technologies being matured during the Technology Development phase. This plan is distinct from the separately developed and approved Test and Evaluation Strategy discussed in detail in section 9.6.1 of this Guidebook. The Test and Evaluation Strategy takes a broader view and is the tool used to begin developing the entire program test and evaluation strategy, including the initial test and evaluation concepts for Technology Development, System Development and Demonstration, and beyond.

DoD Instruction 5000.2 requires that each increment of an evolutionary acquisition program have a Milestone Decision Authority-approved Technology Development Strategy. It suggests that multiple technology development demonstrations may be necessary before the user and developer agree that a proposed technology solution is affordable, militarily useful, and based on mature technology. The Instruction also requires that the Technology Development Strategy be reviewed and updated upon completion of each technology spiral and development increment, and that approved updates support follow-on increments.

2.3. Systems Acquisition: Acquisition Strategy

The Acquisition Strategy results from extensive planning and preparation and a thorough understanding of both the specific acquisition program and the general defense acquisition environment. Development of the acquisition strategy requires collaboration between the Milestone Decision Authority, program manager, and the functional communities engaged in and supporting DoD acquisition. A well-developed strategy minimizes the time and cost required to satisfy approved capability needs, and maximizes affordability throughout the program life-cycle. Consistent with DoD Directive 5000.1, the program manager shall be the single point of accountability for accomplishing program objectives for total life-cycle systems management, including sustainment. The charge of DoD executive leadership is to use common sense and sound business practice in developing the acquisition strategy and executing the program. The program manager should organize an Integrated Product Team to assist in development and coordination of the Acquisition Strategy.

When developing the acquisition strategy, the program manager and supporting team members should keep in mind their total systems responsibility. A complete discussion of Total Life Cycle Systems Management, consistent with the policy direction of DoD Directive 5000.1, appears later in this Guidebook.

Consistent with statute and regulation, the program manager should tailor the program planning and required information to the specific program needs. Additionally, the needs of the decision makers who will coordinate or approve the strategy should guide the preparation of the acquisition strategy. 2.3.1. lists the principal considerations associated with developing the acquisition strategy.

Acquisition Strategy Considerations	Acquisition Approach	Modular Open Systems Approach
	Best Practices	
	Business Considerations	Product Support
	Capability Needs Summary	Program Structure
	Environment, Safety, Occupational Health	Relief, Exemption, and Waiver
	Human Systems Integration	Research and Technology Protection

	Information Assurance	
	Information Technology	Resource Management
	Integrated Test and Evaluation	Risk Management
	Interoperability	Systems Engineering

Table 2.3.1. Acquisition Strategy Considerations

DoD Instruction 5000.2, requires an approved Acquisition Strategy at program initiation. The acquisition strategy should be updated for all subsequent major decisions and program reviews, and whenever the approved strategy changes.

An acquisition strategy requires the concurrence of the Program Executive Officer (for programs in all acquisition categories) and the DoD Component Acquisition Executive (for Acquisition Category ID and IAM programs) prior to approval by the Milestone Decision Authority. Milestone Decision Authority approval of the Acquisition Strategy may precede a decision point; however, programs may not proceed beyond a decision point without a Milestone Decision Authority-approved strategy.

This section of the Guidebook covers *all* of the topics or activities the program manager *should* consider when developing a strategy. However, when tailored for a specific program, some topics may not apply. This Guidebook will identify the mandatory topics or practices, consistent with statute and regulation, with which the program manager must comply when planning the program, and indicate the information the program manager must include in the documented acquisition strategy.

2.3.1. Program Structure

The Acquisition Strategy guides program execution across the entire program life-cycle. The strategy evolves over time and should continuously reflect the current status and desired end point of the program. The strategy must be flexible enough to accommodate acquisition oversight decisions both on this program and on other programs that may affect this program. It should address the availability of required capabilities to be provided by other programs.

The Acquisition Strategy establishes the milestone decision points and acquisition phases planned for the program. The strategy should cover development, testing, production, and life-cycle support. It should prescribe the accomplishments for each phase, and identify the critical events affecting program management. The Acquisition Strategy should include a summary of the Integrated Master Plan and Integrated Master Schedule.

If the program manager decides to incorporate concurrency in the program, the Acquisition Strategy should discuss the benefits and risks of the concurrency and address the resultant risk mitigation and testing impacts.

2.3.1.1. Before Program Initiation

Pre-program-initiation activities may directly impact the acquisition strategy. Since this may precede the appointment of a program manager, the engaged DoD Components and other organizations, like the Office of the Director, Defense Research and Engineering, should consider the effect of "Pre-Systems Acquisition" activities on any future DoD acquisition program and the associated acquisition strategy that may evolve from their efforts. These organizations should plan for transition to the formal acquisition process and be prepared to communicate background information to the program manager. Once assigned, the program manager should capitalize on the transition planning and form a Working-Level Integrated Product Team to develop the acquisition strategy.

2.3.1.2. Tailoring

Consistent with statutory and federal regulatory requirements, the program manager and Milestone Decision Authority may tailor the phases and decision points for a program to meet the specific needs of the program. Tailoring should consider program category, risk, urgency of need, and technology maturity.

The acquisition strategy, prepared by the program manager and approved by the Milestone Decision Authority, ties all the acquisition activities together, forming the basis for sound program management. Tailored to the specific program, the strategy defines the entities, activities, and information requirements that will enable successful management and provide a program structure that will deliver timely and affordable capability to the users. Appropriately tailored information requirements support both decision making and provide a historical record of the program's maturation, management, and decision processes.

2.3.2. Acquisition Approach

The Acquisition Strategy defines the approach the program will use to achieve full capability: either evolutionary or single step; it should include a brief rationale to justify the choice. The DoD preference is evolutionary acquisition. When a program uses an evolutionary acquisition strategy, each increment should have a specific set of parameters with thresholds and objectives appropriate to the increment.

In an evolutionary approach, the Acquisition Strategy should fully describe the initial increment of capability (i.e., the initial deployment capability), and how it will be funded, developed, tested, produced, and supported. The Acquisition Strategy should preview similar planning for subsequent increments, and identify the approach to integrate and/or retrofit earlier increments with later increments.

If the capability documents do not allocate increments of capability (leading to full capability) to specific program increments consistent with an evolutionary approach, the program manager should work closely with the user/sponsor to determine whether an evolutionary acquisition approach will serve the user/sponsor needs. Where necessary and acceptable to the user/sponsor, the approval authority should modify the capability documents.

The approved Acquisition Strategy should address the proposed management approach to be used to define both the capability and the strategy applicable to each increment. This

discussion should specifically address whether end items delivered under early increments will be retrofitted with later increment improvements.

The Acquisition Strategy defines the management approach that will achieve program goals. The information included in the Acquisition Strategy should be complete enough to fully describe the planning considerations and decisions. Because the Acquisition Strategy establishes such essential aspects of a program as the degree of competition, contract type, and incentive arrangements, the Acquisition Strategy should be approved before a synopsis is published, a Justification and Approval is approved, or negotiations undertaken.

2.3.3. Capability Needs

To provide context, the acquisition strategy should contain a summary description of the capability the acquisition is intended to satisfy or provide. The summary should highlight system characteristics driven by interoperability and/or joint integrated architectures, capability areas, and families or systems of systems. The summary should also identify any dependency on the planned or existing capability of other programs or systems.

The summary should state whether the approved capability need is structured to achieve full capability in time-phased increments or in a single step. For time-phased capabilities, define the initial increment, as well as subsequent increments.

The acquisition strategy should identify the approved documents that define the requisite capability. These would include the Initial Capabilities Document and Capability Development Document.

The strategy should also briefly describe the status of draft capabilities documents. The strategy should identify significant aspects of the capability or capability area that are unsettled, and anticipate how this uncertainty could impact the acquisition strategy.

2.3.4. Test and Evaluation

Consistent with the direction of DoD Instruction 5000.2, the program manager must integrate test and evaluation throughout the acquisition process. The program manager should engage the Test and Evaluation Working-Level Integrated Product Team in the development of the acquisition strategy, and harmonize the acquisition strategy and the Test and Evaluation Strategy. The organizations managing the pre-Milestone B activities should be aware of the requirement in DoD Instruction 5000.2 that requires a Test and Evaluation Strategy for the Milestone A decision.

2.3.5. Risk Management

The program manager should establish a risk management process consistent with section 4.2.3.5., and summarize the process in the Acquisition Strategy. Effective risk management depends on the knowledge gleaned from all aspects of the program. ***Knowledge reduces risk.*** Risk management is a principal factor in the renewed and increased emphasis on *demonstration* evident in DoD Instruction 5000.2.

2.3.6. Resource Management

The acquisition strategy should address the estimated program cost and the planned program funding, including funding under an evolutionary acquisition strategy and advance procurement.

2.3.6.1. Funding Under an Evolutionary Acquisition Strategy

If an evolutionary approach is being used, the acquisition strategy should fully describe and fully fund the first increment of capability at program initiation. Funding of subsequent increments should be discussed to the extent the additional capability increments can be described. If the capability documents include a firm definition of the capability to be provided, by increment, the acquisition strategy should fully discuss the funding of each subsequent increment. Section 3.1.4. provides additional information on program funding under an evolutionary acquisition strategy.

2.3.6.2. Advance Procurement

DoD 7000.14-R requires that the procurement of end items be fully funded, i.e., the cost of the end items to be bought in any fiscal year must be completely included in that year's budget request. However, there are times when it is appropriate to procure some components, parts, materiel, or effort in advance of the end item buy. These items are referred to as advance procurements. Statutory authority for these advance procurements must be provided in the relevant authorization and appropriations acts.

Advance procurement funds are used in major acquisition programs for advance procurement of components whose long-lead times require purchase early in order to reduce the overall procurement lead-time of the major end item. Advance procurement of long lead components is an exception to the DoD "full funding" policy and must be part of the President's budget request. These expenditures are subject to the following limitations:

1. The cost of components, material, parts, and effort budgeted for advance procurement should be low compared to the total cost of the end item;
2. The program manager judges the benefits of the advance procurement to outweigh the inherent loss of or limitation to future Milestone Decision Authority flexibility;
3. The Milestone Decision Authority approves the advance procurement; and
4. The procurement received statutory authority, as discussed above.

As part of the milestone review, the Milestone Decision Authority should approve specific exit criteria for advance procurement. These specific exit criteria should be satisfied before the program manager releases any advance procurement funding for either the initial long lead-time items contract(s) or the contract(s) for individual, follow-on, long lead-time lots. The contracts office should initiate a separate contract action for advance procurement of long lead materiel.

2.3.7. Systems Engineering Plan

All programs responding to a capabilities or requirements document, regardless of acquisition category, shall apply a robust systems engineering approach and shall develop

a Systems Engineering Plan for Milestone Decision Authority approval in conjunction with each milestone review, and integrated with the Acquisition Strategy. (Acting Under Secretary of Defense for Acquisition, Technology, and Logistics policy memorandum)

The Systems Engineering Plan documents a program's systems engineering strategy early in the program definition stages and is updated periodically as a program matures. The Systems Engineering Plan describes a program's overall technical approach, including processes, resources, and metrics, and applicable performance incentives. The plan should address both government and contractor systems engineering activities across the program's life cycle. It should describe the systems engineering processes to be applied, the approach to be used to manage the system technical baseline, and how systems engineering will be integrated across the integrated product team structure. It should also detail the timing, conduct, entrance criteria, and success/exit criteria of technical reviews. Chapter 4 of this Guidebook provides additional systems engineering implementation guidance.

The plan should address how performance measures for program control will complement the design, development, production, and sustainment efforts to provide the necessary Milestone Decision Authority-level management insights to support the acquisition decision process. Integration and linkage with other program management control efforts such as integrated master plans, integrated master schedules, technical performance measures, and earned value management is fundamental to successful application.

There is no prescribed format for the Systems Engineering Plan. However, the plan should address how systems engineering will support the translation of system capability needs into a technical and system effective, suitable product that is sustainable at an affordable cost. Specifically, a well-prepared Systems Engineering Plan will address the integration of the technical aspects of the program with the overall program planning, systems engineering activities, and execution tracking.

For Acquisition Category ID and IAM programs, DoD Components should submit the Systems Engineering Plan (integrated with the Technology Development Strategy or acquisition strategy) to the Director, Defense Systems, at least 30 days before the scheduled Defense Acquisition Board or Information Technology Acquisition Board milestone review.

2.3.8. Interoperability

The Acquisition Strategy should describe the treatment of interoperability requirements. For example, if an evolutionary acquisition strategy involves successive increments satisfying time-phased capability needs, the program manager should address each increment and the transitions from increment to increment. The Acquisition Strategy should identify any waivers or deviations that have been requested, obtained, or expected to be requested. The Strategy should reflect full compliance with the interoperability considerations discussed in 4.4.2. and, for Information Technology, including National Security Systems, 7.3. and 7.6.

- *Information Interoperability.* The program manager should identify and assess the impact of technical, schedule, cost, and funding critical path issues (i.e., issues

that could impact the program manager's ability to execute the acquisition strategy) related to information interoperability. The program manager should also identify critical path issues in related program(s) (i.e., system(s) that will exchange information with the program manager's delivered system) and assess their potential impact.

- *Other-than Information Interoperability*. The program manager should identify and assess the impact of technical, schedule, cost, and funding critical path issues related to general interoperability concerns for the program manager's acquisition program. The program manager should also identify any critical path issues in other program(s) (i.e., system(s)) that will interoperate with or otherwise materially interact with the program manager's delivered system (e.g., fuel formulation and delivery systems, mechanical connectors, armament, or power characteristics) and assess their potential impact.

2.3.9. Information Technology

The Acquisition Strategy should summarize the Information Technology, including National Security Systems, infrastructure and support considerations identified in the appropriate capability document and described in the Information Support Plan (ISP). The Strategy should identify Information Technology, including National Security Systems, infrastructure enhancements required to support program execution. It should identify technical, schedule, and funding critical path issues for both the acquisition program and the Information Technology, including National Security Systems, infrastructure that could affect execution of the acquisition strategy. The Acquisition Strategy should describe support shortfalls and issues, and plans to resolve them. The Acquisition Strategy need not repeat the details found in the Information Support Plan, but should be consistent with the Information Support Plan and cross-reference it as practicable.

2.3.10. Research and Technology Protection

- *Protection of Critical Program Information*. The program manager should ensure that the Acquisition Strategy is consistent with the program protection measures of Chapter 8. The Acquisition Strategy should identify the technical, schedule, cost, and funding issues associated with protecting critical program information and technologies, and the plans to resolve the issues.
- *Anti-Tamper Measures*. The program manager should ensure the Acquisition Strategy is consistent with the anti-tamper measures of section 8.5.3. The program manager should plan and budget for post-production, anti-tamper validation of end items. The validation budget should not exceed $10 million (in FY 2001 constant dollars), and the duration of anti-tamper validation efforts should not exceed 3 years.

2.3.11. Information Assurance

The program manager should ensure that the Acquisition Strategy identifies the technical, schedule, cost, and funding issues associated with implementing information assurance.

The planning for and documentation of the Acquisition IA Strategy should produce the information required for this section. Section 7.5.9.5 lists potential IA considerations to be included in the Acquisition Strategy.

2.3.12.Product Support Strategy

The program manager should develop a product support strategy for life-cycle sustainment and continuous improvement of product affordability, reliability, and supportability, while sustaining readiness. The support strategy is a major part of the Acquisition Strategy. The IPPD process helps to integrate the support strategy with the systems engineering processes.

The program manager should consider inviting Military Service and Defense Logistics Agency logistics organizations to participate in product support strategy development and integrated product teams.

The support strategy describes the supportability planning, analyses, and trade-offs used to determine the optimum support concept for a materiel system and identify the strategies for continuous affordability improvements throughout the product life cycle. The support strategy evolves in detail, so that by Milestone C, it defines how the program will address the support and fielding requirements necessary to meet readiness and performance objectives, lower total ownership cost, reduce risks, and avoid harm to the environment and human health. The support strategy should address how the program manager and other responsible organizations will maintain oversight of the fielded system. It should also explain the contracting approach for product support throughout the system Life cycle (see section 5.3.1 for additional detail). See the full description of program manager responsibilities regarding Life-Cycle Logistics and Product Support Strategy in Chapter 4 (section 4.1.3) and Chapter 5 (sections 5.1.1 and 5.1.3).

2.3.13.Human Systems Integration

The program manager should integrate manpower, personnel, training, human factors, safety and occupational health, personnel survivability, and habitability considerations into the acquisition process. HSI initiatives optimize total system performance and minimize total ownership cost. The acquisition strategy should identify HSI responsibilities, describe the technical and management approach for meeting HSI requirements, briefly summarize the planning for each of the above elements of HSI, and summarize major elements of the associated training system.

2.3.14.Environment, Safety, and Occupational Health (ESOH)

Per DoD Instruction 5000.2, the program manager shall prevent ESOH hazards, where possible, and manage ESOH hazards where they cannot be avoided. The acquisition strategy will include a summary of the Programmatic ESOH Evaluation (PESHE), including a strategy for integrating ESOH considerations into the systems engineering process; ESOH risks and risk mitigation efforts; and a compliance schedule for National Environmental Policy Act (NEPA) (42 U.S.C. 4321-4370d and Executive Order (E.O.) 12114).

2.3.15.Modular Open Systems Approach (MOSA)

MOSA is the Department of Defense implementation of "open systems." The program manager should incorporate MOSA principles into the acquisition strategy to ensure access to the latest technologies and products, and to facilitate affordable and supportable system development and modernization of fielded assets.

The program manager should plan for MOSA implementation and include a summary of such planning as part of the overall Acquisition Strategy and to the extent feasible, the Technology Development Strategy. The summary of the MOSA planning should describe (1) how MOSA fits into a program's overall acquisition process and strategies for acquisition, technology development, and T&E; (2) what steps a program will take to analyze, develop, and implement a system or a system-of-systems architecture based on MOSA principles; and (3) how such program intends to monitor and assess its MOSA implementation progress and ensure system openness.

If upon completing a business case analysis, the program manager decides to acquire a system with closed interfaces, the program manager must report to the Milestone Decision Authority, in context of the acquisition strategy, the justification for the decision. The justification should describe the potential impacts on the ability to access latest technologies from competitive sources of supply throughout the system life cycle, integrate the system with other systems in a joint integrated architecture venue, and to integrate and/or retrofit earlier increments with later increments in an evolutionary acquisition context.

2.3.16.Business Considerations

As part of the Acquisition Strategy, the program manager should develop a comprehensive business strategy. Figure 2.3.16.1 depicts the principal considerations in developing the business strategy.

Figure 2.3.16.1. Business Considerations

2.3.16.1. Competition

Competition is key to fostering innovation for defense applications. The Acquisition Strategy for all programs should describe the competition planned for all phases of the program's life cycle, or explain why competition is not practicable or not in the best interests of the Government. To promote synergies that facilitate competition and innovation, the program manager should, where feasible, identify other applications for the technologies in development within the functional capability areas identified by the Joint Staff.

2.3.16.1.1. Fostering a Competitive Environment

2.3.16.1.1.1. Competition Advocates

Per 41 U.S.C. 418 and 10 U.S.C. 2318 the Head of each DoD Component with acquisition responsibilities designates competition advocates for the DoD Component and for each procurement activity within the DoD Component. The advocate for competition for each procurement activity promotes full and open competition and promotes the acquisition of commercial items, and challenges barriers to such acquisition such as restrictive statements of need, detailed specifications, or burdensome contract clauses.

2.3.16.1.1.2. Ensuring Future Competition for Defense Products

For some critical and complex Defense products, the number of competitive suppliers is now, or will soon be, limited. While it is DoD policy to rely on the marketplace to meet Department materiel capability needs, there may be exceptional circumstances in which

the Department needs to act to maintain future competition. Accordingly, the program manager, the Milestone Decision Authority, and the DoD Components should be open to and prepared for discussions considering the effects of their acquisition and budget plans on future competition.

The Deputies to CAEs routinely confer with the Deputy Under Secretary of Defense (Industrial Policy) (DUSD(IP)) to discuss areas where future competition may be limited and to provide the DUSD(IP) with information on such areas based on reporting from program managers and other sources. This group reviews areas that have been identified by program acquisition strategies, IPTs, sole-source Justifications and Approvals, and more generally from industry sources. Where appropriate, this group may establish a DoD team to evaluate specific product or technology areas. Based on analysis and findings of the team, the USD(AT&L) will decide what, if any, DoD action is required to ensure future competition in the sector involved. USD(AT&L) may direct any proposed changes in specific programs or may direct the Milestone Decision Authority to make such changes to a specific program.

2.3.16.1.2. Building Competition into Individual Acquisition Strategies

Program managers and contracting officers should provide for full and open competition, unless one of the limited statutory exceptions applies (FAR Subpart 6.3). Program managers and contracting officers should use competitive procedures best suited to the circumstances of the acquisition program. Program managers should plan for competition from the inception of program activity. Such competition planning should precede preparation of an acquisition strategy when, for example, a technology project or an effort involving advanced development or demonstration activities has potential to transition into an acquisition program. Competition planning should consider the immediate effort being undertaken and any foreseeable future procurement as part of an acquisition program. Competitive prototyping, competitive alternative sources, an open systems architecture, and competition with other systems that may be able to accomplish the mission should be used where practicable.

2.3.16.1.2.1. Applying Competition to Acquisition Phases

The acquisition strategy prepared to support program initiation should include the plans for competition for the long term. The strategy should be structured to make maximum use of competition throughout the life of the program. The intent of applying competition is to achieve performance and schedule requirements, improve product quality and reliability, and reduce cost.

2.3.16.1.2.2. Applying Competition to Evolutionary Acquisition

An evolutionary acquisition strategy is based on time-phased capabilities, and delivers an initial increment of capability and some number of subsequent increments until the full required capability is attained. Plans for competition should be tailored to each increment, and should consider successive increments. For example, if each increment adds a discrete capability, in a separable package, to a pre-established modular open system architecture, it may be possible and desirable to obtain full and open competition for each increment.

There is no presumption that successive increments must be developed or produced by the same contractor. The acquisition strategy should:

- Describe the plan for competition for the initial increment. State how the solicitation will treat the initial increment, and why. For example, the first increment may be:
    - A stand-alone capability, independent of any future procurements of subsequent increments;
    - The first in a series of time-phased capabilities, all of which are expected to need to be satisfied by the same prime contractor.
- State, for each successive increment, whether competition at the prime contract level is practicable, and why.
- When competition is practicable, explain plans for the transition from one increment to the next if there is a different prime contractor for each, and the manner in which integration issues will be addressed.

When competition is not planned at the prime contract level, the program manager should identify the FAR Part 6 reason for using other than full and open competition; explain how long, in terms of contemplated successive increments, the sole source is expected to be necessary; and address when and how competition will be introduced, including plans for bringing competitive pressure to bear on the program through competition at major subcontractor or lower tiers or through other means.

2.3.16.1.2.3. Competition and Source of Support

The DoD Directive 5000.1 policy on competition applies to source of support decisions. Specific competitive considerations include the following:

- The program manager should provide for the long-term access to data required for competitive sourcing of systems support throughout its life cycle.
- The source of supply support may be included in the overall system procurement or treated as a separate competition.
- The program manager should use sources of supply that provide for the most cost-effective system throughout its life cycle.

2.3.16.1.2.4. Industry Involvement

DoD policy encourages early industry involvement in the acquisition effort, consistent with the Federal Advisory Committee Act (FACA) and FAR Part 15. The acquisition strategy should address past and planned industry involvement. The program manager should apply knowledge gained from industry when developing the acquisition strategy; however, with the exception of the program manager's support contractors, industry should not directly participate in acquisition strategy development.

2.3.16.1.3. Potential Obstacles to Competition

2.3.16.1.3.1. Exclusive Teaming Arrangements

Two or more companies create an exclusive teaming arrangement when they agree to team to pursue a DoD acquisition program, and agree not to team with other competitors for that program. These teaming arrangements occasionally result in inadequate competition for DoD contracts. While the Department's preference is to allow the private sector to team and subcontract without DoD involvement, the Department may intervene, if necessary, to assure adequate competition. Intervention to break up a team requires Milestone Decision Authority approval.

2.3.16.1.3.2. Sub-Tier Competition

All acquisition programs should foster competition at sub-tier levels, as well as at the prime level. The program manager should focus on critical product and technology competition when formulating the acquisition strategy; when exchanging information with industry; and when managing the program system engineering and life cycle.

Preparation of the acquisition strategy includes an analysis of product and technology areas critical to meeting program needs. The acquisition strategy should identify the potential industry sources to supply these needs. The acquisition strategy should highlight areas of potential vertical integration (i.e., where potential prime contractors are also potential suppliers). Vertical integration may be detrimental to DoD interests if a firm employs internal capabilities without consideration of, or despite the superiority of, the capabilities of outside sources. The acquisition strategy should describe the program manager's approach (e.g., requiring an open systems architecture, investing in alternate technology or product solutions, breaking out a subsystem or component, etc.) to establish or maintain access to competitive suppliers for critical areas at the system, subsystem, and component levels.

During early exchanges of information with industry (e.g., the draft request for proposal process), program managers should identify the critical product and technology areas that the primes plan to provide internally or through exclusive teaming. The program manager should assess the possible effects of these choices on competition, and mitigate any potential loss of competition. If the assessment results in a change to the approved acquisition strategy, the program manager should propose the change to the Milestone Decision Authority.

As the program design evolves, the program manager should continue to analyze how the prime contractor is addressing the program's critical product and technology areas. This analysis may identify areas where the design unnecessarily restricts subsystem or component choices. Contractors should be challenged during requirements and design reviews to defend why planned materiel solutions for subsystem and component requirements critical to the program exclude other competitive choices. This monitoring should continue through the system life cycle (e.g., reprocurements, logistics support).

Similar reviews can be made after contract award. In accordance with FAR Subpart 44.2, *Consent to subcontracts*, program managers and contracting personnel have the right to review and approve or disapprove the make-buy decisions. These reviews should ensure decisions have considered better technical and cost effective solutions from other vendors.

2.3.16.1.4. Potential Sources

The program manager should consider both international and domestic sources, that can meet the required need, as the primary sources of supply (consistent with relevant domestic preference statutes, FAR Part 25, and Defense Federal Acquisition Regulation Supplement Part 225). The program manager should consider national policies on contracting and subcontracting with small business (15 U.S.C. 644); small and disadvantaged business (15 U.S.C. 637); women-owned small business (15 U.S.C. 631); Historically Underutilized Business Zone (HUBZone) small business (15 USC 632); and Service-Disabled, Veteran-Owned small business (15 USC 657f); and address considerations to secure participation of these entities at both prime and sub-tier levels. The program manager should consider intra-Government work agreements, i.e., formal agreements, project orders, or work requests, in which one Government activity agrees to perform work for another, creating a supplier/customer relationship.

2.3.16.1.4.1. Market Research

Market research is a primary means of determining the availability and suitability of commercial items and the extent to which the interfaces for these items have broad market acceptance, standards-organization support, and stability. Market research supports the acquisition planning and decision process, supplying technical and business information about commercial technology and industrial capabilities. Market research, tailored to program needs should continue throughout the acquisition process and during post-production support. FAR Part 10 requires the acquisition strategy include the results of completed market research and plans for future market research. (See also CJCS Manual 3170.01A.)

2.3.16.1.4.2. Commercial Items

The program manager should work with the user to define and, if necessary, modify capability needs to facilitate the use of commercial items. This includes hardware, software, interoperability, data interchange, packaging, transport, delivery, and automatic test systems. Within the constraints of the described capability needs, the program manager should require contractors and subcontractors to use commercial items to the maximum extent possible. While some commercial items may not provide system-level capabilities for Acquisition Category I and IA programs, numerous commercial components, processes, practices, and technologies have applicability to DoD systems. These considerations apply to subsystems, components, and spares based on the use of performance specifications and form, fit, function and interface specifications. The preference is to use commercial items. FAR Section 2.101 contains a definition of "commercial item." (See also section 4.4.5.)

The commercial marketplace widely accepts and supports open interface standards set by recognized standards organizations. These standards support interoperability, portability, scalability, and technology insertion. When selecting commercial items, the Department prefers open interface standards and commercial item descriptions. If acquiring products with closed interfaces, the program manager should conduct a business case analysis to justify acceptance of the potential economic impact on life-cycle cost and risk to technology maturation and insertion over the service life of the system.

2.3.16.1.4.3. Dual-Use Technologies

Dual-use technologies are technologies that meet a military need, yet have sufficient commercial application to support a viable production base. Market research and analysis helps to identify and evaluate possible dual-use technology and component development opportunities. Solicitation document(s) should encourage offerors to use, and the program manager should give consideration to, dual-use technologies and components. System design should facilitate the later insertion of leading edge, dual-use technologies and components throughout the system life cycle.

2.3.16.1.4.4. Use of Commercial Plants

Solicitation document(s) should encourage offerors to use commercial plants and integrate military production into commercial production as much as possible.

2.3.16.1.4.5. Industrial Capability

In many cases, commercial demand now sustains the national and international technology and industrial base. The following considerations will improve industry's capability to respond to DoD needs:

- Defense acquisition programs should minimize the need for new defense-unique industrial capabilities.
- Foreign sources and international cooperative development should be used where advantageous and within limitations of the law (DFARS Part 225).
- The Acquisition Strategy should promote sufficient program stability to encourage industry to invest, plan, and bear their share of risk. However, the strategy should not compel the contractor to use independent research and development funds or profit dollars to subsidize defense research and development contracts, except in unusual situations where there is a reasonable expectation of a potential commercial application.
- Prior to completing or terminating production, the DoD Components should ensure an adequate industrial capability and capacity to meet post-production operational needs.
- Where feasible, acquisition strategies should consider industrial surge capability. Unfinanced but approved requirements are one category. A second category is munitions, spares, and troop support items. These are likely surge candidates and should receive close attention and specific planning, to include use of contract options. Surge capability can be included in evaluation criteria for contract award.

To satisfy 10 U.S.C. 2440, development of the acquisition strategy should include an analysis of the industrial base capability to design, develop, produce, support, and, if appropriate, restart an acquisition program. The approved Acquisition Strategy should include a summary of this analysis (see DoD Directive 5000.60 and DoD 5000.60-H).

Considerations for the analysis include the following:

- The analysis should identify DoD investments needed to create or enhance certain industrial capabilities;

- The analysis should identify the risk of industry being unable to provide program design or manufacturing capabilities at planned cost and schedule;
- If the analysis indicates an issue beyond the scope of the program, the program manager should notify the Milestone Decision Authority and Program Executive Officer ;
- When the analysis indicates that industrial capabilities needed by the Department of Defense are in danger of being lost, the DoD Components should determine whether government action is required to preserve the industrial capability;
- The analysis should also address product technology obsolescence, replacement of limited-life items, regeneration options for unique manufacturing processes, and conversion to performance specifications at the subsystems, component, and spares levels.

DoD Directive 5000.60 imposes oversight restrictions on any proposed action or investment to preserve an industrial capability for an acquisition program. Any such investment with an anticipated cost of equal to or less than $10 million annually must be approved by the appropriate milestone decision authority, and any investment with a cost greater than $10 million annually must be approved by the Under Secretary of Defense for Acquisition, Technology, and Logistics.

2.3.16.1.5. Small Business Innovation Research (SBIR) Technologies

The program manager should develop an acquisition strategy that includes the use of technologies developed under the SBIR program, and gives favorable consideration for funding of successful SBIR technologies. The Department of Defense maintains an on-line, searchable database of SBIR-funded technologies.

2.3.16.2. International Cooperation

The globalization of today's economy requires a high degree of coordination and international cooperation. Consistent with information security and technology transfer limitations, the program manager should consider the following:

2.3.16.2.1. International Cooperative Strategy

The Acquisition Strategy should discuss the potential for increasing, enhancing, and improving the conventional forces of the North Atlantic Treaty Organization (NATO) and the United States, including reciprocal defense trade and cooperation, and international cooperative research, development, production, and logistic support. The Acquisition Strategy should consider the possible sale of military equipment. The discussion should specifically address the following four topics (10 U.S.C.2350a):

- Identification of similar projects under development or in production by a U.S. ally;
- Assessment of whether the similar project could satisfy U.S. capability needs or be modified in scope to satisfy the military need;

- Assessment of the advantages and disadvantages, with regard to program timing, developmental and life-cycle costs, technology sharing, and Rationalization, Standardization, and Interoperability, of seeking a cooperative development program; and
- The recommendation of the USD(AT&L) as to whether the Department of Defense should explore the feasibility and desirability of a cooperative development program.

The Milestone Decision Authority should review and approve the Acquisition Strategy for all programs at each acquisition program decision in accordance with 10 U.S.C. 2350a. All international considerations should remain consistent with the maintenance of a strong national technology and industrial base with mobilization capability. Restricted foreign competition for the program due to industrial base considerations requires prior USD(AT&L) approval. Results of the T&E of systems using approved international test operating procedures may be accepted without repeating the testing.

2.3.16.2.2. International Interoperability

The growing requirement for effective international coalitions requires a heightened degree of international interoperability. Reciprocal trade, international standardization agreements, and international cooperative programs with allies and friendly nations serve that end. The acquisition community should strive to deploy and sustain systems, equipment, and consumables that are interoperable with our potential coalition partners.

2.3.16.2.3. International Cooperation Compliance

To promote increased consideration of international cooperation and interoperability issues early in the development process, the program manager should discuss cooperative opportunities in the Acquisition Strategy at each acquisition program milestone (10 U.S.C. 2350a):

- Include a statement indicating whether or not a project similar to the one under consideration is in development or production by one or more major allies or NATO organizations.
- If there is such a project, provide an assessment as to whether that project could satisfy, or be modified in scope to satisfy, U.S. military capability needs.
- Provide an assessment of the advantages and disadvantages, with regard to program timing, life-cycle costs, technology sharing, standardization, and interoperability, of a cooperative program with one or more major allies or NATO organizations.

Program managers should seek the most efficient and cost-effective solution over the system's life cycle. Many times, the use or modification of systems or equipment that the Department already owns is more cost-effective and schedule-effective than acquiring new materiel.

Section 11.2. has additional details on international cooperation considerations.

2.3.16.2.4. Testing Required for Foreign Military Sales

An Acquisition Category I or II system that has not successfully completed initial operational test and evaluation (IOT&E) requires USD(AT&L) approval prior to any foreign military sale, commitment to sell, or DoD agreement to license for export. This does not preclude Government-sponsored discussions of potential cooperative opportunities with allies, or reasonable advance business planning or marketing discussions with potential foreign customers by defense contractors, provided appropriate authorizing licenses are in place.

2.3.16.3. Contract Approach

The events set forth in contracts should support the exit criteria for the phase.

2.3.16.3.1. Performance-Based Business Strategy

Consistent with a Performance-Based Business Environment, the acquisition strategy should include a performance-based business strategy.

2.3.16.3.2. Modular Contracting

The program manager should use modular contracting, as described in FAR Section 39.103, for major IT acquisitions, to the extent practicable. Program managers should consider using modular contracting for other acquisition programs. (See also section 7.8.3.10.)

2.3.16.3.3. Contract Bundling

Federal Acquisition Regulation 7.103(s) requires that acquisition planners, to the maximum extent practicable, avoid unnecessary and unjustified bundling that precludes small business participation as contractors. As a result of this direction, DoD Instruction 5000.2 requires a Benefit Analysis and Determination. The program manager should consult the Office of Small and Disadvantaged Business Utilization website for additional information concerning this information requirement.

2.3.16.3.4. Major Contract(s) Planned

For each major contract planned to execute the acquisition strategy, the acquisition strategy should describe what the basic contract buys; how major deliverable items are defined; options, if any, and prerequisites for exercising them; and the events established in the contract to support appropriate exit criteria for the phase or intermediate development activity.

2.3.16.3.5. Multi-Year Contracting

In accordance with 10 U.S.C. 2306b, the acquisition strategy should address the program manager's consideration of multiyear contracting for full rate production, and address the program manager's assessment of whether the production program is suited to the use of multiyear contracting based on the requirements in FAR Subpart 17.1.

2.3.16.3.6. Contract Type

For each major contract, the acquisition strategy identifies the type of contract planned (e.g., firm fixed-price (FFP); fixed-price incentive, firm target; cost plus incentive fee; or cost plus award fee) and the reasons it is suitable, including considerations of risk assessment and reasonable risk-sharing by the Government and the contractor(s). The acquisition strategy should not include cost ceilings that, in essence, convert cost-type research and development contracts into fixed-price contracts or unreasonably cap annual funding increments on research and development contracts. Fixed-price development contracts of $25 million or more or fixed-price-type contracts for lead ships require the prior approval of the USD(AT&L) (DFARS Section 235.006), regardless of a program's Acquisition Category.

2.3.16.3.7. Contract Incentives

The Acquisition Strategy should explain the planned contract incentive structure, and how it incentivizes the contractor(s) to provide the contracted product or services at or below the established cost objectives. If more than one incentive is planned for a contract, the Acquisition Strategy should explain how the incentives complement each other and do not interfere with one another.

2.3.16.3.8. Integrated Contract Performance Management

The program manager should obtain integrated cost and schedule performance data to monitor program execution.

2.3.16.3.9. Special Contract Terms and Conditions

The Acquisition Strategy should identify any unusual contract terms and conditions and all existing or contemplated deviations to the FAR or DFARS.

2.3.16.3.10. Warranties

The program manager should examine the value of warranties on major systems and pursue them when appropriate and cost-effective. If appropriate, the program manager should incorporate warranty requirements into major systems contracts in accordance with FAR Subpart 46.7.

2.3.16.3.11. Component Breakout

The program manager should consider component breakout on every program, and break out components when there are significant cost savings (inclusive of Government administrative costs), the technical or schedule risk of furnishing Government items to the prime contractor is manageable, and there are no other overriding Government interests (e.g., industrial capability considerations or dependence on contractor logistics support). The Acquisition Strategy should address component breakout, and briefly justify the component breakout strategy (see DFARS Appendix D). It should list all components considered for breakout, and provide a brief rationale (based on supporting analyses from a detailed component breakout review (which shall not be provided to the Milestone Decision Authority unless specifically requested)) for those not selected. the program manager should provide the rationale for a decision not to break out any components.

2.3.16.4. Leasing

The program manager should consider the use of leasing in the acquisition of commercial vehicles and equipment whenever the program manager determines that leasing of such vehicles is practicable and efficient. Leases are limited to an annual contract with no more than a 5-month lease option.

The program manager may not enter into any lease with a term of 18 months or more, or extend or renew any lease for a term of 18 months or more, for any vessel, aircraft, or vehicle, unless the program manager has considered all costs of such a lease (including estimated termination liability) and has determined, in writing, that the lease is in the best interest of the Government (10 U.S.C. 2401a). It should be noted that a lease of more than 12 months does not permit the extension of one year funding authority.

Leases of equipment to meet a valid need under the provisions of CJCS Instruction 3170.01 will be categorized in accordance with the criteria in DoD Instruction 5000.2.

For further guidance on leasing, see Office of Management and Budget Circular A-11, Appendix B, *Budgetary Treatment of Lease-Purchases and Leases of Capital Assets*; and Office of Management and Budget Circular A-94, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*.

2.3.16.5. Equipment Valuation

Equipment Valuation is a DoD initiative to value, capitalize, and depreciate DoD equipment. The activity will enable the Department of Defense to identify, track, and account for military assets, and assists in computing the net costs of operations.

2.3.16.5.1. Program Description

To implement this initiative, the program manager for any program, project, product, or system that has deliverable end items with a unit cost at or above $100,000 (the current *capitalization threshold*) should prepare a program description as part of the acquisition strategy at Milestone C. The program manager should calculate the unit cost by summing the estimated cost of the end item with the estimated costs of all associated government furnished equipment, training manuals, technical data, engineering support, etc., NOT including spares and support equipment. The description should identify the following deliverables:

- The end item(s) meeting the unit cost threshold (i.e., $100,000);
- The government furnished property that will be included in the end item;
- Other deliverables that will accompany the end item (e.g., manuals, tech data, etc.); and
- Other types of deliverables that will be bought with program funding (e.g., initial spares, support equipment, special tooling and test equipment, etc.) but that cannot be directly attributed to a specific end item.

2.3.16.5.2. Accounting Review

The program manager should provide a copy of the program description to the accounting specialist who supports the accounting transactions for the program. The accounting specialist will review the description(s) and compare them to applicable federal accounting standards (e.g., *Statement of Federal Financial Accounting Standard Number 23)* and financial management regulations.

If the accounting specialist determines that the program will not deliver end items that fall within applicable accounting standards/regulation criteria, no further actions are needed. However, if the accounting specialist determines that the program will deliver end items that fall within applicable accounting standards/regulation criteria (i.e., the program is a "capital" program), the program manager must include a statement in the appropriate commitment documents and contract requisitions that these documents and requisitions are part of a capital program.

2.3.16.5.3. Contract Implications

In addition to the statement in the commitment document and contract requisitions, the proposed statement of objectives must make clear which of the end items, GFP or other deliverables identified in the description required by paragraph 2.3.16.5.1 are within the scope of the proposed contract, i.e., which of the deliverables are to be procured by this contract.

Additional guidance for contracting officers will be provided separately.

2.3.17.Best Practices

In tailoring an acquisition strategy, the program manager should address management constraints imposed on contractors. Program managers should avoid imposing Government-unique restrictions that significantly increase industry compliance cost, or unnecessarily deter qualified contractors, including non-traditional defense firms, from proposing. Examples of practices that support the implementation of these policies include Integrated Product and Process Development; performance-based specifications; management goals; reporting and incentives; a modular open systems approach that emphasizes modularity and use of commercially supported practices, products, performance specifications, and performance-based standards; replacement of Government-unique management and manufacturing systems with common, facility-wide systems; technology insertion for continuous affordability improvement throughout the product life cycle; realistic cost estimates and cost objectives; adequate competition among viable offerors; best value evaluation and award criteria; the use of past performance in source selection; results of software capability evaluations; Government-Industry partnerships consistent with contract documents; and the use of pilot programs to explore innovative practices. The Milestone Decision Authority should review best practices at each decision point. While not mandatory, program managers should not release Requests for Proposal until the Milestone Decision Authority has approved the Acquisition Strategy.

2.3.18.Relief, Exemption, or Waiver

The program manager should identify mandatory acquisition process requirements that fail to add value, are not essential, or are not cost effective, and seek the appropriate relief, exemption, or waiver.

2.3.19.Additional Acquisition Strategy Topics

The Acquisition Strategy should also briefly address the program manager's consideration of, decisions on, and planning for the following additional topics:

- ***Program Office Staffing and Support Contractor Resources Available to the Program Manager.*** The program manager should identify resource limitations that prevent the program manager from pursuing a beneficial acquisition strategy or contracting approach (e.g., component breakout (i.e., the Government contracts for a component and furnishes it to the prime contractor), or the use of an award fee contract). The program manager should provide an estimate of the additional resources needed to implement the desirable strategy or approach.
- ***Integrated Digital Environment Management.*** The program manager should summarize plans to establish a cost-effective data management system and digital environment consistent with paragraph 11.12.
- ***Government Property in the Possession of Contractors Management.*** *The program manager should* summarize the planned management of GPPC.
- ***Simulation Based Acquisition and Modeling and Simulation.*** The program manager should summarize the planned implementation of Simulation Based Acquisition and Modeling and Simulation during engineering, manufacturing, and design trade studies; and during developmental, operational, and live fire testing. (See 11.13.)
- ***Software-Intensive Programs Review.*** The program manager should describe the planned use of independent expert reviews for all Acquisition Category I through Acquisition Category III software-intensive programs.

CHAPTER 3
Affordability and Life-Cycle Resource Estimates

3.0. Overview

3.0.1. Purpose

This chapter addresses acquisition program affordability and resource estimation. It provides explanations of the program and pre-program activities and information required by DoD Instruction 5000.2, and discusses the support and documentation provided by Office of the Secretary of Defense staff elements.

3.0.2. Contents

Section 3.1 is informational. It provides introductory background material intended for a general audience. It describes the concept of program Lifecycle cost, and provides definitions of terms used by the DoD cost community.

The next five sections are more specialized; they discuss the specific milestone review procedures, expectations, and best practices for a variety of topics related to acquisition program affordability, cost, and manpower. Section 3.2 describes the basic policies associated with the consideration of affordability in the acquisition process, and offers one possible analytic approach to the preparation of affordability assessments. This section also explains the Department's full-funding policy, and describes the concept known as Cost as an Independent Variable. Section 3.3 describes the Analysis of Alternatives process. Sections 3.4, 3.4.1, and 3.4.2 discuss the Cost Analysis Improvement Group (CAIG), resident in the Office of the Secretary of Defense (OSD). The OSD CAIG prepares independent Lifecycle cost estimates for major defense acquisition programs at major milestone reviews, and concurrently reviews cost estimates prepared by the program office and/or the DoD Component cost agency. Section 3.5 describes the review procedures for manpower estimates. Section 3.6 discusses procedures unique to major automated information systems.

The last section, 3.7,is intended for less experienced cost analysts working in the acquisition community. This section provides a recommended analytic approach for preparing a Lifecycle cost estimate for a defense acquisition program.

3.1. Lifecycle Costs/Total Ownership Costs

3.1.1. Introduction

Both DoD Directive 5000.1, *The Defense Acquisition System*, and DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, make reference to Lifecycle cost and total ownership cost. This section of the Guidebook explains the meaning of each these terms. The terms are similar in concept, but significantly different in scope and intent. For a defense acquisition program, Lifecycle cost consists of research and development costs, investment costs, operating and support costs, and disposal costs over

the entire Lifecycle. These costs include not only the direct costs of the acquisition program, but also include indirect costs that would be logically attributed to the program. The concept of total ownership cost is related, but broader in scope. Total ownership cost consists of the elements of Lifecycle cost, as well as other infrastructure or business process costs not necessarily attributable to the program. Susequent sections more carefully define and describe these concepts.

When programs are less mature (in pre-systems acquisition or system development and demonstration), program cost estimates that are supporting the acquisition system normally are focused on Life-cycle cost or elements of Life-cycle cost. Examples of such cases where cost estimates support the acquisition system at a macro level include affordability assessments, analyses of alternatives, cost-performance trades, and establishment of program cost goals. In addition, more refined and discrete Life-cycle cost estimates may be used within the program office to support internal decision-making such as evaluations of design changes and assessment of producibility, reliability, maintainability, and supportability considerations. However, as programs mature (transition from production and deployment to sustainment), cost estimates that support the acquisition system or program management in many cases may need to be expanded in scope to embrace total ownership cost concepts.

3.1.2.. Life-Cycle Cost Categories and Program Phases

DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures*, provides standardized definitions of cost terms that in total comprise system Lifecycle costs. Lifecycle cost can be defined as the sum of four major cost categories, where each category is associated with sequential but overlapping phases of the program Lifecycle. Lifecycle cost consists of (1) research and development costs, associated with the Concept Refinement phase, Technology Development phase, and the System Development and Demonstration phase, (2) investment costs, associated with the Production and Deployment phase, (3) operating and support costs, associated with the sustainment phase, and (4) disposal costs, occurring after initiation of system phase-out or retirement, possibly including demilitarization, detoxification, or long-term waste storage. Figure 3.1.2.1. depicts a notional profile of annual program expenditures by cost category over the system Lifecycle.

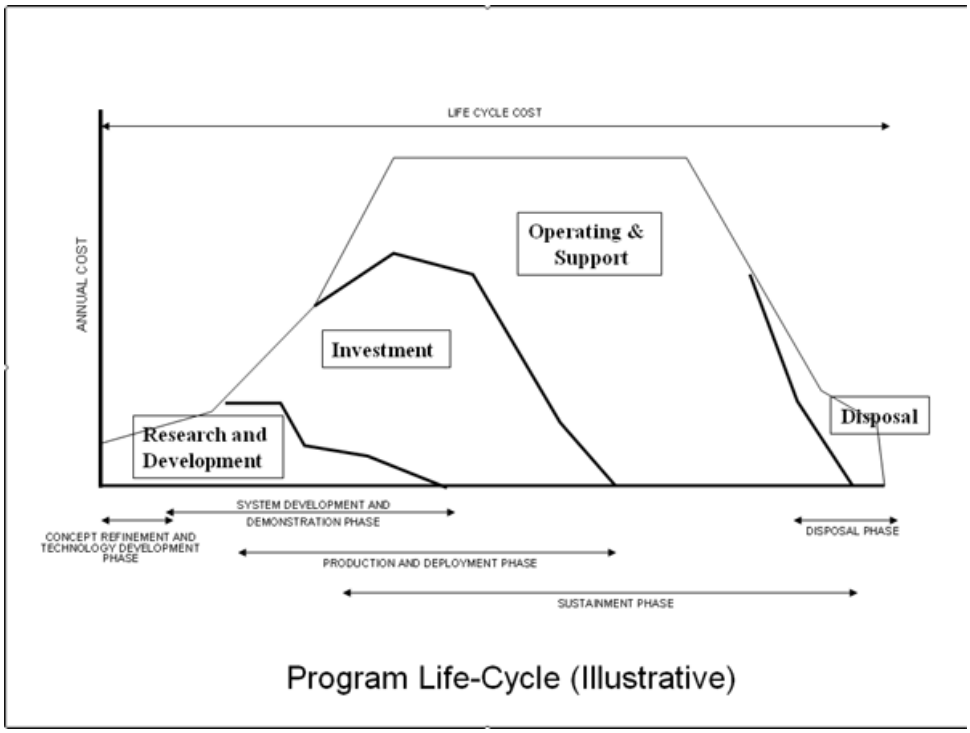

Figure 3.1.2.1. Illustrative Program Life Cycle

3.1.3. Life-Cycle Cost Category Definitions

The following paragraphs summarize the primary cost categories associated with each program Lifecycle phase:

- **Research and Development** consists of development costs incurred from the beginning of the conceptual phase through the end of the System Development and Demonstration phase, and potentially into Low-Rate Initial Production. Typically includes costs of concept refinement trade studies and advanced technology development; system design and integration; development, fabrication, assembly, and test of hardware and software for prototypes and/or engineering development models; system test and evaluation; system engineering and program management; peculiar support (peculiar and common support equipment, peculiar training equipment/initial training, and technical publications/data) and initial spares and repair parts associated with prototypes and/or engineering development models.
- **Investment** consists of production and deployment costs incurred from the beginning of low rate initial production through completion of deployment. Typically includes costs associated with producing and deploying the primary hardware; system engineering and program management; peculiar support

(peculiar and common support equipment, peculiar training equipment/initial training, and technical publications/data) and initial spares and repair parts associated with production assets; and military construction and operations and maintenance associated with system site activation.

- **Operating and Support** consists of sustainment costs incurred from the initial system deployment through the end of system operations. Includes all costs of operating, maintaining, and supporting a fielded system. Specifically, this consists of the costs (organic and contractor) of personnel, equipment, supplies, software, and services associated with operating, modifying, maintaining, supplying, training, and supporting a system in the DoD inventory. This includes costs directly and indirectly attributable to the system (i.e., costs that would not occur if the system did not exist), regardless of funding source or management control. Direct costs refer to the resources immediately associated with the system or its operating unit. Indirect costs refer to the resources that provide indirect support to the system's manpower or facilities. For example, the pay and allowances reflected in composite standard rates for a unit-level maintenance technician would be treated as a direct cost, but the (possibly allocated) cost of medical support for the same technician would be an indirect cost.
- **Disposal** consists of costs associated with demilitarization and disposal of a military system at the end of its useful life. These costs in some cases represent only a small fraction of a system's Lifecycle cost and may not be considered when preparing Lifecycle cost estimates. However, it is important to consider demilitarization and disposal early in the Lifecycle of a system because these costs can be significant, depending on the characteristics of the system. Costs associated with demilitarization and disposal may include disassembly, materials processing, decontamination, hardware, collection/storage/disposal of hazardous materials and/or waste, safety precautions, and transportation of the system to and from the disposal site. Systems may be given credit in the cost estimate for resource recovery and recycling considerations.

The Lifecycle cost categories correspond not only to phases of the acquisition process, but also to budget appropriations as well. Research and Development costs are funded from RDT&E appropriations, and investment costs are funded from Procurement and MILCON appropriations. Operating and support costs are funded from Military Personnel, Operations and Maintenance, and Procurement appropriations. However, some major automated information system programs may use defense working capital fund (DWCF) financing in place of appropriated funding (such as DWCF capital funds instead of procurement funds, or DWCF operating funds instead of operations and maintenance funds). The cost categories used in most acquisition documents (such as Selected Acquisition Reports and Acquisition Program Baselines) and in most budget documents (such as budget item justifications) are based on the appropriation terms. (Note that the term “program acquisition cost” as used in acquisition documents is the sum of RDT&E, Procurement, and possibly MILCON costs.)

3.1.4.. Implications of Evolutionary Acquisition

The application of Lifecycle cost categories to program phases may need to be modified for programs with evolutionary acquisition strategies. DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, describes the evolutionary acquisition approach for acquisition programs. In an evolutionary approach, the ultimate capability delivered to the user is provided in increasing increments. Evolutionary acquisition strategies (1) define, develop, produce and deploy an initial, militarily useful capability (Increment 1) based on proven technology, demonstrated manufacturing capabilities, and time-phased capabilities needs; and (2) plan for subsequent development, production and deployment of increments beyond the initial capability over time (Increments 2 and beyond). DoD Instruction 5000.2 offers two types of approaches to achieve evolutionary acquisition:

Spiral Development. The capability needs document(s) include a firm definition of the first increment, but the remaining interim increments and the precise end-state capabilities are not known at program initiation. The acquisition strategy defines the first increment of capability, and how it will be funded, developed, tested, produced, and supported. The acquisition strategy also describes the desired general capability the evolutionary acquisition is intended to satisfy, and establishes a management approach that will be used to define the exact capabilities needs for each subsequent increment.

Incremental Development. The capability needs documents(s) include a firm definition of the entire end-state capability, as well as firm definitions of interim increments, including an initial operating capability date for each increment. In this case, the program acquisition strategy defines each increment of capability and how it will be funded, developed, tested, produced, and operationally supported.

For a program with evolutionary acquisition, the question often arises concerning the scope of the Lifecycle cost estimate presented at a milestone review. In the case of incremental development, the entire acquisition program (including all future increments) is included in the scope of the program to be approved at the review. The entire program therefore typically is included in the corresponding Lifecycle cost estimate. In the case of spiral development, the situation will vary somewhat depending on circumstances. Normally, the Lifecycle cost estimate should attempt to reflect in the Cost Analysis Requirements Description (CARD) as much of the program as can be defined at the time of the milestone review, and any exclusions (for portions of the program that cannot be defined at that time) should be clearly identified.

In either case, the application of Lifecycle cost categories and program phases (as described in section 3.1.2) may need to be modified to account for the evolutionary acquisition strategy. Figure 3.1.4.1. depicts a notional profile of annual program expenditures by cost category for a program with evolutionary acquisition.

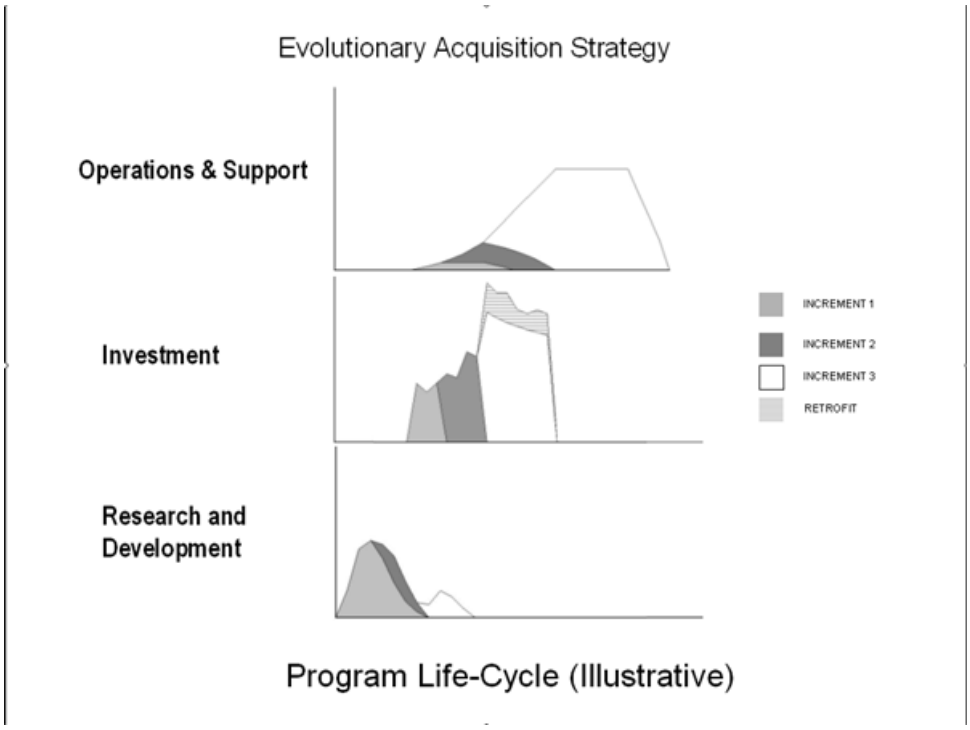

Figure 3.1.4.1.. Illustrative Program Life Cycle under Evolutionary Acquisition

3.1.5. Total Ownership Costs

As explained earlier, total ownership cost consists of the elements of a program's Lifecycle cost, as well as other infrastructure or business processes costs not necessarily attributable to the program. Infrastructure is used here in the broadest possible sense, and consists of all military department and defense agency activities that sustain the military forces assigned to the combatant and component commanders. Major categories of infrastructure are support to equipment (acquisition and central logistics activities), support to military personnel (non-unit central training, personnel administration and benefits, and medical care), and support to military bases (installations and communications/information infrastructure).

In general, traditional Lifecycle cost estimates are in most cases adequate in scope to support decisions involving system design characteristics (such as system weight, material mix, or reliability and maintainability). However, in special cases, depending on the issue at hand, the broader perspective of total ownership cost may be more appropriate than the Lifecycle cost perspective, which may be too narrow to deal with the particular context. As discussed previously, for a defense acquisition program, Lifecycle costs include not only the direct costs of the program, but also include indirect costs that would be logically attributed to the program. In a typical Lifecycle cost estimate, the estimated indirect costs would include only the costs of infrastructure support specific to

the program's military manpower (primarily medical support and system-specific training) and the program's associated installations or facilities (primarily base operating support and facilities sustainment, restoration and modernization). Many other important infrastructure activities (such as recruiting and accession training of new personnel, individual training other than system-specific training, environmental and safety compliance, contract oversight support from the Defense Contract Management Agency and the Defense Contract Audit Agency, and most management headquarters functions) are normally not considered in the scope of a traditional acquisition program Lifecycle cost estimate. In addition, important central (i.e., wholesale) logistics infrastructure activities such as supply chain management are implicitly incorporated in a traditional Lifecycle cost estimate, but their costs are somewhat hidden (because these costs are reflected in the surcharges associated with working capital fund arrangements and are not explicitly identified). However, there could easily be cases where consideration of such infrastructure activities would be important and would need to be explicitly recognized in a cost estimate or analysis. Examples of such cases are cost analyses tied to studies of alternative system support concepts and strategies; reengineering of business practices or operations; environment, safety, and occupational health considerations; or competitive sourcing of major infrastructure activities. In these cases, the traditional Lifecycle cost structure may not be adequate to analyze the issue at hand, and the broader total ownership cost perspective would be more appropriate. For such instances, the typical Lifecycle cost tools and data sources would need to be augmented with other tools and data sources more suitable to the particular issue being addressed.

3.2. Affordability

DoD Directive 5000.1 provides the fundamental acquisition policies for cost and affordability and program stability. Affordability can be defined as the degree to which the Lifecycle cost of an acquisition program is in consonance with the long-range modernization, force structure, and manpower plans of the individual DoD Components, as well as for the Department as a whole. The remainder of this section discusses different aspects of affordability. Section 3.2.1 describes how affordability is considered during the identification of military capability needs, and at acquisition milestone reviews. Section 3.2.2 provides some recommended analytic approaches to the preparation of affordability assessments. Section 3.2.3 explains the Department's full-funding policy. And section 3.2.4 describes a process known as Cost As an Independent Variable, which can be used to ensure that Lifecycle cost has equal consideration with performance and schedule in program decisions. (See section 5.1.3.5.)

3.2.1. Affordability Considerations

Affordability plays an important part in program decisions throughout the Life-cycle. Even before a program is formally approved for initiation, affordability plays a key role in the identification of capability needs. Program affordability is part of the Joint Capabilities Integration and Development System analysis process, which balances cost versus performance in establishing key performance parameters. Moreover, all elements of Life-cycle cost (or total ownership cost, if applicable) are included in the resulting capability needs document(s). Cost goals are established in terms of thresholds and

objectives to provide flexibility for program evolution and to support further Cost-as-an-Independent-Variable trade-off studies.

The Milestone Decision Authority considers affordability at each decision point. In part, this consideration ensures that sufficient resources (funding and manpower) are programmed and budgeted to execute the program acquisition strategy. The Milestone Decision Authority also examines the realism of projected funding over the programming period and beyond, given likely DoD Component resource constraints. To support this determination, the DoD Components are required to submit affordability assessments. The affordability assessment is discussed in the next section.

3.2.2. Affordability Assessments

For major defense acquisition programs and major automated information system programs, affordability assessments are required at Milestones B and C (see DoD Instruction 5000.2, Enclosure 3). The purpose of the assessment is for the DoD Component to demonstrate that the program's projected funding and manpower requirements are realistic and achievable, in the context of the DoD Component's overall long-range modernization plan. Normally, this assessment requires a DoD Component corporate perspective, and so the affordability assessment should not be prepared by the program manager. Rather, the assessment typically should be conducted by resource analysts in the DoD Component headquarters or supporting organization. For a joint program, the affordability assessment should be prepared by the lead DoD Component, although it may be necessary to display separate analyses for each DoD Component, as appropriate.

The exact approach to the affordability assessment can vary, depending on the nature of the program. However, in general, the assessment should address program funding and manpower requirements over the six-year programming period, and several years beyond. The assessment also should show how the projected funding and manpower fits within the overall DoD Component plan for modernization and manpower. In most cases, the overall long-range modernization plan will be portrayed across the DoD Component's mission areas. The assessment then should use this information to examine, for the acquisition program's mission area, the projected modernization funding and manpower demands, as a percentage of the DoD Component's total funding and manpower. The assessment should highlight those areas where the projected funding or manpower share exceeds historical averages, or where the projected funding or manpower exceeds zero real growth from the last year of the programming period. For the issues highlighted, the assessment should provide details as to how excess funding or manpower demands will be accommodated by reductions in other mission areas, or in other (i.e., non-modernization) accounts. To illustrate this approach, this section provides a notional example of the type of analyses that could be incorporated in an affordability assessment. Although this example only addresses modernization funding, the approach for manpower would be similar.

In this hypothetical example, a major defense acquisition program is nearing Milestone B approval. For discussion purposes, this program arbitrarily is assumed to be a mobility program. A first step in the program's affordability assessment is to portray the projected annual modernization funding (RDT&E plus procurement, measured as total obligation

authority, or TOA) in constant dollars for the six-year programming period, and, in addition, for an additional twelve years beyond that. Similar funding streams for other acquisition programs in the same mission area (in this example, mobility) also would be included.Figure 3.2.2.1 is a sample chart for this first step. In this example, the acquisition program nearing milestone approval is labeled “Mobility MDAP #3.” Funding also is shown for the other modernization programs in the same mission area, consisting of three other major defense acquisition programs, three other (Acquisition Category II) programs, and one miscellaneous category for minor procurement. In this example, there appears to be a significant modernization bow wave beginning around 2014, which would then be subject to further analysis and discussion in the assessment. The term “bow wave” refers to a requirement for excess modernization funds during a period beyond the programming period, resulting from acquisition decisions made earlier.

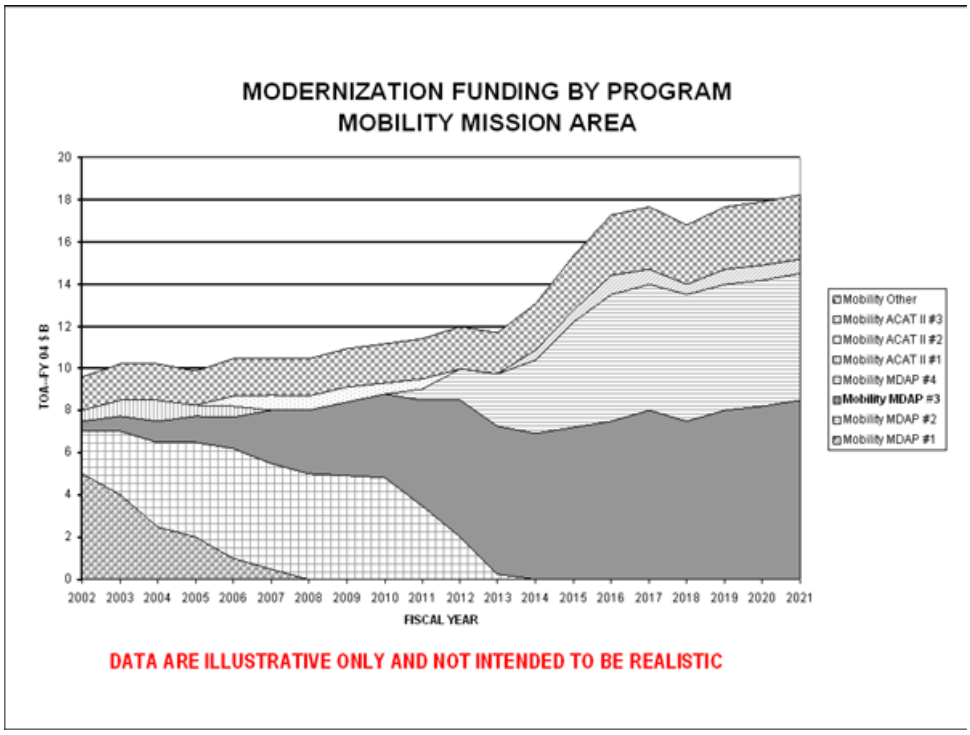

Figure 3.2.2.1. Sample Chart of Funding Streams by Program

The second step in this assessment is to portray DoD Component modernization funding stratified by mission areas, rather than by individual program. Figure 3.2.2.2 shows a notional example of this second step. The choice of mission areas will vary depending upon circumstances. Clearly, an analysis by an individual DoD Component would portray funding only for applicable mission areas. Also, for a DoD Component like the Army, where almost all of its modernization funding is in a single mission area (Land Forces), the mission area should be further divided into more specialized categories (such as digitization, helicopters, ground combat vehicles, etc.).

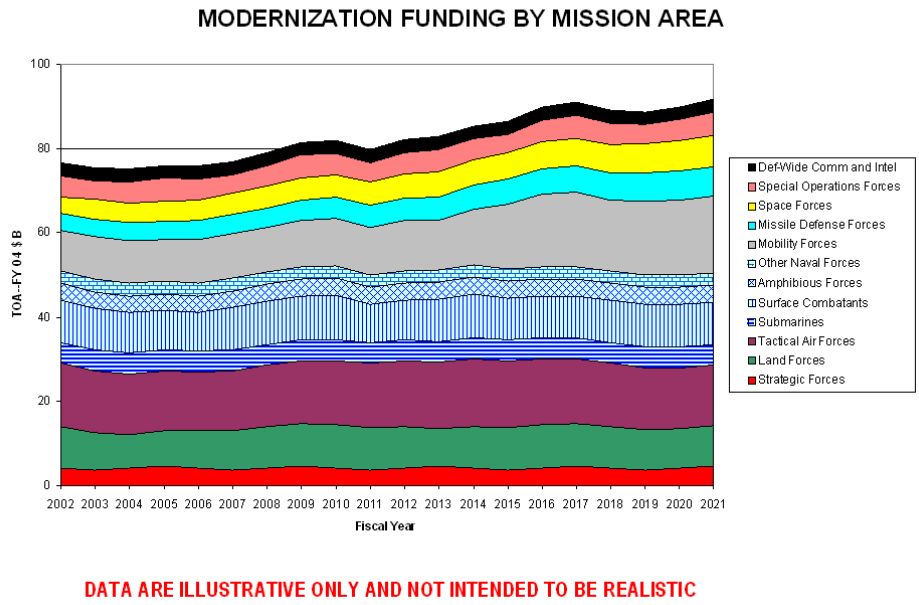

Figure 3.2.2.2. Sample Chart of Funding Streams by Mission Area

For this example, Figure 3.2.2.2 shows funding growth in three mission areas (space, missile defense, and mobility). What remains to be determined is whether this projected growth is realistically affordable relative to the DoD Component's most likely overall funding (top-line). The third step in this assessment is to portray annual modernization funding compared to the DoD Component actual or projected funding top-line, as shown in Figure 3.2.2.3. There are three distinct time periods considered in this figure. The first is a twelve-year historical period, the second is the six-year programming period, and the third is the twelve-year projection beyond the programming period. What this chart shows for this example is that the assumed mobility programs are projected to require a significantly higher share of DoD Component funding in the years beyond the programming period. In such a circumstance, the DoD Component would be expected to rationalize or justify this projected funding growth as realistic (by identifying offsets in modernization for other lower priority mission areas, or perhaps identifying savings in other accounts due to business process improvements or reforms).

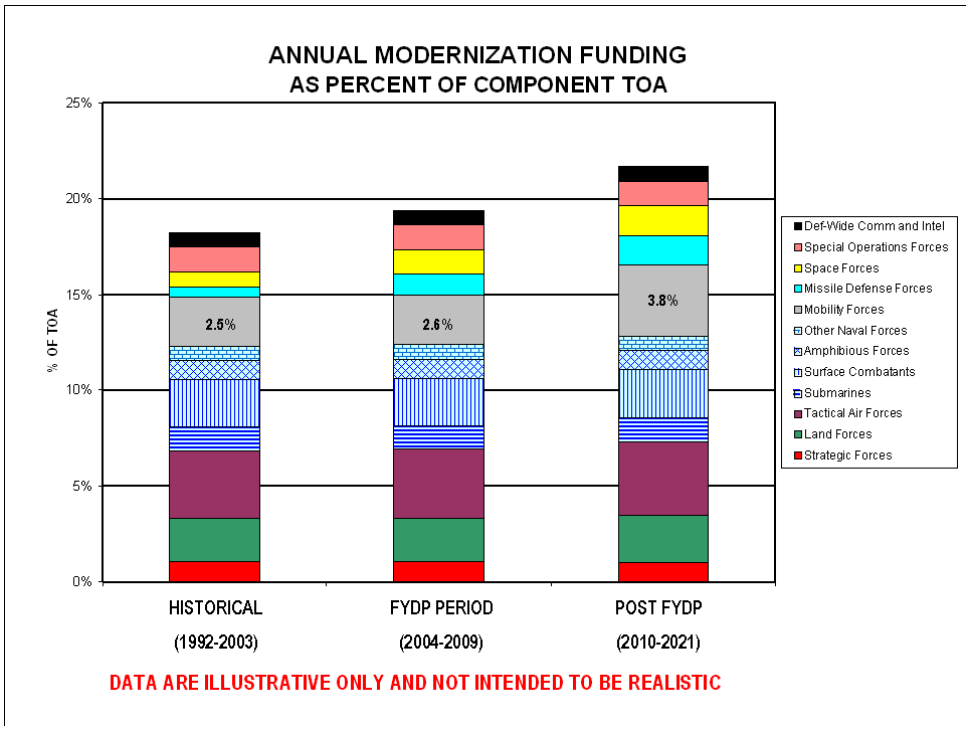

Figure 3.2.2.3. Sample Annual Modernization Funding

In preparing affordability assessments, one possible source of data for resource analysts to consider is the Future Years Defense Program (FYDP). The FYDP is an OSD resource database with future projections of resources (funding, manpower, and forces) over the programming period by program, where each program is associated with one (or a few) FYDP entities known as program elements. For acquisition programs, there are usually separate program elements for development and procurement. The FYDP also has comparable historical data going back several years. The FYDP data structure also provides options for assigning FYDP program elements to mission areas. One common approach for assigning resources to mission areas is the use of Defense Mission Categories. Further information on the FYDP, as well as Defense Mission Categories, can be found at the web site (accessible from .mil only) for the FYDP Structure Management System. Note: Access to this web site requires a ".mil" address. For projections beyond the FYDP programming period, many DoD Components (or their major commands) have long-range modernization roadmaps which can be incorporated in the assessment. In addition, annual funding projections beyond the FYDP for major defense acquisition programs can be obtained from the appropriate Selected Acquisition Reports.

The approach used in this example would need to be modified for a major automated information system, since most likely the mission areas associated with weapon systems would not apply. An alternative would be to portray AIS modernization funding by joint

warfighting capability area or business domain (such as logistics, accounting and finance, or human resources management, etc.)

3.2.3. Full Funding

It has been a long-standing DoD policy to seek full funding of acquisition programs, based on the most likely cost, in the budget year and out-year program years. Experience has shown that full funding is a necessary condition for program stability. DoD Directive 5000.1, affirms this full funding policy. Moreover, DoD Instruction 5000.2 requires full funding—defined as inclusion of the dollars and manpower needed for all current and future efforts to carry out the acquisition and support strategies—as part of the entrance criteria for the transition into system development and demonstration.

Full funding and program stability is especially important in joint and international acquisition programs. Underfunding or program instability on the part of one DoD Component can lead to unintended cost growth or instability for another DoD Component in a joint program, or even for another nation in an approved international cooperative program commitment. DoD Instruction 5000.2, Enclosure 9, imposes very strict approval requirements that must be met before DoD Components are permitted to terminate or make significant reduction to their share of approved international or joint programs. DoD Components contemplating termination of an international program should be aware of the termination provisions in the international agreement for that program. Current practice requires the nation terminating its participation in the program to pay substantial termination costs. Therefore, any DoD Component considering unilateral withdrawal from an international agreement must take into account the resultant costs that would be incurred.

Full funding is assessed by the Milestone Decision Authority at each decision point. As part of this assessment, the Milestone Decision Authority reviews the actual funding (in the most recent President's Budget submission or Future Years Defense Program position) in comparison to the (time-phased) program office cost estimate. In addition, the Milestone Decision Authority considers the funding recommendations made by the OSD Cost Analysis Improvement Group (for Acquisition Category ID programs) or the DoD Component cost analysis team (for Acquisition Category IC programs). If the Milestone Decision Authority concludes that the current funding does not support the acquisition program, then the acquisition decision memorandum may direct a funding adjustment and/or program restructure in the next FYDP update.

3.2.4. Cost As an Independent Variable

As stated in DoD Directive 5000.1, all participants in the acquisition system are expected to recognize the reality of fiscal constraints, and to view cost as an independent variable. Cost in this context refers to Lifecycle cost, which should be treated as equally important to performance and schedule in program decisions. To institutionalize this principle, program managers should consider developing a formal Cost As an Independent Variable (CAIV) plan as part of the acquisition strategy. This section describes one possible approach for developing such a plan.

The implementation steps in a CAIV plan will depend on the type of system and its current stage in the acquisition framework. In general, however, a CAIV plan would include the following elements:

Set Cost Goals. The CAIV plan would include cost goals for unit production cost and operating and support costs. The unit production cost goal typically would be established for a specified quantity of systems and a specified peak production rate. The O&S cost goal typically would be an annual cost per deployable unit (e.g., battalion or squadron) or individual system (e.g., ship or missile). The goals should be challenging but realistically achievable. The goals should be challenging but realistically achievable. The goals in the CAIV plan might be the same as the cost goals in the acquisition program baseline, or possibly might be more aggressive. Conceivably, the APB goals might be more conservative for programs with a greater degree of risk, to provide some margin for error.

Perform Trade-off Studies. Cost, schedule, and performance may be traded off within the "trade space" between thresholds and objectives documented in the capability needs document. The CAIV plan would show the timing, content, and approach for the specific trade studies to be performed. Over time, as the system design matures, the trade studies become more refined and specialized.

Establish Cost Performance Integrated Product Team. Although led by the program manager, the CAIV process requires collaboration with other acquisition and logistics organizations as well as the user. The CAIV plan would establish a Cost Performance Integrated Product Team, which most likely would receive considerable support from the system contractor. The Cost Performance IPT would monitor the CAIV implementation and oversee the trade studies.

Provide Incentives. The elements of the acquisition strategy should describe incentives to the contractor that directly support, or are at least complementary to, the CAIV plan. Such incentives might include award fees, sharing of cost savings, or other (positive or negative) incentives. Chapter 2 provides further discussion on contract incentives.

Establish Metrics. The CAIV plan should address how metrics will be established to track progress and achievement of unit production and O&S cost goals. The plan should identify how progress toward achieving the goals will be monitored and reported. The plan also should describe how cost estimates will be updated and refined over time, and compared to the original cost goals. The plan should identify specific organizational responsibilities, and identify related major events where progress toward achieving goals will be assessed.

As part of the Reduction of Total Ownership Costs (R-TOC) Program, the R-TOC working group has developed templates that could be used as guidelines in the development of CAIV implementation plans. The use of these templates is optional. The templates may be found at the DoD R-TOC web site.

3.3. Analysis of Alternatives

For a major defense acquisition program (Acquisition Category I), an Analysis of Alternatives (AoA) is required at major milestone decision points (DoD Instruction 5000.2). For a major automated information system program (Acquisition Category IA),

current law (Pub. L. 107-248, Section 8088, or successor provision) requires an AoA at Milestones A and B and at the full-rate production decision (or their equivalents) (DoD Instruction 5000.2).

AoAs are an important element of the defense acquisition process. An AoA is an analytical comparison of the operational effectiveness, suitability, and Life-Cycle cost of alternatives that satisfy established capability needs. Initially, the AoA process typically explores numerous conceptual solutions with the goal of identifying the most promising options, thereby guiding the Concept Refinement Phase (see section 3.3.3). Subsequently, at Milestone B (which usually represents the first major funding commitment to the acquisition program), the AoA is used to justify the rationale for formal initiation of the acquisition program. An AoA normally is not required at Milestone C unless significant changes to threats, costs, or technology have occurred, or the analysis is otherwise deemed necessary by the Milestone Decision Authority. For a joint program, the lead DoD Component normally is responsible for the preparation of a single comprehensive analysis.

The Office of the Director, Program Analysis and Evaluation (OD/PA&E), provides basic policies and guidance associated with the AoA process. For potential and designated Acquisition Category I and IA programs, OD/PA&E prepares the initial AoA guidance, reviews the AoA analysis plan, and reviews the final analysis products (briefing and report). After the review of the final products, OD/PA&E provides an independent assessment to the Milestone Decision Authority (see DoD Instruction 5000.2).

3.3.1. AoA Plan

The first major step leading to a successful AoA is the creation and coordination of a well-considered analysis plan. The plan should establish a roadmap of how the analysis will proceed, and who is responsible for doing what. A recommended outline for the AoA plan would resemble the following:

- Introduction
  - Background
  - Purpose
  - Scope
- Ground Rules
  - Scenarios
  - Threats
  - Environment
  - Constraints and Assumptions
- Alternatives
  - Description of Alternatives
  - Nonviable Alternatives

    - Operations Concepts
    - Support Concepts
- Determination of Effectiveness Measures
    - Mission Tasks
    - Measures of Effectiveness
    - Measures of Performance
- Effectiveness Analysis
    - Effectiveness Methodology
    - Models, Simulations, and Data
    - Effectiveness Sensitivity Analysis
- Cost Analysis
    - Lifecycle Cost Methodology
    - Models and Data
    - Cost Sensitivity and/or Risk Analysis
- Cost-Effectiveness Comparisons
    - Cost-Effectiveness Methodology
    - Displays or Presentation Formats
    - Criteria for Screening Alternatives
- Organization and Management
    - Study Team/Organization
    - AoA Review Process
    - Schedule

Of course, every AoA is unique, and the above outline may need to be tailored or streamlined to support a given situation.

The introduction to the AoA plan describes the developments that led to the AoA, including relevant analyses that preceded it. It should reference the applicable capability needs document(s) and other pertinent documents, such as any applicable AoA guidance. It also should identify in general terms the level of detail of the study, and the scope (breadth and depth) of the analysis necessary to support the specific milestone decision.

The ground rules described in the analysis plan include the scenarios and threats, as well as the assumed physical environment and any constraints or additional assumptions. The scenarios are typically derived from defense planning scenarios, augmented by more detailed intelligence products such as target information and enemy and friendly orders of battle. Environmental factors that impact operations (e.g., climate, weather, or terrain) are important as well. In addition, environment, safety, and occupational health factors

associated with the use of chemical and/or biological weapons may need to be considered as excursions to the baseline scenario(s).

The analysis plan also should document the range of alternatives to be addressed in the analysis. In many cases, there will be a minimum set of alternatives required by the initial analysis guidance. Additional direction during subsequent AoA reviews may insert yet other alternatives. Practically, the range of alternatives should be kept manageable. Selecting too few or too many are both possibilities, but experience has shown that selecting too many, exceeding the available resources of effectiveness and/or cost analysts, is the greater concern. The number of alternatives can be controlled by avoiding similar but slightly different alternatives and by early elimination of alternatives (due to factors such as unacceptable Lifecycle cost or inability to meet key performance parameters). In many studies, the first alternative (base case) is to retain one or more existing systems, representing a benchmark of current capabilities. An additional alternative based on major upgrades and/or service-life extensions to existing systems also may be considered. For each alternative, evaluating its effectiveness and estimating its Lifecycle cost requires a significant level of understanding of its operations and support concepts. The operations concept describes the details of the peacetime, contingency, and wartime employment of the alternative within projected military units or organizations. It also may be necessary to describe the planned basing and deployment concepts (contingency and wartime) for each alternative. The support concept describes the plans for system training, maintenance, and other logistics support.

The analysis plan should describe how the AoA will establish metrics associated with the military worth of each alternative. Military worth often is portrayed in AoAs as a hierarchy of mission tasks, measures of effectiveness, and measures of performance. Military worth is fundamentally the ability to perform mission tasks, which are derived from the identified capability needs. Mission tasks are usually expressed in terms of general tasks to be performed to correct the gaps in needed capabilities (e.g., hold targets at risk, or communicate in a jamming environment). Mission tasks should not be stated in solution-specific language. Measures of effectiveness are more refined and they provide the details that allow the proficiency of each alternative in performing the mission tasks to be quantified. Each mission task should have at least one measure of effectiveness supporting it, and each measure of effectiveness should support at least one mission task. A measure of performance typically is a quantitative measure of a system characteristic (e.g., range, weapon load-out, logistics footprint, etc.) chosen to enable calculation of one or more measures of effectiveness. Measures of performance are often linked to key performance parameters or other parameters contained in the approved capability needs document(s). They also may be linked to system contract specifications.

The analysis plan spells out the analytic approach to the effectiveness analysis, which is built upon the hierarchy of military worth, the assumed scenarios and threats, and the nature of the selected alternatives. The analytic approach describes the level of detail of the effectiveness analysis. In many AoAs involving combat operations, the levels of effectiveness analysis can be characterized by the numbers and types of alternative and threat elements being modeled. A typical classification would consist of four levels: (1) *system performance*, based on analyses of individual components of each alternative or threat system, (2) *engagement*, based on analyses of the interaction of a single alternative

and a single threat system, and possibly the interactions of a few alternative systems with a few threat systems, (3) *mission*, based on assessments of how well alternative systems perform military missions in the context of many-on-many engagements, and (4) *campaign*, based on how well alternative systems contribute to the overall military campaign, often in a joint context. For AoAs involving combat support operations, the characterization would need to be modified to the nature of the support. Nevertheless, most AoAs involve analyses at different levels of detail, where the outputs of the more specialized analysis are used as inputs to more aggregate analyses. At each level, establishing the effectiveness methodology often involves the identification of suitable models (simulation or otherwise), other analytic techniques, and data. This identification primarily should be based on the earlier selection of measures of effectiveness. The modeling effort should be focused on the computation of the specific measures of effectiveness established for the purpose of the particular study. Models are seldom good or bad per se; rather, models are either suitable or not suitable for a particular purpose. It also is important to address excursions and other sensitivity analyses in the overall effectiveness analysis. Typically, there are a few critical assumptions that often drive the results of the analysis, and it is important to understand and point out how variations in these assumptions affect the results. As one example, in many cases the assumed performance of a future system is based on engineering estimates that have not been tested or validated. In such cases, the effectiveness analysis should describe how sensitive the mission or campaign outcomes are to the assumed performance estimates.

The AoA plan also describes the approach to the Lifecycle cost analysis. The cost analysis normally is performed in parallel with the operational effectiveness analysis. It is equal in importance in the overall AoA process. It estimates the total Lifecycle cost of each alternative, and its results are later combined with the operational effectiveness analysis to portray cost-effectiveness comparisons. When the costs of the alternatives have significantly different time periods or distributions, appropriate discounting methods should be used to calculate the Lifecycle cost of each alternative. A recommended analytic approach for preparing a Lifecycle cost estimate is provided in section 3.7 of this chapter. What is important to emphasize is that the cost analysis is a major effort that demands the attention of experienced, professional cost analysts.

Typically, the last analytical section of the AoA plan deals with the planned approach for the cost-effectiveness comparisons of the study alternatives. In most AoAs, these comparisons involve alternatives that have both different effectiveness and cost, which leads to the question of how to judge when additional effectiveness is worth additional cost. Cost-effectiveness comparisons in theory would be simplified if the analysis structured the alternatives so that all the alternatives have equal effectiveness (the best alternative is the one with lowest cost) or equal cost (the best alternative is the one with greatest effectiveness). In actual practice, the ideal of equal effectiveness or equal cost alternatives is difficult or impossible to achieve due to the complexity of AoA issues. A common alternative for the comparison is a scatter plot of effectiveness versus cost. Figure 3.3.1.1. presents a notional example of such a plot.

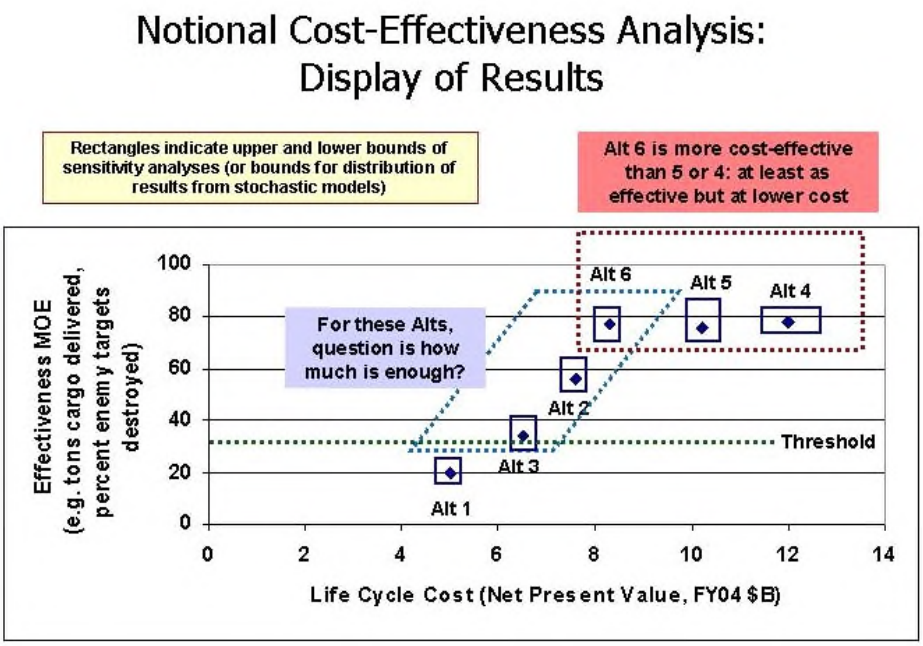

Figure 3.3.1.1. Sample Scatter Plot of Effectiveness versus Cost

Note that the notional sample display shown in Figure 3.3.1.1. does not make use of ratios (of effectiveness to cost) for comparing alternatives. Usually, ratios are regarded as potentially misleading because they mask important information. The advantage to the approach in the figure above is that it reduces the original set of alternatives to a small set of viable alternatives for decision makers to consider.

Finally, the AoA plan should address the AoA study organization and management. Often, the AoA is conducted by a working group (study team) led by a study director and staffed appropriately with a diverse mix of military, civilian, and contractor personnel. The program office may provide assistance or data to the AoA study team, but the responsibility for the AoA should not be assigned to the program manager, and the study team members should not reside in the program office. In some cases, the AoA may be assigned to a federally funded research and development center or similar organization. The AoA study team is usually organized along functional lines into panels, with a chair for each panel. Typical functional areas for the panels could be threats and scenarios, technology and alternatives (responsible for defining the alternatives), operations and support concepts (for each alternative), effectiveness analysis, and cost analysis. In most cases, the effectiveness panel occupies the central position and integrates the work of the other panels. The study plan also should describe the planned oversight and review process for the AoA. It is important to obtain guidance and direction from senior reviewers with a variety of perspectives (operational, technical, and cost) throughout the entire AoA process.

The analysis plan is fundamentally important because it defines what will be accomplished, and how and when it will be accomplished. However, the plan should be treated as a living document, and updated as needed throughout the AoA to reflect new information and changing study direction. New directions are inevitably part of the AoA process, and so the analysis should be structured so as to be flexible. Frequently, AoAs turn out to be more difficult than originally envisioned, and the collaborative analytical process associated with AoAs is inherently slow. There are often delays in obtaining proper input data, and there may be disagreements between the study participants concerning ground rules or alternatives that lead to an increase in excursions or cases to be considered. The need to scale back the planned analysis in order to maintain the study schedule is a common occurrence.

3.3.2. AoA Final Results

The final results of the AoA initially are presented as a series of briefings. The final AoA results are provided to OD/PA&E no later than 60 days prior to the milestone decision meeting (Defense Acquisition Board or Information Technology Acquisition Board review). Providing emerging results to OD/PA&E prior to the final briefing is wise to ensure that there are no unexpected problems or issues. The AoA final results should follow all of the important aspects of the study plan, and support the AoA findings with the presentation. In particular, all of the stated AoA conclusions and findings should follow logically from the supporting analysis.

Usually, in addition to a final briefing, the AoA process and results are documented in a written final report. The report serves as the principal supporting documentation for any decisions made as a result of the AoA. The report also may serve as a reference for future AoAs. The final report can follow the same format as the study plan, with the addition of these sections:

- Effectiveness Analysis
    - Effectiveness Results
- Cost Analysis
    - Lifecycle Cost Results
- Cost-Effectiveness Comparisons
    - Cost-Effectiveness Results
    - Assessment of Preferred Alternative(s)

By following the same format, much of the material from the (updated) study plan can be used in the final report.

3.3.3. Role of the AoA in Concept Refinement

The analysis of alternatives process is expected to play a key role in support of the Concept Refinement phase. After a program has an approved concept decision, the analysis of alternatives process is expected to contribute to the refinement of the initial concept and the identification of critical associated technologies, based on a balanced

assessment of technology maturity and risk, and cost, performance, and schedule considerations (as shown in Figure 3.3.3.1.).

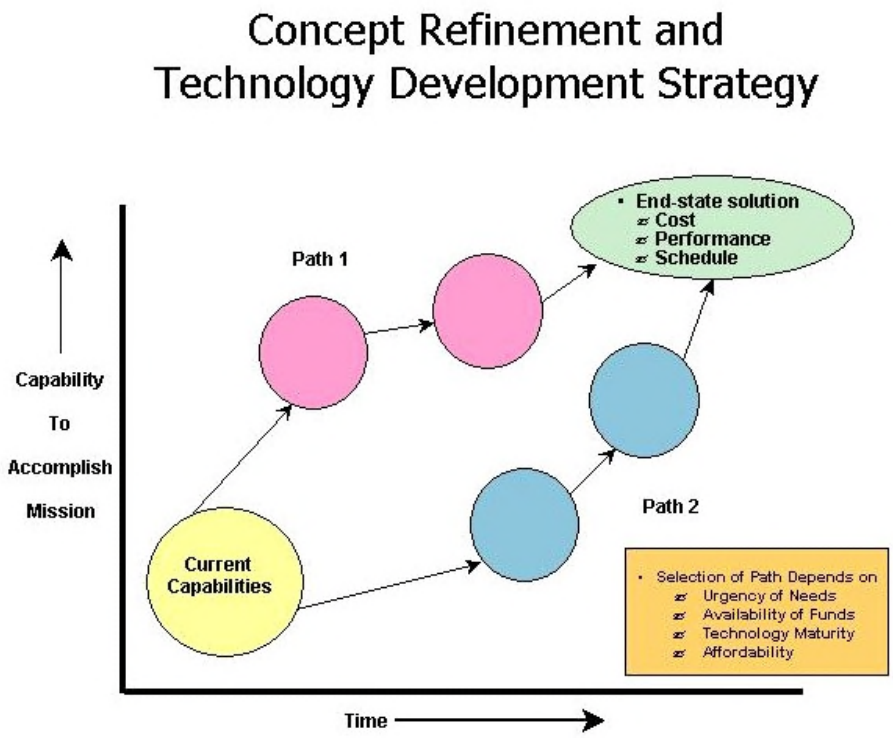

Figure 3.3.3.1. The Role of the AoA in Concept Refinement

The analysis plan required by DoD Instruction 5000.2 for the Concept Decision is satisfied by an AoA plan that addresses the issues unique to the program's Concept Refinement phase and Technology Development Strategy. The AoA plan should build upon the prior analyses conducted as part of the Joint Capabilities Integration and Development System (Joint Capabilities Integration and Development System). The Joint Capabilities Integration and Development System process is briefly described in section 1.3, and is fully described in CJCS Instruction 3170.01. The Joint Capabilities Integration and Development System analysis process that leads to an approved Initial Capabilities Document includes an assessment known as the Functional Solution Analysis (FSA). The Functional Solution Analysis identifies both materiel and non-materiel potential solutions that address the documented gaps in validated capability needs. The last step of the Functional Solution Analysis, known as the Analysis of Materiel Approaches (AMA), provides a preliminary assessment of candidate materiel approaches. The result of the AMA is a prioritized list of materiel approaches (or combination of approaches) that is documented as part of the Initial Capabilities Document. In this way, the Initial Capabilities Document can be used to establish boundary conditions for the scope of alternatives to be considered in the subsequent AoA. These constraints should be crafted

to provide a fair balance between focusing the AoA and ensuring that the AoA considers novel and imaginative alternatives.

3.3.4. AoA Considerations for Major Automated Information Systems

DoD Instruction 5000.2 requires an analysis of alternatives (AoA) for MAIS programs at major milestone decisions. Much of the discussion on AoAs provided earlier is more applicable to weapon systems, and should be modified somewhat for MAIS programs.

To satisfy the requirement for an AoA at Milestone A for MAIS programs, the Functional Solution Analysis completed according to the Joint Capabilities Integration and Development System process may meet the analytic intent of the AoA. In some cases, more detailed analyses among the most promising alternatives will be needed in an AoA, based on OD/PA&E's assessment of the Functional Solution Analysis. In either case, the analysis should include a discussion as to whether the proposed program (1) supports a core/priority mission or function performed by the DoD Component, (2) needs to be undertaken because no alternative private sector or governmental source can better support the function, and (3) supports improved work processes that have been simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial off-the-shelf technology. The analysis should be tied to benchmarking and business process reengineering studies (such as analyses of simplified or streamlined work processes, or outsourcing of non-core functions).

For all MAIS AoAs, one alternative should be the status quo alternative as used in the economic analysis, and one alternative should be associated with the proposed MAIS program. Other possible alternatives could be different system, network, and/or data architectures, or they might involve different options for the purchase and integration of commercial-off-the-shelf products, modifications, and upgrades of existing assets, or major in-house development.

Most likely, the effectiveness analysis in a MAIS AoA will not involve scenario-based analysis as is common for the weapon system AoAs. The effectiveness analysis for an MAIS program should be tied to the organizational missions, functions, and objectives that are directly supported by the implementation of the system being considered. The results of the AoA should provide insight into how well the various alternatives support the business outcomes that have been identified as the business goals or capabilities sought. In some cases, it may be possible to express the variation in effectiveness across the alternatives in monetary terms, and so effectiveness could be assessed as benefits in the economic analysis framework. In other cases, the effectiveness might be related to measurable improvements to business capabilities or better or more timely management information (leading to improved decision-making, which can be difficult or impossible to quantify). In these cases, a common approach is to portray effectiveness by the use of one or more surrogate metrics. Examples of such metrics might be report generation timeliness, customer satisfaction, or supplier responsiveness. In addition to management information, the effectiveness analysis also may need to consider information assurance or interoperability issues.

The cost analysis supporting the AoA should follow the economic analysis framework. The Life-cycle cost estimates of the alternatives considered in the AoA should be

consistent with and clearly linked to the alternatives addressed in the economic analysis. Both the effectiveness analysis and the cost analysis should address the risks and uncertainties for the alternatives, and present appropriate sensitivity analysis that describes how such uncertainties can influence the cost-effectiveness comparison of the alternatives.

The appropriate sponsor or domain owner should lead the development of the AoA for a MAIS program. Experience has shown that the MAIS programs for which the sponsor or domain owner engages with OD/PA&E early in the process are much more likely to be successful than those that select a preferred alternative before contacting OD/PA&E or before completing the AoA.

The Acquisition Community Connection web site has additional information on the AoA.

3.4. Cost Analysis Improvement Group

10 U.S.C. 2434 requires that an independent Lifecycle cost be prepared and provided to the milestone decision authority before the approval of a major defense acquisition program to proceed with either system development and demonstration, or production and deployment. In DoD Directive 5000.4, *Cost Analysis Improvement Group* (CAIG), the specific responsibility for fulfilling this requirement for such an independent cost estimate is assigned to the OSD Cost Analysis Improvement Group (for Acquisition Category ID programs, pre-Major Defense Acquisition Program projects approaching formal program initiation as a likely Acquisition Category ID program, and Acquisition Category IC programs when requested by the USD(AT&L)). DoD Instruction 5000.2 specifies that the CAIG independent cost estimate will be provided in support of major milestone decision points (Milestone B, Milestone C, or the full-rate production decision review). In addition, the DAB Milestone Decision Authority also may request the CAIG to prepare other independent cost estimates, or conduct other ad-hoc cost assessments, for programs subject to DAB review or oversight, at any time. Overall, the CAIG serves as the principal advisory body to the Milestone Decision Authority on all matters concerning an acquisition program's Lifecycle cost.

The CAIG also has other more general responsibilities in its charter, as described in DoD Directive 5000.4. Some of these major responsibilities are:

- Establish substantive guidance on the preparation of Lifecycle cost estimates subject to CAIG review (this guidance can be found in DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures*). This guidance includes standard definitions of cost terms in the management of DoD acquisition programs.
- Sponsor an annual DoD-wide Cost Research Symposium, where all DoD Components describe their plans for performing or sponsoring cost research. This symposium facilitates the exchange of cost research, and helps avoid duplication of effort between the DoD Components.
- Establish policy guidance on the Contractor Cost Data Reporting (CCDR) system, and monitor its implementation to ensure consistent and appropriate application throughout the DoD. The CCDR system is fully explained in DoD 5000.4-M-1,

Contractor Cost Data Reporting (CCDR) Manual. This manual can be found at the Defense Cost and Resource Center (DCARC) web site.

- Establish policy guidance on the Software Resources Data Reporting (SRDR) system, and monitor its implementation to ensure consistent and appropriate application throughout the Department of Defense. DoD Instruction 5000.2 requires SRDR reporting for major contracts and sub-contracts associated with major software elements within Acquisition Category I and Acquisition Category IA programs. The SRDR system is briefly described in section 3.4.2.3, and is fully explained in the draft SRDR Manual. This manual can be found at the Defense Cost and Resource Center (DCARC) web site.
- Establish policy guidance on the Visibility and Management of Operating and Support Costs (VAMOSC) Program, and monitor its implementation by each military department. In support of this program, each military department has developed and maintains a historical operating and support (O&S) cost data collection system. Guidance on the VAMSOC program is contained in DoD 5000.4-M, Chapter 4.

3.4.1. CAIG Milestone Reviews

For programs subject to CAIG review that are approaching major milestone decision points, the OSD CAIG conducts a comprehensive assessment of program Lifecycle cost. The assessment is based not only on the preparation of the CAIG independent cost estimate, but also on a review of the program manager's Lifecycle cost estimate (LCCE) and the DoD Component cost position, if applicable. This section provides a brief summary of the major events associated with an OSD CAIG review, and also provides additional clarifying discussion on the procedures for each event. A more comprehensive description of the CAIG review process is found in DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures*.

Table 3.4.1.1. provides a brief summary of the major events and timelines associated with an OSD CAIG review leading to a DAB milestone decision review:

Event	Date
• OSD CAIG Review Kick-off Meeting o Draft Cost Analysis Requirements Description (CARD) Delivered by DoD Component	180 days before OIPT meeting
• CAIG Briefs Preliminary Independent LCCE to Program Manager o Draft Documentation of Program Office Estimate/DoD Component Cost Position Delivered by DoD Component o Final CARD Delivered by DoD Component	45 days before OIPT meeting
• OSD CAIG Review Meeting o Program Manager briefs program defined in CARD and Component Cost Position	21 days before OIPT meeting

o CAIG Briefs Final Estimate of Independent LCCE to Program Manager	
• Final Documentation of Program Office Estimate/DoD Component Cost Position Delivered by DoD Component	10 days before OIPT meeting
• OSD CAIG Report Delivered to OIPT Members	3 days before OIPT meeting

Table 3.4.1.1. CAIG Major Events and Timelines Associated with a DAB Milestone Decision Review

The CAIG review process begins roughly six months before the planned DAB milestone review. At that time, the draft Cost Analysis Requirements Description (CARD) is provided to the CAIG for review. The CARD is used to describe formally the acquisition program for purposes of preparing both the program office cost estimate (and the Component cost position, if applicable) and the OSD CAIG independent cost estimate. The CAIG staff promptly evaluates the CARD for completeness and consistency with other program documents (such as capability needs documents). The expectation is that the CARD should be sufficiently comprehensive in program definition to support a Lifecycle cost estimate. Normally, the CAIG staff provides any necessary feedback to the DoD Component if any additional information or revisions are needed. If the CARD is found to be deficient to the point of unacceptability, the CAIG Chair will advise the Overarching Integrated Product Team (OIPT) leader that the planned milestone review should be postponed.

At roughly the same time that the draft CARD is submitted, the CAIG announces its upcoming review in a formal memo. The memo initiates a working-level kick-off meeting that is held with representatives from the program office cost estimating team, the CAIG independent cost estimate team, and other interested parties (typically DoD Component or OSD staff members). The purpose of the meeting is to discuss requirements and issues for the upcoming milestone review, the scope of the cost estimates, and ground rules and assumptions on which the estimates will be based. Much of the discussion will focus on material provided in the draft CARD. This ensures that both cost teams have a common understanding of the program to be costed. In addition, ground rules are established for CAIG interactions with the program office. The CAIG also coordinates any travel or visit requirements with appropriate DoD Component points of contact.

Per DoD Instruction 5000.2, the CAIG will brief the preliminary independent LCCE to the program manager (PM) 45 days before the OIPT meeting. In a similar timeframe, the program office should provide their estimate to the CAIG, and, if required, the DoD Component should provide the DoD Component Cost Position. The CAIG report eventually submitted to the Overarching Integrated Product Team and to the Defense Acquisition Board provides not only the OSD CAIG independent cost estimate, but also an evaluation of the program office cost estimate (and DoD Component cost position, if applicable). It is therefore important for the DoD components to submit well-documented

cost estimates that are ready for review. The specific standards for the cost documentation are described in DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures*. In general, the documentation should be sufficiently complete and well organized that a cost professional could replicate the estimate, given the documentation. Along with the draft documentation of the program office cost estimate, the DoD Component provides an updated (and final) CARD to the CAIG. The expectation is that at this point no further changes to program definition will be considered. At the same time that the documents are provided, the CAIG staff will provide feedback and identify any emerging cost issues to the program manager and DoD Component staff, in part based on the CAIG work to date on its independent cost estimate.

Per DoD Instruction 5000.2, the CAIG will brief the final independent estimate to the program manager 21 days before the OIPT meeting. At this time, the program office should provide their final estimate to the CAIG, and, if required, the DoD Component should provide the final DoD Component Cost Position. Other invited OSD and Joint Staff representatives may attend these reviews/exchanges. A typical presentation format for the CAIG review meeting would include:

- Program overview and status
- Program office acquisition cost estimate
    - Summary of results
    - Methodology for high-cost elements
- Rationale for DoD Component cost position, if any
- Comparison of (time-phased) program office cost estimate to current funding
- Operating and Support (O&S) cost estimate

In addition, at the CAIG meeting, the CAIG staff provides any further feedback to the program office and DoD Component staff. If appropriate, the CAIG will provide a presentation of the major areas of difference between its independent cost estimate and the program office cost estimate and/or DoD Component cost position.

The CAIG's final report is delivered to the OIPT leader at least three days before the OIPT meeting. Immediately thereafter, it is distributed to the OIPT members and also is available to the DoD Component staff. The expectation is that any issues had already emerged in prior discussions and that the final CAIG report should not contain any surprises. The report normally is two to three pages, and typically includes the following:

- Summary of program office cost estimate
- Summary of CAIG independent cost estimate
- Comparison or reconciliation of the two estimates
- Assessment of program risks
- Comparison of (time-phased) CAIG cost estimate to current program funding
    - Recommendations concerning program funding

3.4.2.. CAIG Reporting Requirements

3.4.2.1. Cost Analysis Requirements Description

A sound cost estimate is based on a well-defined program. For Acquisition Category I and Acquisition Category IA programs, the Cost Analysis Requirements Description (CARD) is used to formally describe the acquisition program (and the system itself) for purposes of preparing both the program office cost estimate (and the DoD Component cost position, if applicable) and the OSD CAIG independent cost estimate. DoD Instruction 5000.2, Enclosure 3 specifies that for major defense acquisition programs the CARD will be provided in support of major milestone decision points (Milestone B, Milestone C, or the full-rate production decision review). In addition, for major AIS programs, the CARD is prepared whenever an Economic Analysis is required. The CARD is prepared by the program office and approved by the DoD Component Program Executive Officer (PEO). For joint programs, the CARD includes the common program agreed to by all participating DoD Components as well as all unique program requirements of the participating DoD Components. DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures*, Chapter 1, provides further guidelines for the preparation of the CARD.

The CARD typically provides both narratives and tabular data, roughly following the following outline:

- System description and characteristics
  - System work breakdown structure
  - Detailed technical and physical description
  - Subsystem descriptions, as appropriate
  - Technology maturity levels of critical components
- System quality factors
  - Reliability/Maintainability/Availability
- PM's assessment of program risk and risk mitigation measures
- System operational concept
  - Organizational/unit structure
  - Basing and deployment description (peacetime, contingency, and wartime)
- System support concept
  - System logistics concept
  - Hardware maintenance and support concept
  - Software support concept
  - System training concept
- Time-phased system quantity requirements
- System manpower requirements
- System activity rates (OPTEMPO or similar information)

- System milestone schedule
- Acquisition plan or strategy

For each topic listed above, the CARD should provide information and data for the program to be costed. In addition, the CARD should include quantitative comparisons between the proposed system and a predecessor and/or reference system for the major topics, as much as possible. A reference system is a currently operational or pre-existing system with a mission similar to that of the proposed system. It is often the system being replaced or augmented by the new acquisition. For a program that is a major upgrade to an existing weapon platform, such as an avionics replacement for an operational aircraft, the new system would be the platform as equipped with the upgrade, and the reference system would be the platform as equipped prior to the upgrade. For major AIS programs, the CARD format described above may need to be tailored.

Naturally, the level of detail provided in the CARD will depend on the maturity of the program. Programs at Milestone B are less well-defined than programs at Milestone C or at full-rate production. In cases where there are gaps or uncertainties in the various program descriptions, these uncertainties should be acknowledged as such in the CARD. This applies to uncertainties in either general program concepts or specific program data. For uncertainties in program concepts, nominal assumptions should be specified for cost-estimating purposes. For example, if the future depot maintenance concept were not yet determined, it would be necessary for the CARD to provide nominal (but specific) assumptions about the maintenance concept. For uncertainties in numerical data, ranges that bound the likely values (such as low, most likely, and high estimates) should be included. In general, values that are “to be determined” (TBD) are not adequate for cost estimating. Dealing with program uncertainty in the CARD greatly facilitates subsequent sensitivity or quantitative risk analyses in the Lifecycle cost estimate.

For programs employing an evolutionary acquisition strategy, the CARD should be structured to reflect the specifics of the approach. For programs in incremental development, the entire acquisition program, including all increments, is included in the scope of the program to be approved at the program initiation milestone review. The entire program therefore typically is included in the CARD and in the subsequent program Lifecycle cost estimate. For programs in spiral development, the situation will vary somewhat depending on circumstances. Normally, the CARD should attempt to include as much of the program as can be described at the time of the decision review, and clearly document any exclusions for portions of the program that cannot be defined.

Clearly, much of the information needed for the CARD is often available in other program documents. The CARD should stand-alone as a readable document, but can make liberal use of appropriate references to the source documents to minimize redundancy and effort. In such cases, the CARD should briefly summarize the information pertinent to cost in the appropriate section of the CARD, and provide a reference to the source document. The source documents should be readily available to the program office and independent cost estimating teams, or alternatively can be provided as an appendix to the CARD. Many program offices provide controlled access to source documents through a web site (perhaps at a “dot” MIL web address or on the SIPRNET).

3.4.2.2. Contractor Cost Data Reporting (CCDR)

CCDR is the primary means within the Department of Defense to systematically collect data on the development and production costs incurred by contractors in performing DoD acquisition program contracts. Often, CCDR data from historical programs is used to make parametric cost estimates for future acquisition programs. CCDR reporting is required by DoD Instruction 5000.2, Enclosure 3, for major contracts and sub-contracts (regardless of contract type) associated with Acquisition Category ID and IC programs. Specific dollar thresholds for CCDR can be found in section 11.3.2.1 of this Guidebook. Detailed procedures and other implementation guidance are found in DoD 5000.4-M-1, *Contractor Cost Data Reporting (CCDR) Manual*. This manual (as well as downloadable report formats and definitions, specific report examples, and other related information) can be found at the Defense Cost and Resource Center (DCARC) web site. The DCARC is the OSD office responsible for administering the CCDR system. Access to CCDR data is provided by the DCARC to DoD government cost analysts who are registered users.

3.4.2.3. Software Resources Data Reporting

SRDR is a recent initiative. The SRDR is intended to improve the ability of the Department of Defense to estimate the costs of software intensive programs. SRDR reporting is required by DoD Instruction 5000.2, Enclosure 3, for major contracts and sub-contracts (regardless of contract type) associated with high-cost software elements within Acquisition Category I and Acquisition Category IA programs. Specific dollar thresholds for SRDR can be found in section 11.3.3. of this Guidebook. Data collected from applicable contracts include type and size of the software application(s), schedule, and labor resources needed for the software development. Further information is provided in the draft SRDR Manual, which can be found (along with downloadable report formats and definitions, specific report examples, and other related information) at the Defense Cost and Resource Center (DCARC) web site. The DCARC is the OSD office responsible for administering the SRDR system. Access to SRDR data is provided by the DCARC to DoD government cost analysts who are registered users.

3.5. Manpower Estimates

For Major Defense Acquisition Programs, 10 U.S.C. 2434 requires the Secretary of Defense to consider the estimate of the personnel required to operate, maintain, support, and provide system-related training, in advance of approval of the development, or production and deployment of the system. To satisfy this requirement, Table E3.T1, "Statutory Information Requirements," of DoD Instruction 5000.2, directs the development of a manpower estimate at Milestones B and C and at the Full-Rate Production decision review. Further guidance is provided in the USD(P&R) memorandum, "Interim Policy and Procedures for Strategic Manpower Planning and Development of Manpower estimates," dated December 10, 2003.

Manpower estimates serve as the authoritative source for out-year projections of active-duty and reserve end-strength, civilian full-time equivalents, and contractor support work-years. As such, references to manpower in other program documentation should be consistent with the manpower estimate once it is finalized. In particular, the manpower

estimates should be consistent with the manpower levels assumed in the final affordability assessment and the Cost Analysis Requirements Description.

Organizational responsibilities in preparing the manpower estimate vary by DoD Component. Normally, the manpower estimate is prepared by an analytic organization in the DoD Component manpower community, in consultation with the program manager. The manpower estimates are approved by the DoD Component manpower authority (for the military departments, normally the Assistant Secretary for Manpower and Reserve Affairs).

For Acquisition Category ID programs, a preliminary manpower estimate should be made available at least three to six months in advance of the Defense Acquisition Board (DAB) milestone review in order to support the development of cost estimates and affordability assessments. The final manpower estimate should be submitted to the Under Secretary of Defense (Personnel and Readiness) in sufficient time to support the Overarching Integrated Product Team (OIPT) review in preparation of the DAB meeting. Normally this would be three weeks prior to the OIPT review meeting. The USD(P&R) staff will review the final manpower estimate and provide comments to the OIPT.

The exact content of the manpower estimate is tailored to fit the particular program under review. A sample format for the manpower estimate is displayed in the table below. In addition, the estimate should identify if there are any resource shortfalls (i.e., discrepancies between manpower requirements and authorizations) in any fiscal year addressed by the estimate. Where appropriate, the manpower estimate should compare manpower levels for the new system with those required for similar legacy systems, if any. The manpower estimate also should include a narrative that describes the methods, factors, and assumptions used to estimate the manpower.

MANPOWER ESTIMATE
(Program Title)
SERVICE1

	FYxx2	FYxx+l	FYxx+2	FYxx+3	FYxx+4	… 3
OPERATE:4						
Military						
Officers						
Enlisted						
Civilian						
Contractor						
Sub-Total						
MAINTAIN:[4]						
Military						
Officers						
Enlisted						
Civilian						
Contractor						
Sub-Total						
SUPPORT: [4]						
Military						
Officers						
Enlisted						
Civilian						
Contractor						
Sub-Total						
TRAIN: [4]						
Military						
Officers						
Enlisted						
Civilian						
Contractor						
Sub-Total						
TOTAL:						

1 Provide separate estimates for Active and Reserve Components for each Service.

2 Report manpower by fiscal year (FY) starting with initial fielding and continuing through retirement and disposal of the system (to include environmental clean-up).

3 Until fielding is completed.

4 Provide estimates for manpower requirements and authorizations. Provide deltas between requirements and authorizations for each fiscal year.

3.6. Major Automated Information Systems Economic Analysis

3.6.1. Introduction

An automated information system (AIS) is an acquisition program that acquires information technology that is not embedded in a weapon system. AIS programs normally are involved with and directly related to information storage, processing, and display—requiring resources for hardware, software, data, telecommunications, etc. AIS programs that meet the specified dollar thresholds in DoD Instruction 5000.2, Enclosure 2, qualify as major automated information systems (MAISs). MAIS programs that are subject to review by the Office of the Secretary of Defense (OSD)—through the Information Technology Acquisition Board (ITAB)—are designated Acquisition Category IAM. Other MAIS programs—delegated to the appropriate DoD Component acquisition executive—are designated Acquisition Category IAC. In some cases, an Acquisition Category IA program also meets the definition of a Major Defense Acquisition Program (MDAP). The USD(AT&L) and the ASD(NII)/DoD CIO decide who shall be the Milestone Decision Authority for such programs. Regardless of who is the Milestone Decision Authority, the statutory requirements that apply to MAIS programs and/or MDAPs (see DoD Instruction 5000.2, Enclosure 3) apply to such programs.

DoD Instruction 5000.2, Enclosure 3, requires that an Economic Analysis be performed in support of the Milestone A, Milestone B, and full-rate production decision reviews. The purpose of the Economic Analysis is to determine the best AIS program acquisition alternative, by assessing the net costs and benefits of the proposed AIS program relative to the status quo. In general, the best alternative will be the one that meets validated capability needs at the lowest Life-cycle cost (measured in present value terms), and/or provides the most favorable return on investment.

Whenever an Economic Analysis is required, the DoD Component responsible for the program also may be required to provide a DoD Component Cost Analysis, which is an independent estimate of program Life-cycle costs. Normally, the Economic Analysis is prepared by the AIS program office, and the DoD Component Cost Analysis is prepared by an office or entity not associated with the program office or its immediate chain of command. The need for a Component Cost Analysis at Milestone A is evaluated for each program in tailoring the oversight process.

3.6.2. OD(PA&E) Review Procedures

For Acquisition Category IAM programs, both the Economic Analysis and the DoD Component Cost Analysis are subject to independent review and assessment by the Office of the Director, Program Analysis and Evaluation (OD(PA&E)) resident in OSD. The purpose of the OD(PA&E) assessment is to provide the milestone decision authority with an independent determination that (1) the estimates of Lifecycle costs and benefits are reasonable and traceable, (2) the return on investment calculation is valid, and (3) the cost estimates are built on realistic program and schedule assumptions.

3.6.2.1. Kick-Off Meeting

The review process normally begins with a kick-off meeting held with the OD(PA&E) staff, representatives from the AIS program office, the DoD Component Cost Analysis Team, and any DoD Component functional or headquarters sponsors. The purpose of the meeting is to reach a common understanding on the expectations for the upcoming activities and events leading to the Information Technology Acquisition Board milestone review. As a starting point, the DoD Component staff and/or sponsors' representatives should review the contents of the most recently approved capability needs documents, and explain any prior analysis (such as an analysis of materiel approaches) used to justify the need for a materiel solution (that will be met by the AIS program).

At the kick-off meeting, the DoD Component staff and/or sponsors' representatives also should be prepared to explain the planned approach for the upcoming Economic Analysis. To facilitate this dialogue, the AIS program office should prepare and provide a brief Economic Analysis development plan. The development plan should document the organizational responsibilities, analytic approach, ground rules and assumptions, and schedule for the economic analysis. The development plan should identify the specific alternatives that will be compared in the Economic Analysis. Normally, at least one alternative should be associated with the proposed AIS program, and one alternative should be associated with the status quo (no modernization investment). It may well be the case that the status quo alternative represents an unacceptable mission posture—it may cost too much to sustain, be unable to meet critical capability needs, or be unsupportable due to technological obsolescence. Nevertheless, the status quo concept, applied over the same time frame (Life-cycle) as the proposed AIS program, is used for comparative purposes in the Economic Analysis. The Economic Analysis development plan should document the DoD Component Cost Analysis approach and schedule as well.

As part of the Economic Analysis development plan, the program office should propose the cost element structure that will be used to organize and categorize cost estimates in the Economic Analysis. The cost element structure provides a hierarchal framework of defined cost elements that in total comprise the program Life-cycle cost. The cost element structure should include phase-out costs associated with the status quo (legacy or predecessor) system. These costs would be incurred in managing, preserving, and maintaining the operations of the status quo system as it runs parallel to the phasing in of the new system. The status quo phase-out cost elements are not used in the estimate of the status quo alternative. A sample of a generic cost element structure is available from the OD(PA&E) staff. OD(PA&E) can also provide advice on a consistent approach to net present value and return on investment computations.

3.6.2.2. Use of the CARD for AIS Programs

As soon as possible after the kick-off meeting, the draft Cost Analysis Requirements Description (CARD) is provided to the OD(PA&E) staff for review. The CARD is used to define and describe the AIS program for purposes of preparing both the Economic Analysis and the DoD Component Cost Analysis. For an AIS program, the CARD typically would address the following elements:

- Program description

- Program operational concept
- Program data management requirements
- Program quantity requirements
- Program manpower requirements
- Program fielding strategy
- Program milestone schedule
- Program acquisition plan or strategy

Procedures for the preparation of the CARD are described in DoD Instruction 5000.2. Additional guidelines on CARD preparation are found in DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures*, Chapter 1. However, these guidelines are for the most part oriented toward weapon systems, and may need to be tailored somewhat for automated information systems. The system description in the CARD should address both hardware and software elements. The CARD should describe each major hardware item (computers, servers, etc.), noting those items that are to be developed, and those items that are off-the-shelf. The CARD also should describe each software configuration item (including applications as well as support software) and identify those items that are to be developed. For software items to be developed, the CARD should provide (1) some type of sizing information (such as counts of source lines of code or function points) suitable for cost estimating, and (2) information about the programming language and environment. In addition, the CARD should describe any special (physical, information, or operations) system security requirements, if applicable.

Clearly, much of the information needed for the CARD is often available in other program documents. The CARD should stand-alone as a readable document, but can make liberal use of appropriate references to the source documents to minimize redundancy and effort. In such cases, the CARD should briefly summarize the information pertinent to the Economic Analysis in the appropriate section of the CARD, and provide a reference to the source document.

3.6.2.3. OD(PA&E) Assessment

To facilitate the OD(PA&E) review and assessment, the Economic Analysis and DoD Component Cost Analysis teams should provide written documentation early enough to permit a timely report to the Overarching Integrated Product Team and Information Technology Acquisition Board. Normally, the documentation is provided 30 to 60 days prior to the OIPT meeting. The documentation serves as an audit trail of source data, methods, and results. The documentation should be easy to read, complete and well organized Milestone Decision Authority; to allow any reviewer to understand the estimate fully. The documentation also serves as a valuable reference for future cost analysts, as the program moves from one acquisition milestone to the next.

After review of the documentation, the OD(PA&E) staff provides feedback to the program office and DoD Component staff. Subsequently, the OD(PA&E) staff prepares a written report containing the findings of their independent assessment to the milestone decision authority. Depending on the circumstances, the report may contain

recommended cost and benefits positions, and it may raise funding or schedule issues. The expectation is that any issues raised have already emerged in prior discussions and that the final OD(PA&E) report should not contain any surprises.

3.7. Principles for Lifecycle Cost Estimates

Section 3.4.1 of this Guidebook primarily focused on procedures associated with Life-cycle cost estimates for major defense acquisition programs—subject to review by the Cost Analysis Improvement Group (CAIG)—prepared in support of major milestone or other program reviews held by the Defense Acquisition Board. This section is more generally applicable, and describes a recommended analytic approach for planning, conducting, and documenting a Life-cycle cost estimate for a defense acquisition program (whether or not the estimate is subject to CAIG review).

The recommended analytic approach for preparing a Life-cycle cost estimate is shown in Figure 3.7.1:

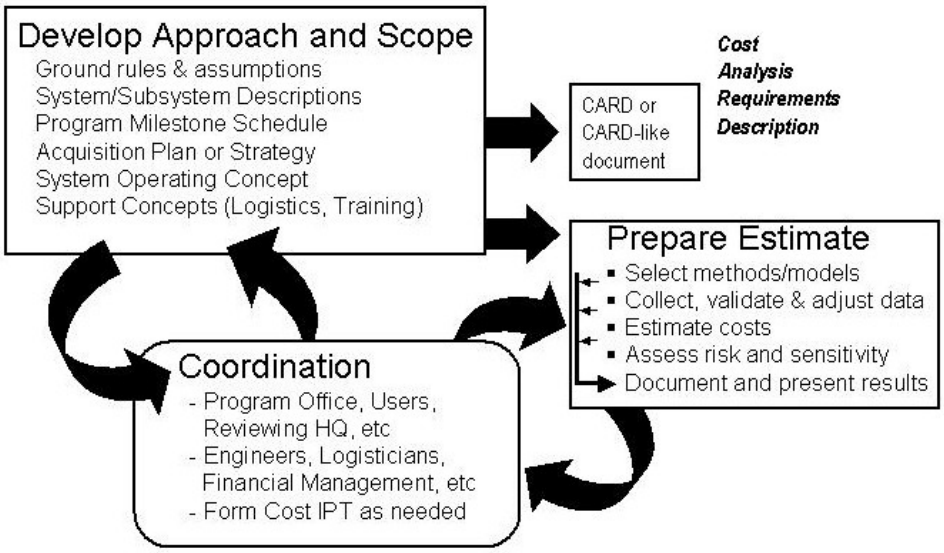

Figure 3.7.1. A Recommended Analytic Approach for Lifecycle Cost Estimates

The next few sections describe this process. In addition, the Acquisition Community Connection website has additional information on cost analysis.

3.7.1. Develop Approach and Scope

The first step in preparing a credible cost estimate is to begin with the development of a sound analytic approach. During this planning phase, critical ground rules and assumptions are established, the scope of the estimate is determined, and the program to be costed is carefully defined and documented. The program definition includes not only a technical and physical description of the system (and perhaps major subsystems), but

also a description of the system's program schedule, acquisition strategy, and operating and support concepts. In some cases, it is necessary to state explicitly the costs to be included, and the costs to be excluded. For example, when systems have complex interfaces with other systems or programs (that are outside the scope of the system being costed), the interfaces should be carefully defined.

For programs that will be reviewed by the OSD CAIG, the program office is required to define its program in a comprehensive formal written document known as a Cost Analysis Requirements Description, or CARD. The format for this document is briefly summarized in section 3.4.2.1 of this Guidebook, and is completely described in DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures.* For programs preparing a cost estimate not subject to OSD CAIG review, the CARD format, with appropriate tailoring, nevertheless provides a useful and flexible framework for developing a written program description suitable for a Life-cycle cost estimate. Much of the necessary information to prepare a written program description can be extracted and synthesized from common program source documents and contract specifications. The written program description should stand-alone as a readable document, but can make liberal use of suitable references to the source documents to minimize redundancy and effort.

Part of the system definition typically includes the program work breakdown structure. The program Work Breakdown Structure (WBS) is a hierarchy of product-oriented elements (hardware, software, data, and services) that collectively comprise the system to be developed or produced. The program WBS relates the elements of work to each other and to the end product. The program WBS is extended to a contract WBS that defines the logical relationship between the elements of the program and corresponding elements of the contract work statement. The WBS provides the framework for program and technical planning, cost estimating, resource allocation, performance measurement, technical assessment, and status reporting. In particular, the contract WBS provides the reporting structure used in contract management reports (such as cost performance reports or reports in the Contractor Cost Data Reporting system). Further information can be found in MIL-HDBK-881 (Work Breakdown Structure), which is available at the Defense Cost and Resource Center web site.

Another step in developing the analytic approach to the cost estimate is establishing the cost element structure that will be used as the format for the operating and support (O&S) cost estimate. The cost element structure describes and defines the specific elements to be included in the O&S cost estimate in a disciplined hierarchy. Using a formal cost element structure (prepared and coordinated in advance of the actual estimating) identifies all of the costs to be considered, and organizes the estimate results. The cost element structure is used to organize an O&S cost estimate similar to the way that a work breakdown structure is used to organize a development or production cost estimate. A standard cost element structure used by the OSD CAIG can be found in DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures.* Although each DoD component (military department or defense agency) may have its own preferred cost element structure, it is expected that each DoD Component will have a cross-walk or mapping structure so that any presentation to the CAIG can be made using the standard structure in DoD 5000.4-M.

It also is important that the analytic approach to the cost estimate be documented and reviewed by all potentially interested parties, before the actual work on preparing the cost

estimate begins. This helps ensure that there are no false starts or misunderstandings later in the process. Normally, cost estimates are sponsored by a system program office and are prepared by a multi-disciplinary team with functional skills in financial management, logistics, engineering, and other talents. The team also should include participants or reviewers from major affected organizations, such as the system's operating command, product support center, maintenance depot, training center or command, and so forth. Typically, the analytic approach to the cost estimate has a written study plan that includes a master schedule (of specific tasks, responsible parties, and due dates). For sufficiently complex efforts, the estimating team may be organized as a formal Integrated Product Team (IPT). For independent cost estimates, the team may be smaller and less formal, but the basic principle—complete coordination of the analytic approach with all interested parties—still applies.

3.7.2. Prepare the Estimate

The remainder of this section describes the typical steps in preparing a Lifecycle cost estimate. The discussion summarizes the steps entailed in selecting estimating techniques or models, collecting data, estimating costs, and conducting sensitivity or risk analysis.

In addition, the importance of good documentation of the estimate is explained.

Throughout the preparation of the estimate, coordination with all interested parties remains important. Frequent in-progress reviews or meetings are usually a good practice.

3.7.3. Select Methods and/or Models

A number of techniques may be employed to estimate the costs of a weapon system. The suitability of a specific approach will depend to a large degree on the maturity of the program and the level of detail of the available data. Most cost estimates are accomplished using a combination of the following estimating techniques:

- **Parametric.** The parametric technique uses regression or other statistical methods to develop Cost Estimating Relationships (CERs). A CER is an equation used to estimate a given cost element using an established relationship with one or more independent variables. The relationship may be mathematically simple (e.g. a simple ratio) or it may involve a complex equation (often derived from regression analysis of historical systems or subsystems). CERs should be current, applicable to the system or subsystem in question, and appropriate for the range of data being considered.
- **Analogy.** An analogy is a technique used to estimate a cost based on historical data for an analogous system or subsystem. In this technique, a currently fielded system, similar in design and operation to the proposed system, is used as a basis for the analogy. The cost of the proposed system is then estimated by adjusting the historical cost of the current system to account for differences (between the proposed and current systems). Such adjustments can be made through the use of factors (sometimes called scaling parameters) that represent differences in size, performance, technology, and/or complexity. Adjustment factors based on quantitative data are usually preferable to adjustment factors based on judgments from subject-matter experts.

- **Engineering Estimate.** With this technique, the system being costed is broken down into lower-level components (such as parts or assemblies), each of which is costed separately for direct labor, direct material, and other costs. Engineering estimates for direct labor hours may be based on analyses of engineering drawings and contractor or industry-wide standards. Engineering estimates for direct material may be based on discrete raw material and purchase part requirements. The remaining elements of cost (such as quality control or various overhead charges) may be factored from the direct labor and material costs. The various discrete cost estimates are aggregated by simple algebraic equations (hence the common name "bottoms-up" estimate). The use of engineering estimates requires extensive knowledge of a system's (and its components') characteristics, and lots of detailed data.
- **Actual Costs.** With this technique, actual cost experience or trends (from prototypes, engineering development models, and/or early production items) are used to project estimates of future costs for the same system. These projections may be made at various levels of detail, depending on the availability of data. Cost estimates that support a full-rate production milestone decision should be based on actual cost data to the greatest extent possible. A common mistake is to use contract prices as a substitute for actual cost experience. Contract prices should not be used to project future costs unless it is known that the contract prices are associated with profitable ventures, and that it is reasonable to assume that similar price experience will be obtained for subsequent contracts.

In many instances, it is a common practice to employ more than one cost estimating method, so that a second method can serve as a cross-check to the preferred method. Analogy estimates are often used as cross-checks, even for mature systems.

3.7.4. Collect, Validate, and Adjust Data

There are many possible sources of data that can be used in cost estimates. Regardless of the source, the validation of the data (relative to the purpose of its intended use) always remains the responsibility of the cost analyst. In some cases, the data will need to be adjusted or normalized. For example, in analogy estimates, the reference system cost should be adjusted to account for any differences—in system characteristics (technical, physical, complexity, or hardware cost) or operating environment—between the reference system and the proposed system being costed.

Actual cost experience on past and current acquisition programs often forms the basis of estimates of future systems. The Contractor Cost Data Reporting (CCDR) system is the primary means within the Department of Defense to systematically collect data on the development and production costs incurred by contractors in performing DoD acquisition program contracts.

CCDR reports can provide for each contract a display of incurred costs to date and estimated incurred costs at completion by elements of the work breakdown structure, with nonrecurring costs and recurring costs separately identified. In addition, CCDR reports can display incurred costs to date and estimated incurred costs at completion by functional category (manufacturing, engineering, etc.). Each functional category is

broken out by direct labor hours and major cost element (direct labor, direct material, and overhead). The CCDR manual (which provides report formats and definitions, specific report examples, and other related information) can be found at the Defense Cost and Resource Center (DCARC) web site. The DCARC is the OSD office responsible for administering the CCDR system.

For currently fielded major systems, historical O&S cost data for the most part is available from the Visibility and Management of Operating and Support Costs (VAMOSC) data system managed by each DoD Component. The data can be displayed in several different formats, including the CAIG standard cost element structure described previously. Data can be obtained for entire systems, or at lower levels of detail. VAMOSC provides not only cost data, but related non-cost data (such as OPTEMPO or maintenance man-hours) as well. This type of data is useful for analogy estimates (between proposed systems and appropriate predecessor or reference systems) and for "bottoms-up" engineering estimates (for fielded systems or components, possibly adjusted for projected reliability and maintainability growth). VAMOSC data should always be carefully examined before use in a cost estimate. The data should be displayed over a period of a few years (not just a single year), and stratified by different sources (such as major command or base). This should be done so that abnormal outliers in the data can be identified, investigated, and resolved as necessary.

3.7.4.1. Estimate Costs

With the completion of the steps described earlier in this chapter, the actual computations of the cost estimate can begin. It is important to assess critically the outputs from the estimating methods and models, drawing conclusions about reasonableness and validity. Peer review is often helpful at this point. For complex cost estimates, with many elements provided from different sources, considerable effort and care are needed to deconflict and synthesize the various elements.

3.7.4.2. Assess Risk and Sensitivity

For any system, estimates of future Lifecycle costs are subject to varying degrees of uncertainty. The overall uncertainty is not only due to uncertainty in cost estimating methods, but also due to uncertainties in program or system definition or in technical performance. Although these uncertainties cannot be eliminated, it is useful to identify associated risk issues and to attempt to quantify the degree of uncertainty as much as possible. This bounding of the cost estimate may be attempted through sensitivity analyses or through a formal risk analysis.

Sensitivity analysis attempts to demonstrate how the cost estimate would change if one or more assumptions change. Typically, for the high-cost elements, the analyst identifies the relevant cost-drivers, and then examines how costs vary with changes in the cost-driver values. For example, a sensitivity analysis might examine how maintenance manning varies with different assumptions about system reliability and maintainability values, or how system manufacturing labor and material costs vary with system weight growth. In good sensitivity analyses, the cost-drivers are not changed by arbitrary plus/minus percentages, but rather by a careful assessment of the underlying risks.

Sensitivity analysis is useful for identifying critical estimating assumptions, but has limited utility in providing a comprehensive sense of overall uncertainty.

In contrast, quantitative risk analysis can provide a broad overall assessment of variability in the cost estimate. In risk analysis, selected factors (technical, programmatic and cost) are described by probability distributions. Where estimates are based on cost models derived from historical data, the effects of cost estimation error may be included in the range of considerations included in the cost risk assessment. Risk analysis assesses the aggregate variability in the overall estimate due to the variability in each input probability distribution, typically through Monte-Carlo simulations. It is then possible to derive an estimated empirical probability distribution for the overall Lifecycle cost estimate. This allows the analyst to describe the nature and degree of variability in the estimate.

3.7.4.3. Document and Present Results

A complete cost estimate should be formally documented. The documentation serves as an audit trail of source data, methods, and results. The documentation should be easy to read, complete and well organized-to allow any reviewer to understand the estimate fully. The documentation also serves as a valuable reference for future cost analysts, as the program moves from one acquisition milestone to the next.

The documentation should address all aspects of the cost estimate: all ground rules and assumptions; the description of the system and its operating and support concepts; the selection of cost estimating methods; data sources; the actual estimate computations; and the results of any sensitivity or risk analyses. The documentation for the ground rules and assumptions, and the system description, should be written as an updated (final) version of the CARD or CARD-like document described earlier. The documentation for the portion of the cost estimate dealing with data, methods, and results often is published separately from the CARD or CARD-like document, but if that is the case, the two documents should be completely consistent.

CHAPTER 4

Systems Engineering

4.0. Overview

DoD policy and guidance recognize the importance of and introduce the application of a systems engineering approach in achieving an integrated, balanced system solution. DoD Directive 5000.1 requires:

> ***Systems Engineering.*** *Acquisition programs shall be managed through the application of a systems engineering approach that optimizes total system performance and minimizes total ownership costs. A modular open-systems approach shall be employed, where feasible.*

DoD Instruction 5000.2 emphasizes the use of systems engineering per the following extract:

> *Effective sustainment of weapon systems begins with the design and development of reliable and maintainable systems through the continuous application of a robust systems engineering methodology.*

Finally, the recent USD(AT&L) memorandum establishes systems engineering policy and mandates a Systems Engineering Plan for all programs. This memorandum will be included in the next revision to DoD Instruction 5000.2. An extract from the memorandum follows:

> *Systems Engineering (SE). All programs responding to a capabilities or requirements document, regardless of acquisition category, shall apply a robust SE approach that balances total system performance and total ownership costs within the family-of-systems, systems-of-systems context. Programs shall develop a Systems Engineering Plan (SEP) for milestone Decision Authority (Milestone Decision Authority) approval in conjunction with each Milestone review, and integrated with the Acquisition Strategy. This plan shall describe the program's overall technical approach, including processes, resources, metrics, and applicable performance incentives. It shall also detail the timing, conduct, and success criteria of technical reviews.*

4.0.1. Purpose

The purpose of this chapter is to facilitate compliance with the above mandatory systems engineering direction. This chapter describes systems engineering processes and the fundamentals of their application to DoD acquisition. It addresses the system design issues that a program manager must face to achieve the desired balanced system solution. In its entirety, this chapter thereby provides guidance and describes expectations for completing the Systems Engineering Plan.

4.0.2. Contents

This Chapter begins with Section 4.1, Systems Engineering in DoD Acquisition. This section defines systems engineering and its relationship to acquisition. It also provides perspective on the use of systems engineering processes to translate user-defined capabilities into actionable engineering specifications and on the role of the program manager in integrated system design activities.

Section 4.2, Systems Engineering Processes: How Systems Engineering is Implemented, discusses systems engineering processes and activities. The section groups systems engineering processes into technical management processes and technical process categories. This section contains a discussion of the use and tailoring of process models and standards, as well as what to expect of the contractor's systems engineering process.

Section 4.3, Systems Engineering in the System Life Cycle, provides an integrated technical framework for systems engineering processes throughout the acquisition phases of a system's life cycle, distinguishing the particular systems engineering inputs and outputs of each acquisition phase.

Section 4.4, Systems Engineering Decisions: Important Design Considerations, discusses the many design considerations that should be taken into account throughout the systems engineering processes. This includes an introduction to open systems design; interoperability; software; commercial off-the-shelf items; manufacturing capability; quality; reliability, availability and maintainability; supportability; human systems integration; environment, safety and occupational health; survivability; corrosion prevention and control; disposal and demilitarization; information assurance; insensitive munitions; anti-tamper provisions; system security; and accessibility.

Section 4.5, Systems Engineering Execution: Key Systems Engineering Tools and Techniques, includes the important technical, cost, and schedule oversight methods and techniques used in the technical management and technical processes. This section also discusses general knowledge management tools.

Section 4.6, Systems Engineering Resources, provides links to many systems engineering resources that already exist across the government, industry, and academia. Links to resources will be incorporated throughout the text of this chapter, as appropriate. As a compilation of available resources, this section includes standards and models, handbooks and guides, as well as any additional references deemed appropriate.

4.1. Systems Engineering in DoD Acquisition

Systems engineering is the overarching process that a program team applies to transition from a stated capability need to an operationally effective and suitable system. Systems engineering encompasses the application of systems engineering processes across the acquisition life cycle (adapted to each and every phase) and is intended to be the integrating mechanism for balanced solutions addressing capability needs, design considerations and constraints, as well as limitations imposed by technology, budget, and schedule. The systems engineering processes are applied early in concept definition, and then continuously throughout the total life cycle.

Balanced system solutions are best achieved by applying established systems engineering processes to the planning, development, and implementation of a system or system-of-systems acquisition in an Integrated Product and Process Development framework.

4.1.1. Systems Engineering

Systems engineering is an interdisciplinary approach or a structured, disciplined, and documented technical effort to simultaneously design and develop systems products and processes to satisfy the needs of the customer. Systems engineering transforms needed operational capabilities into an integrated system design through concurrent consideration of *all* Lifecycle needs. As systems become larger and more complex, the design, development, and production of a system or system-of-systems require the integration of numerous activities and processes. Systems engineering is the approach to coordinate and integrate all acquisition Lifecycle activities. Systems engineering integrates diverse technical management processes to achieve an integrated systems design. Although numerous definitions exist, this chapter adopts the following formal definition, adapted from EIA/IS 632, *Processes for Engineering a System*:

> *Systems engineering is an interdisciplinary approach encompassing the entire technical effort to evolve and verify an integrated and total Lifecycle balanced set of system, people, and process solutions that satisfy customer needs. Systems engineering is the integrating mechanism across the technical efforts related to the development, manufacturing, verification, deployment, operations, support, disposal of, and user training for systems and their life cycle processes. System engineering develops technical information to support the program management decision-making process. For example, systems engineers manage and control the definition and management of the system configuration and the translation of the system definition into work breakdown structures.*

Systems engineering provides a systematic set of processes to help coordinate and integrate activities throughout the life cycle of the system. Systems engineering offers a technical framework to enable sound decision making relative to trade studies among system performance, risk, cost, and schedule. The successful implementation of proven, disciplined systems engineering processes results in a total system solution that is--

- Robust to changing technical, production, and operating environments;
- Adaptive to the needs of the user; and
- Balanced among the multiple requirements, design considerations, design constraints, and program budgets.

Systems engineering is a broad topic. Before this Guidebook goes into the full technical detail of implementing systems engineering, we will introduce the various participant's responsibilities in systems engineering, discuss the "total systems approach" and "total life cycle systems management" required by DoD Directive 5000.1, relate systems engineering to the IPPD process, and recommended systems engineering leadership practices.

4.1.2. Participants in Systems Engineering

The program manager should implement a robust systems engineering approach to translate operational needs and capabilities into operationally suitable increments of a system. Systems engineering permeates design, production, test and evaluation, and system support. Systems engineering principles should influence the balance among the performance, cost, and schedule parameters and associated risks of the system. Program managers exercise leadership, decision-making, and oversight throughout the system life cycle. Implementing a systems engineering approach adds discipline to the process and provides the program manager with the information necessary to make valid trade-off decisions throughout a program's life cycle.

Systems engineering is typically implemented through multi-disciplined teams of subject matter experts (often formally chartered as an Integrated Product Team (IPT)). The systems engineering working-level IPT translates user-defined capabilities into operational system specifications consistent with cost, schedule, and performance constraints. (See the DoD Directive 5000.1 discussion of Knowledge Based Acquisition and additional information in this Guidebook.) While the program office usually has a Chief Engineer or Lead Systems Engineer in charge of implementing the systems engineering process, personnel from non-systems engineering organizations or from outside the program management structure may also perform activities related to systems engineering. Most program personnel should see themselves as participants in the systems engineering processes. Systems engineering-like activities include defining architectures and capabilities and conducting functional analyses per CJCS Instruction 3170.01. Warfighters, sponsors, and planners usually complete these activities before a program is initiated.

4.1.3. Total Life Cycle Systems Management (TLCSM) in Systems Engineering

It is fundamental to systems engineering to take a total life cycle, total systems approach to system planning, development, and implementation. Total life cycle systems management (TLCSM) is the planning for and management of the entire acquisition life cycle of a DoD system. Related to the *total systems approach*, DoD Directive 5000.1, E1.29, makes the program manager accountable for TLCSM:

> *E1.29. Total Systems Approach. The program manager shall be the single point of accountability for accomplishing program objectives for total Lifecycle systems management, including sustainment. The program manager shall apply human systems integration to optimize total system performance (hardware, software, and human), operational effectiveness, and suitability, survivability, safety, and affordability. PMs shall consider supportability, life cycle costs, performance, and schedule comparable in making program decisions. Planning for Operation and Support and the estimation of total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system life cycle.*

Because of TLCSM, the program manager should consider nearly all systems development decisions in context of the effect that decision will have on the long term operational effectiveness and logistics affordability of the system. TLCSM considerations should permeate the decision making of all acquisition functions and communities, during all acquisition phases. In fact, TLCSM factors should be considered by the participants in the Joint Capabilities Integration and Development System (Joint Capabilities Integration and Development System) even before a program manager is assigned; the Joint Capabilities Integration and Development System determination of performance capabilities should reflect TLCSM considerations. Later, TLCSM should frame the decision making for sustainment logistics.

TLCSM encompasses the following concepts:

- Single point of accountability;
- Evolutionary acquisition;
- Supportability and sustainment as key elements of performance;
- Performance-based strategies, including logistics;
- Increased reliability and reduced logistics footprint; and
- Continuing reviews of sustainment strategies.

In executing TLCSM responsibilities, program managers should apply systems engineering processes and practices known to reduce cost, schedule, and performance risks. This includes best public sector and commercial practices and technology solutions (see section 4.5.9.1 for links to best practice examples). The resulting system solution should be interoperable and should meet Joint Capabilities Integration and Development System and Joint Capabilities Integration and Development System-related (e.g., Condition Based Maintenance Plus or affordability) performance capabilities needs. The TLCSM business approach means that all major materiel alternative considerations and major acquisition functional decisions reflect an understanding of the effects and consequences of these decisions on Operations and Sustainment Phase (including disposal) system effectiveness and affordability.

The cost to implement a system change increases as a program moves further along the system life cycle. The greatest leverage exists in the early stages of development, when the program is most flexible. Early in the life cycle, thorough analyses of Lifecycle issues and cost/performance trade-off studies can reveal a balanced, Lifecycle design that prevents costly changes later in the system life cycle.

The program manager should apply a robust systems engineering methodology to achieve the optimal balance of performance and total ownership costs. Effective sustainment of weapons systems begins with the development of a balanced system solution. The key is to apply the systems engineering processes throughout the DoD 5000 Defense Acquisition Management Framework. Systems engineering should play a principal role in each acquisition phase. See Section 4.3 for a detailed description of these systems engineering activities by acquisition phase.

Consequently, systems engineering should applied at the initial stages of program formulation to provide the integrated technical basis for program strategies; acquisition plans; acquisition decisions; management of requirements, risk, and design trades; and integration of engineering, logistics, test, and cost estimation efforts among all stakeholders. Likewise, the Systems Engineering Plan (SEP) should be established early in the program definition stages and updated periodically as the program matures. The overall systems engineering strategy should be addressed in and integrated with all other program strategies. Systems engineering enables TLCSM, and provides the framework to aid decision making about trade-offs between system performance, cost, and schedule.

4.1.4. Systems Engineering and the New Acquisition Environment

Evolutionary acquisition strategies integrate advanced, mature technologies into producible systems that can be deployed to the user as quickly as possible. An evolutionary acquisition strategy matches available technology and resources to approved, time-phased, capability needs. Systems engineering processes provide the disciplined, integrated development and production environment that supplies increasing capability to a materiel solution. In spiral and incremental development, capability is developed and fielded in increments with each successive increment building upon earlier increments to achieve an overall capability. These approaches to evolutionary acquisition are particularly effective in quickly fielding an initial capability or increment of functionality while allowing continued efforts to incrementally attain the final, full, end-state capability. Robust systems engineering processes ensure that systems are designed to easily and affordably accommodate additive capabilities in subsequent increments. Examples of these processes include the modular, open systems approach.

There are various development and Lifecycle models to support systems engineering within an evolutionary acquisition strategy. They include the waterfall, spiral, and "Vee" models. All models provide an orderly approach to implementing and integrating the systems engineering processes during each acquisition phase. The spiral and Vee models rely heavily on prototyping, both physical and virtual, to get user feedback.

Evolutionary acquisition has increased the importance of traceability in program management. If a defense system has multiple increments, systems engineering can trace the evolution of the system. It can provide discipline to and documentation of the repeated trade-off analyses and decisions associated with the program. Due to the nature of evolutionary acquisition, design, development, deployment, and sustainment can each be occurring simultaneously for different system increments.

4.1.5. The Integrated Product and Process Development (IPPD) Framework and Systems Engineering

The Department of Defense defines IPPD as a management technique that uses multidisciplinary teams (Integrated Product Teams (IPTs)) to optimize design, manufacturing, and supportability processes. IPPD facilitates meeting cost and performance objectives from system concept out through production and field support. It is a broad, interdisciplinary approach that includes not only the engineers, technical specialists, and customers in the IPTs, but also business and financial analysts as well. (See also 10.3, 11.8, and the IPPD Handbook.)

Systems engineering is consistent with IPPD. It creates and verifies an integrated and Lifecycle-balanced set of system product and process solutions that satisfy stated customer needs. Systems engineering integrates the development of the system with the development of all system-related processes. The systems engineering process provides a common basis for and improves the communication between IPT members. All members of the development IPTs, who possess expertise in one or more disciplines in a system's life cycle, perform systems engineering; everyone involved in the system's development should be a "total systems-thinker." Each member of the team should apply the systems engineering process to their respective area of expertise.

4.1.6. Systems Engineering Leadership

As part of their overall role in technical oversight of assigned programs, acquisition components should maintain a systems engineering technical authority. A technical authority is the organization outside the program manager's chain of command with responsibility and accountability to establish, approve, and judge conformance of products and technical processes to technical requirements and policy during all phases of product development, acquisition, and sustainment. This technical authority should ensure proper systems engineering process application to programs and ensure proper training, qualification, and oversight of systems engineering personnel assigned to programs. As part of this overall responsibility for technical oversight, the technical authority should:

- Nominate a lead/chief systems engineer to the program manager at the initial stages of program formulation. The lead/chief systems engineer should be accountable to the program manager for meeting program objectives and accountable to the systems engineering technical authority for the proper application of systems engineering, and
- Nominate a chair for program technical reviews that is independent of the assigned program team and approved by the program manager. Technical reviews should include participation by program team personnel and independent (of the program team) subject matter experts as identified by the chair.

4.2. Systems Engineering Processes: How Systems Engineering is Implemented

This section discusses the use and tailoring of process models and standards, presents the program office systems engineering processes as management processes and technical processes, and describes common expectations of the Systems Engineering processes used by contractors.

4.2.1. Processes Overview

Overall, the flow of the systems engineering processes is iterative within any one phase of the acquisition process and is recursive at lower and lower levels of the system structure. Systems engineering processes are applied to allow an orderly progression from one level of development to the next more detailed level through the use of controlled baselines. These processes are used for the system, subsystems, and system components

as well as for the supporting or enabling systems used for the production, operation, training, support, and disposal of that system. During the course of technical management processes and activities, such as trade studies or risk management activities, specific requirements, interfaces, or design solutions may be identified as non-optimal and changed to increase system-wide performance, achieve cost savings, or meet scheduling deadlines. The value of these processes is not only the transition of requirements from design to system, but as an integrated framework within which the universe of requirements can be, as a collective whole, defined, analyzed, decomposed, traded, managed, allocated, designed, integrated, tested, fielded, and sustained.

4.2.2. Standards and Models

Many systems engineering process standards and models exist that describe best practice in accomplishing systems engineering. These models usually contain guidance for tailoring, which is best done in conjunction with a risk assessment on the program that leads the program manager to determine which specific processes and activities are vital to the program. Some examples of systems engineering process standards and models include the following:

- ISO/IEC 15288, *Systems Engineering-System Life Cycle Processes*
- ANSI/EIA 632, *Processes for Engineering a System*
- IEEE 1220, *Application and Management of the Systems Engineering Process*
- EIA 731, *Systems Engineering Capability Model*
- CMMI SWE/SE/IPPD/SS, *Capability Maturity Model-Integration for Software Engineering, Systems Engineering, Integrated Product and Process Development and Supplier Sourcing*

4.2.2.1. Primary Standards

Three primary systems engineering standards represent different levels of application:

- The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15288, *Systems Engineering-System Life Cycle Processes*, covers the life cycle of a man-made system from concept through retirement. "It provides the processes for acquiring and supplying system products and services that are configured from one or more of the following types of system components: hardware, software, and humans. In addition, the framework provides for the assessment and improvement of the life cycle." This standard is designed to be used by an organization, a project within an organization, or an acquirer and a supplier via an agreement.
- The Electronic Industry Alliance (EIA) 632, *Processes for Engineering a System,* defines the set of requirements for engineering a system. The processes in EIA 632 describe "what to do" with respect to the processes for engineering a system, which is the next level down from the ISO/IEC 15288 level of system life cycle processes.

- The Institute of Electrical and Electronic Engineers (IEEE) 1220 defines a systems engineering process. It gives the next level of detail below the process requirements described in EIA 632. The process is described more at the task or application level. IEEE 1220 does not worry about "who does what" as some of the other standards do with the "acquirer-supplier" concepts.

To actually accomplish systems engineering, an organization would most likely need all three standards or a hybrid model of their own.

4.2.2.2. Standardized Terminology

The many systems and software engineering process models and standards use different terms to describe the processes, activities, and tasks within the systems engineering and other Lifecycle processes. This chapter uses the following terminology to represent generic systems engineering processes. They are grouped in two categories: Technical Management Processes and Technical Processes:

Technical Management Processes

- Decision Analysis
- Technical Planning
- Technical Assessment
- Requirements Management
- Risk Management
- Configuration Management
- Technical Data Management
- Interface Management

Technical Processes

- Requirements Development
- Logical Analysis
- Design Solution
- Implementation
- Integration
- Verification
- Validation
- Transition

These generic processes are described briefly below and applied throughout the life-cycle phases. More detail with regard to systems engineering processes can be found in any of the above-mentioned standards or models. Since systems engineering cannot be conducted without good organization and project processes as well as sufficient infrastructure, these standards and models also may include processes and activities, such

as organizational training, that are beyond the technical ones that may be considered specific to systems engineering.

4.2.3. Technical Management Processes

The program manager uses technical management processes to *manage* the technical development of the system increments, including the supporting or enabling systems. Section 4.5 describes the key techniques and tools for technical management in detail.

4.2.3.1. Decision Analysis

Decision Analysis activities provide the basis for evaluating and selecting alternatives when decisions need to be made. Decision Analysis involves selecting the criteria for the decision and the methods to be used in conducting the analysis. For example, during system design, analysis must be conducted to help chose amongst alternatives to achieve a balanced, supportable, robust, and cost effective system design. These analyses include, but are not limited to, trade studies, models and simulation, supportability analysis, level of repair analysis, post fielding support analysis, repair versus discard, and cost analysis. These studies should be augmented with virtual and/or physical prototypes, where applicable, prior to making decisions on best alternative. Decision criteria will be influenced by such things as interoperability constraints; size; transportability requirements; maintenance concept; affordability; reliability, availability, and maintainability goals; and schedule.

4.2.3.2. Technical Planning

Technical Planning activities ensure that the systems engineering processes are applied properly throughout a system's life cycle. Technical planning, as opposed to program planning, addresses the scope of the technical effort required to develop the system. A mandated tool for this activity is the Systems Engineering Plan. Each of the technical processes requires technical planning. Technical planning for Implementation, Integration, Verification, Validation, and Transition processes and their accompanying systems can reveal constraints and interfaces that will result in derived technical requirements.

4.2.3.3. Technical Assessment

Technical Assessment activities measure technical progress and the effectiveness of plans and requirements. Activities within Technical Assessment include the activities associated with Technical Performance Measurement and the conduct of technical reviews. A structured review process should demonstrate and confirm completion of required accomplishments and exit criteria as defined in program and system planning. Technical reviews are discussed in detail in section 4.3. Technical assessment activities discover deficiencies or anomalies that often result in the application of corrective action.

4.2.3.4. Requirements Management

Requirements Management provides traceability back to user-defined capabilities as documented through the Joint Capabilities Integration and Development System. In evolutionary acquisition, the management of requirements definition and changes to

requirements takes on an added dimension of complexity. The program manager should institute Requirements Management to (1) maintain the traceability of all requirements from capabilities needs, (2) to document all changes to those requirements, and (3) to record the rationale for those changes. Emerging technologies and threats can influence the requirements in the current as well as future increments of the system.

4.2.3.5. Risk Management

Risk management in systems engineering examines the risks of deviating from the program plan. It examines all aspects of the program, from conception to disposal, early in the program and in relation to each other. Most risk management approaches have in common the practice of integrating design (performance) requirements with other Lifecycle issues such as manufacturing, operations, Environment, Safety, and Occupational Health considerations, and support.

The program manager establishes a risk management process, including planning, assessment (identification and analysis), handling, and monitoring, to be integrated and continuously applied throughout the program, including, but not limited to, the design process. The risk management effort addresses:

- Risk planning;
- Risk assessment;
- Risk handling and mitigation strategies; and
- Risk monitoring approaches.

Risk assessment includes identification and analysis of potential sources of risk to the program plan, including, but not limited to, cost, performance, and schedule risks based on such factors as:

- The technology being used and its related design;
- Manufacturing capabilities;
- Potential industry sources; and
- Test and support processes.

The overall risk management effort interfaces with technology transition planning, including the establishment of transition criteria for such technologies.

More specifically, technology transfer risk management is a systematic methodology to identify, evaluate, rank, and control inadvertent technology transfer. It is based on a three-dimensional model: the *probability* of occurrence, the *consequence* if realized, and *countermeasure cost* to mitigate the occurrence. This is a key element of a program manager's executive decision-making - maintaining awareness of technology alternatives and their potential sensitivity while making trade-off assessments to translate desired capabilities into actionable engineering specifications. To successfully manage the risk of technology transfer, the program manager should:

- Identify contract vehicles which involve the transfer of sensitive data and technology to partner suppliers;

- Evaluate the risks that unfavorable export of certain technologies could pose for the program; and

Develop alternatives to mitigate those risks (see also sections 4.4.17 and 8.4).

More information can be found in the DoD Risk Management Guide.

4.2.3.6. Configuration Management

Configuration Management (See DoD Directive 5000.1) is the application of sound business practices to establish and maintain consistency of a product's attributes with its requirements and product configuration information. It involves interaction among government and contractor program functions such as systems engineering, design engineering, logistics, contracting, and manufacturing in an Integrated Product Team environment. Configuration management includes system hardware, software, and documentation (data). A configuration management process guides the system products, processes, and related documentation, and facilitates the development of open systems. Configuration Management efforts result in a complete audit trail of decisions and design modifications. The elements of configuration management include:

- Configuration Management Planning and Management -- Provides total life cycle configuration management planning for the program/project and manages the implementation of that planning;
- Configuration Identification -- Establishes a structure for products and product configuration; selects, defines, documents, and baselines product attributes; and assigns unique identifiers to each product and product configuration information item;
- Configuration Change Control -- Ensures that changes to a configuration baseline are properly identified, recorded, evaluated, approved or disapproved, and incorporated and verified, as appropriate;
- Configuration Status Accounting -- Manages the capture and maintenance of product configuration information necessary to account for the configuration of a product throughout the product life cycle; and
- Configuration Verification and Audit -- Establishes that the performance and functional requirements defined in the product definition information have been achieved by the design and that the design has been accurately documented in the product definition information.

Some examples of configuration management process standards and best practices are:

- ANSI/EIA 649A, *Configuration Management*, on the GEIA website (Click on STANDARDS);
- ISO 10007, *Quality Management - Guidelines for Configuration Management*;
- EIA 836, *Configuration Management Data Exchange and Interoperability*, located on the GEIA website (Click on STANDARDS); and
- MIL-HDBK-61A, Military Handbook, *Configuration Management Guidance*.

4.2.3.7. Data Management

Data are defined as recorded information regardless of the form or method of recording. The term includes technical data, computer software documentation, management information, representation of facts, numbers, or datum of any nature that can be communicated, stored, and processed to form information required by a contract or agreement to be delivered, or accessed by, the Government. The term includes similar information generated directly by Government activities, as well. The data are used to gain insight and provide management and guidance to systems development programs.

For purposes of this chapter, "data" refers to the information necessary for or associated with product development and sustainment, including the data associated with system development; modeling and simulation used in development or test; test and evaluation; installation; parts; spares; repairs; usage data required for product sustainment; and source and/or supplier data. Data specifically not included would be data relating to tactical operations information; sensor or communications information; financial transactions; personnel data; transactional data; and other data of a purely business nature. Guidance for logistics data can be found in section 5.1.3.3.

Data Management plays an important role in the systems engineering process. In the program office, data management consists of the disciplined processes and systems used to plan for, acquire, access, manage, protect, and use data of a technical nature to support the total life cycle of the system. Under the Total Life Cycle Systems Management concept, the program manager is responsible for Data Management. The program manager should develop a plan for managing defense system data during each phase of the system life cycle and include it in the Systems Engineering Plan.

Data Management applies policies, systems, and procedures to identify and control data requirements; to responsively and economically acquire, access, and distribute data; and to analyze data use. Adherence to data management principles enables the sharing, integration, and management of data by government and industry, and ensures that data products (information) meet or exceed customer requirements. Recent government and industry initiatives in Data Management have changed the approach and scope of data management, and made it a stronger element in the systems engineering process.

Data Management has a leading role in capturing, organizing, and providing information for the following uses in the systems engineering process:

- Enabling collaboration and life cycle use of acquisition system product data;
- Capturing and organizing all systems engineering inputs, as well as current, intermediate, and final outputs;
- Providing data correlation and traceability among requirements, designs, solutions, decision, and rationale;
- Documenting engineering decisions, including procedures, methods, results, and analyses;
- Functioning as a reference and support tool for the systems engineering effort and process;

- Facilitating technology insertion for affordability improvements during re-procurement and post-production support; and
- Supporting configuration procedures, as needed.

Examples of Data Management process standards and guidance documents are listed below:

- S1000D International Specification for Technical Publications Utilizing a Common Source Database;
- Data Management Community of Practice (CoP), located on the Acquisition Community Connection on the DAU website;
- DoD 5010.12-M, *Procedures for the Acquisition and Management of Technical Data*, May 1993;
- DoD 5200.1-M *Acquisition System Protection Program*, March 1994;
- GEIA-859, *Consensus Standard for Data Management*, located on the GEIA website (Click on STANDARDS). (Note: This document is currently being published.);
- *Intellectual Property: Navigating Through Commercial Waters*, October 15, 2001,
- ISO 10303, *Standard for the Exchange of Product Model Data (STEP)*, website.

The program manager should develop a plan for managing defense system data during each phase of the system life cycle. Government inspection and acceptance is required for technical publications, product definition data elements, and other data that will be used by DoD Component personnel for the installation, operation, or maintenance of equipment or software. Establishing data exchange formats promotes data reuse, fosters competition, and helps to ensure that data can be used consistently throughout the system, family of systems, or system of systems.

4.2.3.7.1. Data Acquisition

Defense system data are acquired when needed to support the acquisition, operations, maintenance, or disposal of the system and to evaluate contractor performance. The applied systems engineering process requires *access* to data to facilitate decision making, but does not necessarily require *acquisition* of *all* data. The data management processes assist in decision-making. Data management processes reveal the proper data to be acquired or accessed. The decision to purchase data should be made when access to required data is not sufficient to provide for life-cycle planning and system maintenance. The cost of data delivery should be a primary consideration. Other considerations include the following:

- Data requirements for spare and repair parts;
- Technical data needed for ordering and purchasing items for contingencies; and
- Circumstances under which the data may evolve over time to more useful or updated data.

4.2.3.7.2. Data Protection

The program manager is responsible for protecting system data, whether the data are stored and managed by the government or by contractors. The DoD policy with regard to data protection, marking, and release can be found in DoD Directive 5230.24, DoD Directive 5230.25, and DoD 5400.7-R. Data containing information subject to restrictions are required to be protected in accordance with the appropriate guidance, contract, or agreement. Guidance on distribution statements, restrictive markings, and restrictions on use, release, or disclosure of data, can be found in the DFARS Part 252.227-7013 & 7014, and DoD Directive 5230.24. When digital data are used, the data should display applicable restriction markings, legends, and distribution statements clearly visible when the data are first opened or accessed. These safeguards not only assure government compliance with use of data, they also guarantee and safeguard contractor data that are delivered to the government, and extend responsibilities of data handling and use to parties who subsequently use the data.

All data deliverables should include distribution statements. Processes should be established to protect all data which contain critical technology information, as well as assure that limited distribution data, intellectual property data, or proprietary data are properly handled during systems engineering activities - whether the data are in hard copy or digital format.

4.2.3.7.3. Data Storage

The program manager also has responsibility for addressing long-term storage and retrieval of data and associated program information - planning for digitizing continued need information, as appropriate and cost-effective. Such long-term planning and incremental digitization, as required, will assure that applicable data is available, preserved, and migrated to successive formats for future planning and use.

4.2.3.8. Interface Management

The Interface Management process ensures interface definition and compliance among the elements that compose the system, as well as with other systems with which the system or system elements must interoperate. Interface management control measures ensure that all internal and external interface requirement changes are properly documented in accordance with the configuration management plan and communicated to all affected configuration items.

Many of the external interfaces are identified through the Joint Capabilities Integration and Development System process and its accompanying documents and architectures. As system interface control requirements are developed, they are documented and made available to the appropriate Integrated Product Team. Documented interface control requirements serve critical functions at all levels of the system. Some of these functions include the following: to facilitate competitive bids; to enable integration of system and sub-systems; to support system maintenance, future enhancement, and upgrades; and provide input data for continuous risk management efforts. Refinement of the interfaces is achieved through iteration. As more is learned about the system during the design phases, lower-level, verifiable requirements and interfaces are defined and refined.

Impacts to the original defined capabilities and interfaces, performance parameter thresholds and objectives, and the system are evaluated when defining and modifying interfaces.

4.2.4. Technical Processes

The program manger uses technical processes to design the system, subsystems, and components, including the supporting or enabling systems required to produce, support, operate, or dispose of a system. (The terminology used to indicate a subsystem is system element, component, or configuration item, depending on the systems engineering context and phase of acquisition under discussion.) Section 4.5 discusses some key techniques and tools for conducting the analyses required in technical processes.

4.2.4.1. Requirements Development

The Requirements Development process takes all inputs from relevant stakeholders and translates the inputs into technical requirements. DoD systems engineers primarily respond to the Joint Capabilities Integration and Development System (JCIDS) documents that identify capability gaps in need of a materiel solution. The program manager should work with the user to establish and refine operational needs, attributes, performance parameters, and constraints that flow from JCIDS-described capabilities, and then ensure that all relevant requirements are addressed (see Figure 4.4.1., System Operational Effectiveness Diagram). Together with the user, the program manager should translate "customer needs" into the following program and system requirements:

- Performance parameter objectives and thresholds;
- Affordability constraints;
- Scheduling constraints; and
- Technical constraints.

Since some of the requirements may become defined only through system decomposition at later stages of the program, iterative application of rigorous systems engineering is key.

Requirements Development encompasses the definition and refinement of system-, subsystem-, and lower-level functional and performance requirements and interfaces to facilitate the design of open systems. It allocates and balances interoperability requirements among systems that should interoperate successfully to satisfy all appropriate integrated architectures and CRDs under which the proposed system falls. An integral part of defining and refining requirements is to provide technical support to the market research required early in the program life cycle. Systems engineers within DoD face the same sorts of requirements definition tasks that their commercial counterparts encounter in addressing market research (and customer needs). These tasks involve analyzing if and how an existing product (commercial or non-developmental item) can meet user requirements. This analysis ensures that open systems principles are applied to the maximum extent possible to reduce both life-cycle costs and development cycle time.

Requirements Development complements Logical Analysis and Design Solution technical processes. These three processes are iterated at each level of the system

structure, and then applied recursively to lower levels of the physical architecture throughout development. The objective is to help ensure that the requirements derived from the customer-designated capabilities are feasible and effective, as well as updated, as more information is learned about the requirements and interfaces through analysis.

4.2.4.2. Logical Analysis

Logical Analysis is the process of obtaining sets of logical solutions to improve understanding of the defined requirements and the relationships among the requirements (e.g., functional, behavioral, temporal). Once the logical solution sets are formed, the engineers allocate performance parameters and constraints, and then define derived technical requirements to be used for the system design.

There are many ways to attain the logical solution sets. Traditionally, the Department of Defense has used functional analysis/allocation. However, other approaches, such as behavioral analysis, timeline analysis, object-oriented analysis, data-flow analysis, and structured analysis, may also apply.

The design approach resulting from Logical Analysis:

- Partitions a system into self-contained, cohesive, logical groupings of interchangeable and adaptable elements to enable ease of change, achieve technology transparency, and mitigate the risk of obsolescence; and
- Uses rigorous and disciplined definitions of interfaces and, where appropriate, defines the key interfaces within a system by widely supported standards (including interface standards, protocols, and data interchange language and standards) that are published and maintained by recognized standards organizations.

When using a functional approach, the output of this process is the functional architecture that puts all of the functions in order, thereby sequencing all of the system tasks that should occur. The functional architecture provides a functional "picture" of the system. It details the complete set of functions to be performed along with the relationships among the functions.

4.2.4.3. Design Solution

The Design Solution process translates the outputs of the Requirements Development and Logical Analysis processes into alternative design solutions and selects a final design solution. The alternative design solutions include:

- People, products, and process entities; and
- Related internal and external interfaces.

Not only does this process iterate with Requirements Development and Logical Analysis, it also integrates with the program decision processes to identify and select the best solution. If the process finds that specified objectives and thresholds are infeasible, ineffective, or result in an inefficient system, it may then be necessary to re-evaluate the defined performance parameters.

The output of this process is the design or physical architecture that forms the basis for design definition documentation such as specifications, baselines, and Work Breakdown Structures. Physical architectures should be sufficiently detailed to allow the following:

- Confirmation of upward and downward traceability of requirements;
- Confirmation of interoperability and open system performance requirements; and
- Demonstration of the appropriate products to satisfy the applicable acquisition phase exit criteria.

Confirmation of requirements traceability and the soundness of the selected physical architecture can be accomplished using a cost-effective combination of design analysis, design modeling, and simulation, as applicable.

4.2.4.4. Implementation

Implementation is the process that actually yields the lowest level system elements in the system hierarchy. The system element is made, bought, or reused. Making it involves the hardware fabrication processes of forming, removing, joining, and finishing; or the software processes of coding, etc. If implementation involves a production process, a manufacturing system is required to be developed using these same technical and technical management processes.

Depending on the technologies and systems chosen when a decision is made to produce a system element, the Implementation process imposes constraints on the Design Solution process. If the decision is made to purchase or reuse an existing system element, the Implementation process may involve some adaptation or adjustments to the system element. The Implementation process gets the system element ready for the processes of Integration, Verification, and Validation. It should include some testing of the implemented system element before the element passes to the Integration Process. Implementation may also involve packaging, handling, and storage, depending on where or when the system element needs to be integrated into a higher-level assembly. Developing the supporting documentation for the system element--such as the manuals for operations, maintenance, and/or installation--are also a part of the Implementation process.

4.2.4.5. Integration

Integration is the process of incorporating the lower-level system elements into a higher-level system element in the physical architecture. The plan or strategy for the Integration process, including the assembly sequence, may impose constraints on the design solution. An assembled system element, also developed with the technical and technical management processes, may include fixtures for hardware or compilers for software.

Integration also refers to the incorporation of the final system into its operational environment and defined external interfaces.

Interface Management plays an important role with Integration, and iteration between the two processes will occur.

4.2.4.6. Verification

The Verification Process confirms that the system element meets the design-to or build-to specifications. It answers the question "Did you build it right?" As such, it tests the system elements against their defined requirements ("build-to" specifications). The purpose of Verification is to:

- Conduct verification of the realized (implemented or integrated) system element (including interfaces) from the lowest level system element up to the total system to ensure that the realized product conforms to the build-to specifications;
- Generate evidence necessary to confirm that system elements at each level of the system hierarchy meet their build-to specifications; and

Verify the materials employed in system solutions can be used in a safe and environmentally compliant manner.

The nature of verification activities changes as designs progress from concept to detailed designs to physical products. Throughout the system's life cycle, however, design solutions at all levels of the physical architecture are verified through a cost-effective combination of analysis, examination, demonstration, and testing, all of which can be aided by modeling and simulation.

4.2.4.7. Validation

The Validation Process answers the question of "Did you build the right thing". As such, it tests the performance of systems within their intended operational environment, with anticipated operators and users. In the early stages of the system life cycle, validation may involve prototypes, simulations, or mock-ups of the system and a model or simulation of the system's intended operational environment.

4.2.4.8. Transition

Transition is the process applied to move the system element to the next level in the physical architecture or, for the end-item system, to the user. This process may include installation at the operator or user site.

4.2.5. The Contractor's Systems Engineering Process

Contractor selection should depend on demonstrated process capability and organizational maturity in their systems engineering processes, as well as on demonstrated domain expertise and past performance commensurate with the needs of the program. Organizations use different standards and models and their accompanying assessment methods to establish the initial capability of their systems engineering processes and then to improve those processes. Some of the different standards and models for systems engineering were discussed in section 4.2.2. The remainder of this section covers some of the things a program manager needs to know when a contractor uses these systems engineering standards or models and their accompanying methods for appraisals and assessments.

4.2.5.1. The Use of Standards versus Capability and Maturity Models

The major distinction between standards and capability and maturity models lies in their purpose. Standards provide recommended processes to apply within an organization, describe expected tasks and outcomes, and describe how the processes and tasks integrate to provide required inputs and outputs. Standards are meant to provide an organization with a set of processes that, if done by qualified persons using appropriate tools and methods, will provide a capability to do effective and efficient engineering of systems. Capability and maturity models, on the other hand, are for process improvement. Capability and maturity models are used to assess, from an organizational perspective, how well the standard processes are being performed. Both capability and maturity models and standard processes are useful to an organization, but the role for each should be kept in perspective. The solicitation effort should seek descriptions of potential offerors' models and standards.

In general, the program manager should ensure that the contractor has established a process or processes to conduct systems engineering, that the contractor maintains these processes, and that throughout the organization, work adheres to these processes. Selecting an offeror with a weak systems engineering process will likely result in problems such as poor understanding of requirements and design constraints and how these are managed, little or no system design evolution documentation, poor configuration control, and inadequate manufacturing quality control.

4.2.5.2. Capability Reviews

Capability reviews such as manufacturing capability and software capability reviews are a useful tool available during source selections to assess the offerors' capability in selected critical process areas. Capability reviews may be the appropriate means for evaluating program-specific critical processes such as systems engineering, software development, configuration management, etc. The reviews would be useful to supplement process past performance data to ascertain the risks in selecting a given offeror and to assist in establishing the level of government oversight needed to manage the process-associated risks if that offeror is awarded the contract. The trade-off in determining whether or not to do a capability review would be the criticality of the process versus the time and resources to do the review versus the availability, adequacy, and currency of an offeror's process past performance data.

4.2.5.3. Capability Appraisals

In all cases, the program manager retains the right (and is encouraged) to independently evaluate the process capabilities of the selected team prior to or immediately after contract award in order to have a better understanding of potential risks associated with the development team's process capabilities. Once the developer is selected, the program manager can conduct an evaluation to support the up-front risk assessment of the developer's capability to deliver.

Periodic appraisals are encouraged as part of contract process monitoring activities. The selection of assessment or appraisal method would be dependent upon the needs of the particular project, the level of risk associated with the project, and any areas of concern the program manager may have. The program manager should understand that: 1) appraisal and assessment results are another tool (like past performance) to gauge the

likelihood that the contractor will succeed and perform to the requirements of the contract; 2) assessments are most valuable when they apply across the full program team, and not just one segment of the organization; and 3) domain experience is at least as important as process maturity level when evaluating the program team's capability.

4.2.6. System of Systems Engineering

System of systems engineering deals with planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems into a system of systems capability greater than the sum of the capabilities of the constituent parts. It is a top-down, comprehensive, collaborative, multidisciplinary, iterative, and concurrent technical management process for identifying system of systems capabilities; allocating such capabilities to a set of interdependent systems; and coordinating and integrating all the necessary development, production, sustainment, and other activities throughout the life cycle of a system of systems. The overall objective for developing a system of systems is to satisfy capabilities that can only be met with a mix of multiple, autonomous, and interacting systems. The mix of constituent systems may include existing, partially developed, and yet-to-be-designed independent systems. Systems of systems should be treated and managed as a system in their own right, and should therefore be subject to the same systems engineering processes and best practices as applied to individual systems.

The engineering of a system of systems differs from the engineering of a single system. The consideration of system of systems engineering should include the following factors or attributes:

- Larger scope and greater complexity of integration efforts;
- Collaborative and dynamic engineering;
- Engineering under the condition of uncertainty;
- Emphasis on design optimization;
- Continuing architectural reconfiguration;
- Simultaneous modeling and simulation of emergent system of systems behavior; and
- Rigorous interface design and management.

System of Systems Engineering Implications for Single System Developers. Systems should not be developed as stand-alone systems, but as parts of larger meta-systems delivering unique and encompassing capabilities. Program managers should be aware of the distinguishing system of systems engineering attributes that might apply to their system and the possible impact on their system architecture. Program managers should use the following list of questions to address system of systems concerns, capitalize on system of systems capability pay-offs, and effectively meet the design and development requirements of current and future system of systems:

1. Will joint warfighting capabilities improve if the Department incorporates my system into the portfolio of existing and planned systems of systems?

2. What additional capabilities and behavior could my system deliver within the context of existing and planned systems of systems?
3. Which are the most valuable capabilities that other systems can provide to my system if it becomes a part of existing or planned systems of systems?
4. To which systems of systems can my system contribute the most value?
5. Are there system of systems capabilities, behavior, and requirements that the system must address to become part of the existing or planned system of systems?
6. Am I designing my system so that it can be easily integrated with other systems?
7. Does my system have an adaptable and open architecture to enable future reconfiguration and integration into a system of systems?
8. Have the system of systems interface requirements been adequately defined and documented in the specification of my system?
9. Has my program developed and documented interface control requirements for external functional and physical interfaces?
10. Has my program identified and established conformance testing or certification mechanisms to assure that standards used by external interfaces conform to the prescribed interface specifications?
11. Has my program verified the external functional interface specifications to ensure that the functional and performance requirements for such interfaces are satisfied?
12. Does my system fully comply with external interface requirements identified through the Joint Capabilities Integration and Development System process and its accompanying documents and architectures (including the Global Information Grid architecture)?
13. Have I established rigorous interface design and management based on conformance and verification of standards at upper layers as well as at the application, transport, network, physical, media, and data link communication layers?

A Contrasting Note about Engineering a Family of Systems. A family of systems is not considered to be a system per se. A family of systems does not create capability beyond the additive sum of the individual capabilities of its member systems. A family of systems is basically a grouping of systems having some common characteristic(s). For example, each system in a family of systems may belong to a domain or product lines (e.g., a family of missiles or aircraft). A family of systems lacks the synergy of a system of systems. The family of systems does not acquire qualitatively new properties as a result of the grouping. In fact, the member systems may not be connected into a whole.

4.3. Systems Engineering Activities in the System Life Cycle

DoD Instruction 5000.2 establishes the framework for acquisition programs. These programs are structured in phases, each separated by milestone decisions. In each phase of a system's life cycle, from concept to disposal, there are important systems engineering actions, which if properly performed, will assist the program manager in managing the program.

The purpose of this section is to acquaint program managers with the variety of acquisition documents that have systems engineering implications, either as sources of system parameters (e.g., the Initial Capabilities Document and Capability Development Document) or as the recipients of systems engineering analyses outputs (e.g., Acquisition Strategy, Analysis of Alternatives, etc.). This section shows how the systems engineering processes of Section 4.2 can be applied and tailored to each acquisition phase:

- Each phase builds upon the previous phase to further define the system technical solution;
- Systems engineering processes are iterated at each system element level; and
- Technical reviews serve to confirm outputs of the acquisition phases and major technical efforts within the acquisition phases.

As the by-phase discussions illustrate, there are a number of technical reviews appropriate to each acquisition phase that are conducted at all appropriate levels within a program. The purpose of these reviews is to provide the program manager with an integrated technical assessment of program technical risk and readiness to proceed to the next technical phase of the effort. Results of these reviews should be used to update the Systems Engineering Plan. Technical reviews should:

- Be event driven (vice schedule driven); conducted when the system under development satisfies review entry criteria as documented in the Systems Engineering Plan; and conducted, at a minimum, at the transition from one acquisition phase to the next and at major transition points of technical effort.
- Have their processes and requirements addressed in and required by contractual documents.

DoD Instruction 5000.2, Enclosure 3, presents the statutory, regulatory, and contract reporting information and milestone requirements for acquisition programs. These requirements are significant, and in some cases, the lead-time for preparation may exceed one year. The information and/or decisions that a program office reports in these documents often rely on analyses begun in pre-acquisition. During pre-acquisition, systems engineering processes translate user-defined capabilities into system specifications. As explained earlier, these systems engineering processes are both iterative and recursive. Likewise, some of the information requirements are iterative by milestone. Throughout this section, the terminology used to indicate a subsystem is either a system element, component, or configuration item, depending on the systems engineering context and phase of acquisition under discussion.

The OSD Systems Engineering Assessment Methodology Defense Acquisition Program Support is the framework that OSD System Assessment Teams apply to Major Defense Acquisition Programs approaching a Defense Acquisition Board review. Defense Acquisition Program Support, however, is also a powerful self-assessment tool for the

program manager to use for technical evaluation of a program's systems engineering process details and health.

4.3.1. Concept Refinement Phase

Pre-acquisition, beginning with Concept Refinement, presents the first substantial opportunity to influence systems design by balancing technology opportunities, schedule constraints, funding availability, performance parameters, and operational requirements. Desired user capabilities, expressed in terms of Key Performance Parameters and other parameters, should be defined in terms of:

- Quantifiable metrics (e.g., speed, lethality) of performance to meet mission requirements affordably; and
- The full range of operational requirements (reliability, effectiveness, logistics footprint, supportability criteria, etc.) to sustain the mission over the long term.

Early and effective employment of systems engineering, applied in accordance with a well-structured Systems Engineering Plan, and monitored with meaningful systems engineering technical reviews, will reduce program risk and identify potential management issues in a timely manner.

The Concept Refinement phase refines the initial concept and generates a Technology Development Strategy. Entrance into this phase requires a successful Concept Decision and an approved Initial Capabilities Document. The Acquisition Decision Memorandum documents Milestone Decision Authority approval of the Analysis of Alternatives Plan and establishes a date for the Milestone A review. The Initial Capabilities Document and Analysis of Alternatives Plan guide Concept Refinement Phase activities.

4.3.1.1. Purpose of Systems Engineering in Concept Refinement

The Joint Capabilities Integration and Development System analysis process provides a structured methodology to identify capability gaps and needs, and suggest various approaches to provide needed capabilities within a specified functional or operational area. These analyses should incorporate innovative practices, including best commercial practices, collaborative environments, modeling and simulation, and electronic business solutions.

After the process identifies a materiel need, and an affirmative Concept Decision initiates Concept Refinement, the Analysis of Alternatives should use systems engineering processes to examine the alternatives and identify a preferred solution. Systems engineering processes can provide a technical evaluation of the operational effectiveness and estimated costs of the alternative system concepts that may provide a materiel solution to a needed mission capability. The analysis should assess the advantages and disadvantages of the alternatives under consideration, and include sensitivity analyses to possible changes in key assumptions or variables.

During Concept Refinement, systems engineering processes should also support development of the Technology Development Strategy for the preferred solution.

4.3.1.2. Inputs to the Systems Engineering Processes in Concept Refinement

The following information sources provide important inputs to the systems engineering processes supporting Concept Refinement:

- Initial Capabilities Document;
- Analysis of Alternatives Plan;
- Exit Criteria for the Concept Refinement Phase; and
- Alternative Maintenance and Logistics Concepts.

4.3.1.3. Key Systems Engineering Activities During Concept Refinement

Figure 4.3.1.3.1. identifies the systems engineering-related steps during the Concept Refinement Phase. All decomposition activities listed below should be done concurrently for hardware and software. Paragraphs below contain additional detail on each step.

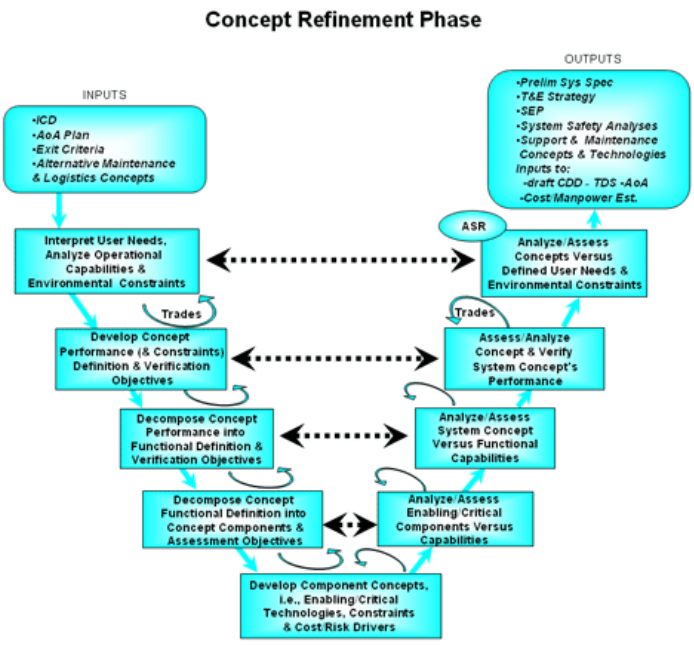

Figure4.3.1.3.1. Systems engineering-related steps during Concept Refinement

4.3.1.3.1. Interpret User Needs; Analyze Operational Capabilities and Environmental Constraints

This step includes the aggregation of all inputs available at this stage of the program (Initial Capabilities Document, Analysis of Alternatives Plan, exit criteria for the phase,

concept alternatives for overall tactical system, as well as associated support system, training system, and interoperable systems). Further analysis and definition is typically required to ascertain all of the related constraints to be applied to the effort:

- Environmental--systems threats, usage environment, support environment, doctrine, operational concepts;
- Resource--industrial base; notional available development, operation, and support budgets; required date for system fielding;
- Technology--applicable technology base to be used for concept maturation; and
- Statutory and regulatory--the Federal Acquisition Regulation; the DoD 5000-series; etc.

Key to this initial step of concept refinement is to ensure that all drivers of the concept definition are completely captured and managed as an integrated whole, and that all of the drivers can be met by each of the concept alternatives under consideration. This defines the expectations of the overall system concept, and defines the trade space and risk associated with each of the constraints, above. Defining the trade space and risk enables the comprehensive analysis of system alternatives, and allows a rational selection of a preferred system concept. The preferred system concept should strike the best balance in providing the needed capabilities within the constraints on the program.

4.3.1.3.2. Develop Concept Performance (and Constraints) Definition and Verification Objectives

This step includes the analysis and decomposition (from capability level to system level) of system performance and system design constraints traceable back to those capabilities and constraints defined in Section 4.3.1.3.1 above. All capabilities and environmental constraints should be decomposed to the system performance level. They should be re-analyzed to determine the extent to which alternative concepts can meet all capability needs within program constraints (as needs and constraints become better understood as a result of decomposition). The trade space and risk should be analyzed and assessed for each alternative concept. For each alternative system concept, expected performance capabilities should be explicitly defined and related to the capability needs. To the extent concept performance can only be met through trade offs (due to incompatibility of capabilities/constraints) changes may be required to the capability or constraints previously defined.

Verification planning should define the test requirements needed to evaluate the ability of the matured system concept(s) to meet requirements.

4.3.1.3.3. Decompose Concept Performance into Functional Definition and Verification Objectives

This step includes the further decomposition of concept system performance to the functional level. Consideration should be given to inclusion of functionality and functional flow definition across the full system concept (tactical system, support system, training system) and how this functionality relates to other interoperable systems (functional interfaces). Critical to this analysis is an understanding of the level of

functionality achievable within program constraints and risk. Trade space and risk should be analyzed and assessed against desired functional performance. Trade offs are made to stay within program constraints and may require changes to higher-level system or concept definitions.

System functional verification planning should enable test and evaluation of the matured system concept functionality.

4.3.1.3.4. Decompose Concept Functional Definition into Concept Components and Assessment Objectives

This step includes the allocation of concept functions into components of the concept that will execute the functionality. Critical to this analysis is an understanding of what functional performance is enabled by multiple systems, or system components, operating as a functional entity. Hardware elements, software elements, physical interfaces, functional interfaces, standards, existing, and to-be-developed elements, should all be considered and defined in the concept. As in previous steps, this level of decomposition and allocation may induce trades to stay within program constraints. These trades need to be reflected in higher level functional, system, and capability definitions, which should be updated accordingly.

Concept component verification planning should enable testing and validation of critical concept components.

4.3.1.3.5. Develop Component Concepts, Including Enabling/Critical Technologies, Constraints, and Cost/Risk Drivers

At this point, all of the basic concept design requirements should have been analyzed, defined, and reconciled with constraints. The system concept(s) components should have been synthesized and substantiated (e.g., through analyses, modeling and simulation, demonstrations, etc.) to allow verification of components against requirements, and integration of the components into an overall system for further verification and validation. Key to this step is the development of conceptual components to demonstrate the viability of the overall concept, indicate where additional technology maturation should occur, and validate that acceptable trade space between expected capabilities and program constraints exists to accommodatepotential risk.

4.3.1.3.6. Analyze and Assess Enabling/Critical Components Versus Capabilities

Utilizing the component verification plans developed as part of the functional allocation, the enabling and/or critical components of the concept should be evaluated. Evaluation results should be assessed against component requirements and the impact on the overall concept capabilities and constraints determined. Critical to this step is the understanding of test results and how the concept component functionality verifies or contradicts the desired capabilities, as well as what component technologies are required and the level of achievable performance. Capability trade offs within the available trade space, or further component concept development within program and concept constraints may be required.

4.3.1.3.7. Analyze and Assess System Concept Versus Functional Capabilities

Utilizing the concept functional verification plans developed as part of the functional analysis and decomposition, overall system functionality should be evaluated. Concept components should be integrated and assessed from a functional standpoint relative to desired capabilities. Critical to this step is understanding how the enabling components work together as an integrated whole to provide functionality at the component and system levels, and how the achieved functionality relates to the overall desired capability. Also important is an understanding of the technology development required to achieve critical functions. Capability trade offs within the available trade space, or further refinement of functionality within program and concept constraints may be required.

4.3.1.3.8. Analyze and Assess Concept and Verify System Concept's Performance

Utilizing the verification objectives previously defined, evaluate the overall integrated concept against system performance objectives and constraints. Concept components are integrated from both physical and functional perspectives across the full concept domain (tactical, support, training, etc.). Critical to this step is an understanding of overall system concept capability versus need, level of achievable performance within the complete set of constraints, and the enabling technologies requiring further development. Trades at this level will include decisions as to acceptable technology risk versus desired performance.

4.3.1.3.9. Analyze and Assess Concepts Versus Defined User Needs and Specified Environmental Constraints

Based upon the results of the verification of components, functionality, and system performance, a determination of the preferred system concept should be made. Advantages and disadvantages of various approaches should be documented and included in the analysis of alternatives. Trade offs of achievable performance should be complete and captured in a preliminary system specification. Enabling technologies requiring further development to achieve acceptable levels of risk should be defined and plans should be developed for technology development. The preliminary system specification serves as the guiding technical requirement for this development effort.

4.3.1.4. Technical Reviews during Concept Refinement

4.3.1.4.1. Initial Technical Review (ITR)

The ITR is a multi-disciplined technical review to support a program's initial Program Objective Memorandum submission. This review ensures that a program's technical baseline is sufficiently rigorous to support a valid cost estimate (with acceptable cost risk), and enable an independent assessment of that estimate by cost, technical, and program management subject matter experts. The ITR assesses the capability needs and conceptual approach of a proposed program and verifies that the requisite research, development, test, engineering, logistics, and programmatic bases for the program reflect the complete spectrum of technical challenges and risks. Additionally, the ITR ensures that historical and prospective drivers of system cost have been quantified to the

maximum extent and that the range of uncertainty in these parameters has been captured and reflected in the program cost estimates.

Per DoD Instruction 5000.2, the program manager for Acquisition Category I and IA programs must define program and system parameters in a Cost Analysis Requirements Description (CARD), as described in DoD 5000.4M. The basic CARD technical and programmatic guidance, tailored to suit the scope and complexity of the program, should be followed to ensure that all pertinent technical cost drivers are addressed. The success of the ITR also depends on independent subject matter expert review of each of the identified cost drivers. The subject matter experts should be drawn from the correct technical competencies that specialize in each of the areas addressed in a CARD-like document, and the cost drivers detailed in the CARD-like document should be used properly in the development of the program cost estimate. Completion of the ITR should provide:

(1) A complete CARD-like document detailing system overview, risk, and system operational concept;

(2) An assessment of the technical and cost risks of the proposed program; and

(3) An independent assessment of the program's cost estimate.

Typical ITR success criteria include affirmative answers to the following exit questions:

(1) Does the CARD-like document capture the key program cost drivers, development costs (all aspects of hardware, human integration, and software), production costs, operation and support costs? Is the CARD-like document complete and thorough?

(2) Are the underlying assumptions used in developing the CARD-like document technically and programmatically sound and complete?

(3) Have the appropriate technical and programmatic competencies been involved in the CARD-like document development, and have the proper subject matter experts been involved in its review?

(4) Are the risks known and manageable within the cost estimate?

(5) Is the program, as captured in the CARD-like document, executable?

4.3.1.4.2. Alternative System Review (ASR)

The ASR is a multi-disciplined technical review to ensure that the resulting set of requirements agrees with the customers' needs and expectations and that the system under review can proceed into the Technology Development phase. The ASR should be complete prior to Milestone A. Generally this review assesses the alternative systems that have been evaluated during the Concept Refinement phase, and ensures that the preferred system alternative is cost effective, affordable, operationally effective and suitable, and can be developed to provide a timely solution to a need at an acceptable level of risk. Of critical importance to this review is the understanding of available system concepts to meet the capabilities described in the Initial Capabilities Document and the affordability, operational effectiveness, and technology risks inherent in each

alternative concept. Depending on the overall acquisition strategy, one or more preferred solutions may carry forward into the Technology Development phase.

By reviewing alternative system concepts, the ASR helps ensure that sufficient effort has been given to conducting trade studies that consider and incorporate alternative system designs that may more effectively and efficiently meet the defined capabilities. A successful review is predicated on the IPT's determination that the operational capabilities, preferred solution(s), available technologies, and program resources (funding, schedule, staffing, and processes) form a satisfactory basis for proceeding into the Technology Development phase. The program manager should tailor the review to the technical scope and risk of the system, and address the ASR in the Systems Engineering Plan.

Completion of the ASR should provide:

(1) An agreement on the preferred system concept(s) to take forward into Technology Development.

(2) Hardware and software architectural constraints/drivers to address Defense Information Infrastructure / Common Operating Environment and system extensibility requirements.

(3) An assessment of the full system software concept to include conceptual definition of the complete deliverable/non-deliverable software, scope, and risk (e.g., operational software elements, software engineering environment, test software, maintenance software, simulation/stimulation software, training software, in-service support software, etc.).

(4) A comprehensive rationale for the preferred solution, including the Analysis of Alternatives that evaluated relative cost, schedule, performance (hardware, human, software), and technology risks.

(5) A comprehensive assessment of the relative risks associated with including commercial off-the-shelf items in the program, with emphasis on host platform environmental design, diagnostic information integration, and maintenance concept compatibility.

(6) A comprehensive risk assessment for the Technology Development phase.

(7) Trade studies/technical demonstrations for concept risk reduction.

(8) Joint requirements for the purposes of compatibility, interoperability, and integration.

(9) Refined thresholds and objectives initially stated as broad measures of effectiveness.

(10) Completed, comprehensive planning for the Technology Development phase (hardware and software), that addresses critical components to be developed and demonstrated, their cost, and critical path drivers.

(11) Initial planning for the System Development and Demonstration phase.

(12) A draft system requirements document if one does not already exist. (This is a high-level engineering document that represents the customer/user capability needs as system requirements.) This systems requirement document should include a system level description of all software elements required by the preferred system concept.

The ASR is important because it is a comprehensive attempt to ensure that the system requirements are aligned with the customer's needs. However, Cost As an Independent Variable may result in Initial Capabilities Document requirement(s) adjustments (IAW 2170 JCIDS procedures.) The ASR attempts to minimize the number of requirements that may need to be changed in later phases. Changing requirements later in the program will usually entail cost increases and scheduling slips.

Typical ASR success criteria include affirmative answers to the following exit questions:

(1) Can the preferred solution(s) satisfy the Initial Capabilities Document which may have been adjusted (IAW 3170 JCIDS procedures) for Cost As an Independent Variable?

(2) Is the preferred solution(s) sufficiently detailed and understood to enable entry into Technology Development with low technical risk?

(3) Are the system software scope and complexity sufficiently understood and addressed in the planning for the Technology Development phase to enable an acceptable/manageable level of software technical risk?

(4) Are the risks for Technology Development known and manageable?

(5) Is the program schedule executable (technical/cost risks)?

(6) Is the program properly staffed?

(7) Is the Technology Development work effort executable within the existing budget?

(8) Has a preliminary system specification, consistent with technology maturity and the proposed program cost and schedule, captured the system technical baseline?

4.3.1.4.3. Summary of Outputs of the Systems Engineering Processes in Concept Refinement

- Preliminary System Specification;
- Test and Evaluation Strategy;
- Systems Engineering Plan;
- System Safety Analyses;
- Support and Maintenance Concepts and Technologies;
- Inputs to draft Capability Development Document;
- Inputs to Technology Development Strategy;
- Inputs to Analysis of Alternatives; and
- Inputs to Cost and Manpower Estimate.

4.3.2. Technology Development Phase

A successful Milestone A decision initiates the Technology Development phase. Per DoD Instruction 5000.2, this phase reduces technology risk and determines the appropriate set of technologies to be integrated into a full system. Technology development is a continuous technology discovery and development process that reflects close collaboration between the Science and Technology community, the user, and the developer. Technology development is an iterative process of assessing technologies and refining user performance parameters. The Initial Capabilities Document, the Technology Development Strategy, and working the draft Capability Development Document guide the phase efforts, leading to the Capability Development Document.

4.3.2.1. Purpose of Systems Engineering in Technology Development

During Technology Development, systems engineering provides comprehensive, iterative processes to accomplish the following activities:

- Convert each required capability into a system performance specification;
- Translate user-defined performance parameters into configured systems;
- Integrate the technical inputs of the entire design team;
- Manage interfaces;
- Characterize and manage technical risk;
- Transition technology from the technology base into program specific efforts; and
- Verify that designs meet operational needs.

Systems engineering processes develop the suite of technologies for the preferred system solution.

4.3.2.2. Inputs to the Systems Engineering Processes in Technology Development

The following information sources provide important inputs to the systems engineering processes supporting Technology Development:

- Initial Capabilities Document and draft Capability Development Document;
- Preferred System Concept;
- Exit Criteria;
- Test and Evaluation Strategy;
- Support and Maintenance Concepts and Technologies;
- Analysis of Alternatives;
- Systems Engineering Plan; and
- Technology Development Strategy.

4.3.2.3. Key Systems Engineering Activities During Technology Development

Figure 4.3.2.3.1. identifies the systems engineering-related steps during the Technology Development Phase. Paragraphs below contain additional detail on each step.

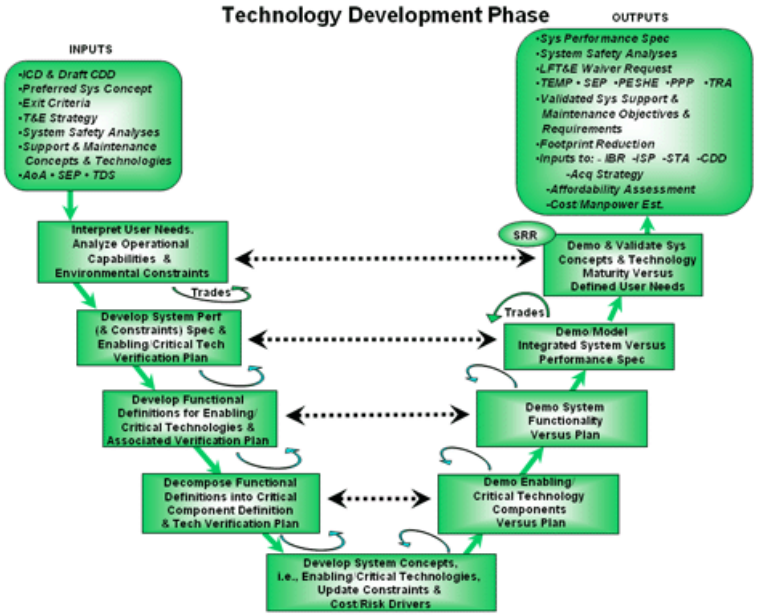

Figure4.3.2.3.1. Systems engineering-related steps during Technology Development

4.3.2.3.1. Interpret User Needs; Analyze Operational Capabilities and Environmental Constraints

This step includes the aggregation of all inputs available at this stage of the program (Initial Capabilities Document, draft Capability Development Document, results of the Analysis of Alternatives and identification of the preferred system concept, exit criteria for the phase, Systems Engineering Plan, Technology Development Strategy, Test and Evaluation Strategy, as well as associated support and maintenance concepts and technologies, training system, and interoperable systems). Additional analysis and definition may be required to ascertain all of the related constraints to be applied to the effort:

- Environmental-systems threats, usage environment, support environment, doctrine, operational concepts, etc.;

- Resource-industrial base; notional available development, operation, and support budgets; and the required date for system fielding;
- Technology-applicable technology base to be used for technology development; and
- Statutory and regulatory-the Federal Acquisition Regulation; the DoD 5000-series; etc.

Key to this technology development effort is ensuring that all aspects of the required technology are adequately matured and managed as an integrated whole, and can support the user needs via the preferred concept. This not only ensures that overall expectations are explicitly defined, but that trade space and risk in each of the areas above are defined to enable comprehensive analysis of technology availability and rational formulation of a system performance specification that strikes the best balance in meeting all of the needed capabilities within the many constraints on the program.

4.3.2.3.2. Develop System Performance (and Constraints) Specifications and Enabling/Critical Technologies Verification Plan

This step includes the further analysis and decomposition (from capability level to system level) of system performance and system design constraints, traceable back to those capabilities and constraints defined above. All capabilities and environmental constraints should be decomposed to the system performance level. They should be re-analyzed to determine the extent to which available technologies can meet the full spectrum of needs and constraints (as needs and constraints become better understood as a result of decomposition). The trade space and risk should be analyzed and assessed against available technologies. The enabling and/or critical technologies should be identified. Each technology performance capability should be explicitly defined and related to the capability needs. To the extent performance can only be met through trade offs of certain aspects (due to incompatibility of capabilities/constraints), changes may be required to the capability or constraints previously defined.

Verification planning should define the test requirements needed to evaluate the ability of enabling and/or critical technologies to meet system requirements.

4.3.2.3.3. Develop Functional Definitions for Enabling/Critical Technologies and Associated Verification Plan

This step requires the further decomposition of system performance to the functional level. The functional requirements should be evaluated against available technologies, such that enabling and/or critical technologies can be defined. Consideration should be given to inclusion of functionality and functional flow definition across the full system (tactical system, support system, training system) and how this functionality relates to other interoperable systems (functional interfaces). Critical to this analysis is an understanding of the level of functionality achievable within the program constraints and program risk. Trade space and risk should be analyzed and assessed against desired functional performance. Trade offs may be required to stay within program constraints and may require changes to higher-level system definitions.

System functional verification planning should develop the test requirements to evaluate system functionality and the maturity of the enabling/critical technologies.

4.3.2.3.4. Decompose Functional Definitions into Critical Component Definition and Technology Verification Plan

This step includes the allocation of system functions into critical components of the system that will provide the required functionality. Key to this analysis is an understanding of what functional performance is enabled by multiple systems, or system components, operating as a functional entity. Hardware elements, software elements, physical interfaces, functional interfaces, standards, existing and to-be-developed technology elements, should all be considered and defined in the system specification. As in previous steps, this level of decomposition and allocation may induce trades to stay within program constraints. These trades should be reflected in higher level functional, system, capability definitions, and system specifications (i.e., these engineering entities should be updated accordingly).

System component verification planning should enable testing and validation of critical system components.

4.3.2.3.5. Develop System Concepts, i.e., Enabling/Critical Technologies; Update Constraints and Cost/Risk Drivers

At this point, all of the basic system design requirements should have been analyzed, defined, and reconciled with constraints. The system components are synthesized and substantiated (e.g., through analyses, modeling and simulation, demonstrations, etc.) to allow verification of the components against requirements, and integration of the components into an overall system for further validation. Key to this step is the development of system concepts that will demonstrate the viability of the overall system, indicate where enabling and/or critical technology maturation should occur, and validation that acceptable trade space and risk exists within the program constraints.

4.3.2.3.6. Demonstrate Enabling/Critical Technology Components Versus Plan

Using the system component verification planning developed as part of the functional allocation, the system enabling/critical technology components should be evaluated. Evaluation results should be assessed against system component requirements, and the impact on the overall system capabilities and constraints determined. Critical to this step is the understanding of test results and how the system component functionality verifies or contradicts the desired capabilities, as well as what enabling and/or critical component technologies are required and the level of achievable performance. Trade offs to system capability or additional system component development may be required, within the program and system constraints and trade space available.

4.3.2.3.7. Demonstrate System Functionality Versus Plan

Utilizing the system functional verification plans developed as part of the functional analysis and decomposition, the overall system functionality should be evaluated. System

components are integrated and assessed from a functional standpoint relative to desired capabilities. Critical to this step is the understanding of how the enabling components work together as an integrated whole to enable functionality at the system level, and how the achieved functionality relates to the overall desired system capability. Also important is an understanding of the enabling and/or critical technology maturity required to achieve critical functions. Trade offs of desired capability, or further refinement of functionality may be required within program and system constraints, and available trade space.

4.3.2.3.8. Demonstrate/Model the Integrated System Versus the Performance Specification

Utilizing Engineering Development Models (EDMs), modeling and simulation, and the verification objectives previously defined (section 4.3.2.3.2.), evaluate the overall integrated system against system performance objectives and constraints. System components are integrated from both physical and functional perspectives across the full system domain (tactical, support, training, etc.). Critical to this step is an understanding of: overall system capability versus need, level of achievable performance within the complete set of constraints, and the enabling/critical technologies requiring further development. Trades at this level will include decisions as to acceptable technology risk versus desired system performance.

4.3.2.3.9. Demonstrate and Validate the System Concepts and Technology Maturity Versus Defined User Needs

Based upon the results of the verification of components, functionality, and system performance, a System Performance Specification should be created. Trade-offs of achievable performance should be complete and captured in the Systems Specification. Critical and/or enabling technologies should have demonstrated adequate maturity to achieve acceptable levels of risk. The System Performance Specification serves as the guiding technical requirement for the system development effort.

4.3.2.4. Technical Reviews during Technology Development

4.3.2.4.1. System Requirements Review (SRR)

The SRR is conducted to ascertain progress in defining system technical requirements. This review determines the direction and progress of the systems engineering effort and the degree of convergence upon a balanced and complete configuration. It is normally held during Technology Development, but may be repeated after the start of System Development and Demonstration to clarify the contractor's understanding of redefined or new user requirements.

The SRR is a multi-disciplined technical review to ensure that the system under review can proceed into the System Development and Demonstration phase, and that all system requirements and performance requirements derived from the Initial Capabilities Document or draft Capability Development Document are defined and are consistent with cost (program budget), schedule (program schedule), risk, and other system constraints. Generally this review assesses the system requirements as captured in the

system specification, and ensures that the system requirements are consistent with the preferred system solution as well as available technologies resulting from the Technology Development phase. Of critical importance to this review is an understanding of the program technical risk inherent in the system specification and in the System Development and Demonstration Phase Systems Engineering Plan. Determining an acceptable level of risk is key to a successful review.

Completion of the SRR should provide:

(1) An approved preliminary system performance specification;

(2) A preliminary allocation of system requirements to hardware, human, and software subsystems;

(3) Identification of all software components (tactical, support, deliverable, non-deliverable, etc.);

(4) A comprehensive risk assessment for System Development and Demonstration;

(5) An approved System Development and Demonstration Phase Systems Engineering Plan that addresses cost and critical path drivers; and

(6) An approved Product Support Plan with updates applicable to this phase.

During the SRR, the systems requirements are evaluated to determine whether they are fully defined and consistent with the mature technology solution, and whether traceability of systems requirements to the Initial Capabilities Document or draft Capability Development Document is maintained. A successful review is predicated on the IPT's determination that the system requirements, preferred system solution, available technology, and program resources (funding, schedule, staffing, and processes) form a satisfactory basis for proceeding into the SDD phase. The program manager should tailor the review to the technical scope and risk of the system, and address the SRR in the Systems Engineering Plan.

Typical SRR success criteria include affirmative answers to the following exit questions:

(1) Can the system requirements, as disclosed, satisfy the Initial Capabilities Document or draft Capability Development Document?

(2) Are the system requirements sufficiently detailed and understood to enable system functional definition and functional decomposition?

(3) Is there an approved system performance specification?

(4) Are adequate processes and metrics in place for the program to succeed?

(5) Have Human Systems Integration requirements been reviewed and included in the overall system design?

(6) Are the risks known and manageable for development?

(7) Is the program schedule executable (technical and/or cost risks)?

(8) Is the program properly staffed?

(9) Is the program executable within the existing budget?

(10) Does the updated cost estimate fit within the existing budget?

(11) Is the preliminary Cost Analysis Requirements Description consistent with the approved system performance specification?

(12) Is the software functionality in the system specification consistent with the software sizing estimates and the resource-loaded schedule?

(13) Did the Technology Development phase sufficiently reduce development risks?

The SRR is important in understanding the system performance, cost, and scheduling impacts that the defined requirements will have on the system. This is the last dedicated review of the system requirements, unless an additional SRR is held after the refining of the system performance constraints during the System Development and Demonstration Phase.

4.3.2.4.2. Integrated Baseline Review (IBR)

Program managers should use the IBR throughout the program when Earned Value Management is required. This review has a business focus, but should include the important technical considerations discussed below. The process is composed of four steps:

(1) The Program Manager's assessment of their understanding of the risks;

(2) Preparation for an IBR;

(3) Execution of the IBR; and

(4) The management process (the source of on-going mutual understanding).

The key step in the process is execution of the IBR. The IBR establishes a mutual understanding of the project performance measurement baseline. This understanding provides for an agreement on a plan of action to evaluate the risks inherent in the program measurement baseline and the management processes that operate during project execution. Completion of the review should result in the assessment of risk within the program measurement baseline and the degree to which the following have been established:

(1) Technical scope of work is fully included and is consistent with authorizing documents;

(2) Key project schedule milestones are identified and supporting schedules reflect a logical flow to accomplish the work;

(3) Resources (budgets, facilities, personnel, skills, etc.) are available and are adequate for the assigned tasks;

(4) Tasks are planned and can be measured objectively relative to the technical progress;

(5) Rationales underlying the Program Measurement Baseline are reasonable; and

(6) Management processes support successful execution of the project.

Section 11.3.4 describes an IBR. The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, in cooperation with industry, has also prepared an IBR handbook.

4.3.2.4.3. Technology Readiness Assessment (TRA)

Per DoD Instruction 5000.2, the TRA is a regulatory information requirement for all acquisition programs. The TRA is a systematic, metrics-based process that assesses the maturity of Critical Technology Elements. The TRA should be conducted concurrently with other Technical Reviews, specifically the Alternative Systems Review, System Requirements Review, or the Production Readiness Review. If a platform or system depends on specific technologies to meet system operational threshold requirements in development, production, and operation, and if the technology or its application is either new or novel, then that technology is considered a Critical Technology Element. The TRA should not be considered a *risk* assessment, but it should be viewed as a tool for assessing program risk and the adequacy of technology maturation planning. The TRA scores the current readiness level of selected system elements, using defined Technology Readiness Levels. The TRA highlights critical technologies and other potential technology risk areas that require program manager attention. The TRA essentially "draws a line in the sand" on the day of the event for making an assessment of technology readiness for critical technologies integrated at some elemental level. If the system does not meet pre-defined Technology Readiness Level scores, then a Critical Technology Element maturation plan is identified. This plan explains in detail how the Technology Readiness Level will be reached prior to the next milestone decision date or relevant decision point. Completion of the TRA should provide:

(1) A comprehensive review, using an established program Work Breakdown Structure as an outline, of the entire platform or system. This review, using a conceptual or established baseline design configuration, identifies program Critical Technology Elements;

(2) An objective scoring of the level of technological maturity for each Critical Technology Element by subject matter experts;

(3) Maturation plans for achieving an acceptable maturity roadmap for Critical Technology Elements prior to critical milestone decision dates; and

(4) A final report documenting the findings of the assessment panel.

After the final report is written, the chairman submits the report to the appropriate Service officials and the program manager. Once approved, the report and cover letter are forwarded to the service acquisition official. For Acquisition Category ID or IAM programs, the service acquisition official provides a recommendation to DDR&E for DUSD(S&T) final approval. If deemed necessary, the DDR&E can conduct an Independent Technical Assessment (ITA) in addition to, and totally separate from, the program TRA.

4.3.2.5. Outputs of the Systems Engineering Processes in Technology Development

- Preliminary System Performance Specification;
- Live-Fire T&E Waiver request;
- Test and Evaluation Master Plan;
- Risk Assessment
- Systems Engineering Plan;
- Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE);
- NEPA Compliance Schedule (as required);
- Program Protection Plan;
- Technology Readiness Assessment;
- Validated System Support and Maintenance Objectives and Requirements;
- Footprint Reduction;
- Inputs to Integrated Baseline Review;
- Inputs to the Information Support Plan;
- Inputs to the System Threat Assessment;
- Inputs to the Capability Development Document;
- Inputs to the Acquisition Strategy;
- Inputs to the Affordability Assessment;
- Inputs to the Cost and Manpower Estimate; and

4.3.3. System Development and Demonstration Phase

A program usually enters the acquisition process at Milestone B, when the Milestone Decision Authority permits the system to enter the System Development and Demonstration phase and initiates the program. A key emphasis during System Development and Demonstration is to ensure operational supportability with particular attention to minimizing the logistics footprint.

The purposes of System Development and Demonstration are to:

- Develop a system or increment of capability;
- Reduce integration and manufacturing risk;
- Ensure operational supportability with particular attention to reducing the logistics footprint;
- Implement human systems integration;
- Design for producibility;
- Ensure affordability and protection of critical program information; and
- Demonstrate system integration, interoperability, safety, and utility.

In System Development and Demonstration, the program, the system architecture, and system elements down to the configuration item level are defined based upon the mature technology suite selected and integrated during Concept Refinement and Technology Development. During System Development and Demonstration, system design requirements are allocated down to the major subsystem level, and are refined as a result of developmental and operational tests, and iterative systems engineering analyses. The support concept and strategy are refined.

Two work efforts, separated by the Design Readiness Review, comprise System Development and Demonstration: System Integration and System Demonstration.

4.3.3.1. Inputs to the Systems Engineering Processes in System Integration

Inputs to the Systems Engineering processes in System Development and Demonstration include the following:

- System Performance Specification;
- Exit Criteria;
- Validated System Support and Maintenance Objectives and Requirements;
- Acquisition Program Baseline;
- Capability Development Document;
- Systems Engineering Plan;
- Information Support Plan;
- Test and Evaluation Master Plan;
- Programmatic Environment, Safety, and Occupational Health Evaluation; and
- Product Support Strategy.

4.3.3.2. Purpose of Systems Engineering in System Integration

The System Integration work effort begins when the program manager has a technical solution for the system or increment of capability, but has not integrated the components and subsystems into a system. Through the use of systems engineering, the System Integration effort integrates components and subsystems, completes the detailed design, and reduces system level risk. The effort typically includes the demonstration of prototype articles or engineering development models.

4.3.3.3. Key Systems Engineering Activities During System Integration

Figure 4.3.3.3.1. identifies the systems engineering-related steps during the System Integration effort of the System Development and Demonstration Phase. Paragraphs below contain additional detail on each step.

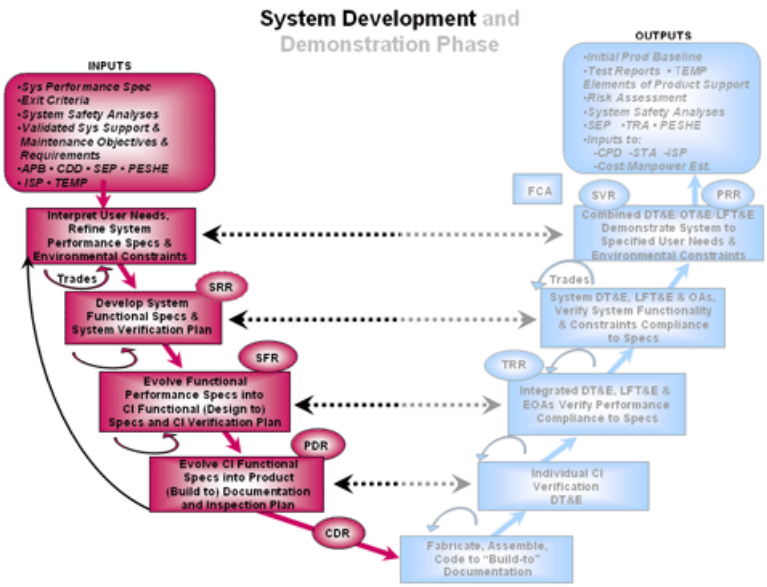

Figure4.3.3.3.1. Systems engineering-related steps during the System Integration effort of System Development and Demonstration.

4.3.3.3.1. Interpret User Needs, Refine System Performance Specifications and Environmental Constraints

This step includes understanding all of the inputs available at this stage of the program, including the Initial Capabilities Document, Capability Development Document, Acquisition Program Baseline, Systems Engineering Plan, Test and Evaluation Master Plan, as well as validated system support and maintenance concepts and technologies. The users and the requirements authority have already approved a minimum set of key performance parameters that are included in the Capability Development Document that guides the efforts of this phase. As the design matures, the program manager may conduct trade studies on the threshold and objective levels, and refine the key performance parameters thresholds and objectives with the approval of the requirements authority.

Throughout the development activities, the program manager should maintain a thorough understanding of the key performance parameters, other specified performance parameters, and the suite of matured technologies resulting from the Technology Development phase. The program manager should ensure that all aspects of the specified system are adequately matured and managed as an integrated whole. The refined system specifications should consider all Lifecycle processes and constraints, such as system

availability, supportability, logistics footprint, training, and other logistics requirements, developmental and operational test environments and scenarios, and disposal. For example, the program manager should plan the Environment, Safety, and Occupational Health assessment. The program manager should develop and manage the system requirements stemming from the Lifecycle considerations, and use prototypes to ensure user and other stakeholder buy-in as the design matures. The program manager should continually update cost and schedule estimates synchronized with the Systems Engineering Plan and Program Plan. The program manager should continually address and characterize technical risk, and prepare for an additional System Requirements Review, if required.

4.3.3.3.2. Develop System Functional Specifications and System Verification Plan

This step determines the required system functions based on the Capability Development Document performance parameters and all other requirements and constraints, and allocates subsystems to each function. Partitioning of the system into subsystems leads to the definition of subsystem interfaces and integration requirements. The engineers define hardware, human, and software functional expectations, and establish the system functional baseline for the System Functional Review that follows this step. The program manager should continually monitor system cost, schedule, and risk. The program manager should factor all design considerations into trade studies, and incorporate them into the design. The program manager should develop plans for the subsystem integration, verification, and validation processes, as well as verification and validation plans for the system as a whole. The planning should consider all interface functional and performance specifications.

4.3.3.3.3. Evolve Functional Performance Specifications into Configuration Item (CI) Functional ("Design-to") Specifications and CI Verification Plan

This step involves allocating functional performance specifications into system functional and performance requirements allocated across the CIs. Enabling or critical technologies, the envisioned operational environment(s), the "ilities" and the other logistics elements should be part of satisfying performance needs. The program manager should plan to test or verify the configuration items for functionality and performance. The program manager should continually monitor risk and assess its impact on cost, schedule, and performance. Additional analyses conducted at this step include a Failure Mode Effects and Criticality Analysis, a Failure Tree Analysis, and a Reliability-Centered Maintenance (RCM) Analysis.

The program manager should convene a Preliminary Design Review after this step and approve the allocated baseline. The allocated baseline includes all functional and interface characteristics allocated from the system, interface requirements with other CIs, and design constraints. The allocated baseline should describe the verification required to demonstrate the achievement of specified functional and interface characteristics.

4.3.3.3.4. Evolve CI Functional Specifications into Product ("Build-to") Documentation and Inspection Plan

This step finalizes the detailed design of the system. The design should include all hardware and software components. The engineers should complete drawings and other documentation for "building" the components (i.e., fabricating hardware components or coding the software element) and plan for the integration and testing of all of the components. The program manager should plan the acquisition of any commercial item components or reuse of components from some other effort. Environment, Safety and Occupational Health and other Lifecycle and/or environmental considerations that affect the component level of the system should be part of the decision-making and trade studies that occur at this level of design. The program manager should continually assess cost, schedule, and performance. Additional analyses at this step include a Level of Repair Analysis and a Maintenance Task Analysis. Analysts should estimate the projected system reliability from demonstrated reliability rates.

The program manager should convene a Critical Design Review at the end of this step. The end product of the Critical Design Review is a product baseline. The majority of production capable system drawings should have been validated and approved prior to the Critical Design Review.

4.3.3.3.5. Fabricate, Assemble, Code to "Build-to" Documentation

This step involves fabricating hardware components and coding software components; acquiring all other components, including commercial items, being bought or reused; and then assembling the components according to the integration (and test) planning. At this point, all the system, subsystem, and component design requirements should have been developed. The program manager should manage the design requirements and plan for corrective action for any discovered hardware and software deficiencies. If any technology is not mature enough to be used in the current increment, the program manager should integrate and test an alternative, mature, technology in its place. The program manager should relegate the immature technology to the next increment of the system. The program manager should continually assess cost, schedule, and performance.

This step will usually result in prototypes and engineering development models, and should include developmental testing to support the Design Readiness Review. During this time, the program manager should prepare the required information for the Design Readiness Review.

4.3.3.4. Technical Reviews During System Integration

4.3.3.4.1. Integrated Baseline Review (IBR)

The program manager may convene an additional IBR to support the System Development and Demonstration contract. Section 4.3.2.4.2 of this Guidebook discusses the systems engineering considerations associated with an IBR. Section 11.3.4describes an IBR in detail, and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, in cooperation with industry, has prepared an IBR handbook.

4.3.3.4.2. System Requirements Review (SRR)

The SRR is a multi-functional technical review to ensure that all system and performance requirements derived from the Capability Development Document are defined and consistent with cost (program budget), schedule (program schedule), risk, and other system constraints. Generally this review assesses the system requirements captured in the system specification. The review ensures consistency between the system requirements and the preferred system solution and available technologies. The assigned manager may convene an SRR prior to program initiation, during Technology Development; and the program manager may convene an SRR during System Development and Demonstration. Section 4.3.2.4.1. of this Guidebook discusses the systems engineering considerations associated with an SRR.

4.3.3.4.3. System Functional Review (SFR)

The SFR is a multi-disciplined technical review to ensure that the system under review can proceed into preliminary design, and that all system requirements and functional performance requirements derived from the Capability Development Document are defined and are consistent with cost (program budget), schedule (program schedule), risk, and other system constraints. Generally this review assesses the system functional requirements as captured in system specifications (functional baseline), and ensures that all required system performance is fully decomposed and defined in the functional baseline. System performance may be decomposed and traced to lower-level subsystem functionality that may define hardware and software requirements. The SFR determines whether the systems functional definition is fully decomposed to a low level, and whether the IPT is prepared to start preliminary design.

Completion of the SFR should provide:

(1) An established system functional baseline;

(2) An updated risk assessment for the System Development and Demonstration phase;

(3) An updated Cost Analysis Requirements Description (CARD) (or CARD-like document) based on the system functional baseline;

(4) An updated program development schedule including system and software critical path drivers; and

(5) An approved Product Support Plan with updates applicable to this phase.

The SFR determines whether the system's lower-level performance requirements are fully defined and consistent with the mature system concept, and whether lower-level systems requirements trace to top-level system performance and the Capability Development Document. A successful SFR is predicated upon the IPT's determination that the system performance requirements, lower level performance requirements, and plans for design and development form a satisfactory basis for proceeding into preliminary design.

The program manager should tailor the review to the technical scope and risk of the system, and address the SFR in the Systems Engineering Plan. The SFR is the last review that ensures the system is credible and feasible before more technical design work commences.

Typical SFR success criteria include affirmative answers to the following exit questions:

(1) Can the system functional requirements, as disclosed, satisfy the Capability Development Document?

(2) Are the system functional requirements sufficiently detailed and understood to enable system design to proceed?

(3) Are adequate processes and metrics in place for the program to succeed?

(4) Are the risks known and manageable for development?

(5) Is the program schedule executable (technical/cost risks)?

(6) Is the program properly staffed?

(7) Is the program with the approved functional baseline executable within the existing budget?

(8) Is the updated Cost Analysis Requirements Description consistent with the approved functional baseline?

(9) Does the updated cost estimate fit within the existing budget?

(10) Has the system Functional Baseline been established to enable preliminary design to proceed with proper Configuration Management?

(11) Is the software functionality in the approved functional baseline consistent with the updated software metrics and resource loaded schedule?

4.3.3.4.4. Preliminary Design Review (PDR)

The PDR is a multi-disciplined technical review to ensure that the system under review can proceed into detailed design, and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints. Generally, this review assesses the system preliminary design as captured in performance specifications for each configuration item in the system (allocated baseline), and ensures that each function in the functional baseline has been allocated to one or more system configuration items. Configuration items may consist of hardware and software elements and include such items as airframes, avionics, weapons, crew systems, engines, trainers/training, etc.

Completion of the PDR should provide:

(1) An established system allocated baseline;

(2) An updated risk assessment for System Development and Demonstration;

(3) An updated Cost Analysis Requirements Description (CARD) (or CARD-like document) based on the system allocated baseline;

(4) An updated program schedule including system and software critical path drivers; and

(5) An approved Product Support Plan with updates applicable to this phase.

For complex systems, the program manager may conduct a PDR for each subsystem or configuration item, leading to an overall system PDR. When individual reviews have been conducted, the emphasis of the overall system PDR should focus on configuration item functional and physical interface design, as well as overall system design requirements. The PDR determines whether the hardware, human, and software preliminary designs are complete, and whether the Integrated Product Team is prepared to start detailed design and test procedure development.

The PDR evaluates the set of subsystem requirements to determine whether they correctly and completely implement all system requirements allocated to the subsystem. The PDR also determines whether subsystem requirements trace with the system design. At this review the Integrated Product Team should review the results of peer reviews of requirements and preliminary design documentation. A successful review is predicated on the Integrated Product Team's determination that the subsystem requirements, subsystem preliminary design, results of peer reviews, and plans for development and testing form a satisfactory basis for proceeding into detailed design and test procedure development.

The program manager should tailor the review to the technical scope and risk of the system, and address the PDR in the Systems Engineering Plan.

Typical PDR success criteria include affirmative answers to the following exit questions:

(1) Does the status of the technical effort and design indicate operational test success (operationally suitable and effective)?

(2) Can the preliminary design, as disclosed, satisfy the Capability Development Document?

(3) Has the system allocated baseline been established and documented to enable detailed design to proceed with proper configuration management?

(4) Are adequate processes and metrics in place for the program to succeed?

(5) Have human integration design factors been reviewed and included, where needed, in the overall system design?

(6) Are the risks known and manageable for development testing and operational testing?

(7) Is the program schedule executable (technical/cost risks)?

(8) Is the program properly staffed?

(9) Is the program executable with the existing budget and with the approved system allocated baseline?

(10) Does the updated cost estimate fit within the existing budget?

(11) Is the preliminary design producible within the production budget?

(12) Is the updated Cost Analysis Requirements Description consistent with the approved allocated baseline?

(13) Is the software functionality in the approved allocated baseline consistent with the updated software metrics and resource-loaded schedule?

The program manager should conduct the PDR when all major design issues have been resolved and work can begin on detailed design. The PDR should address and resolved critical, system-wide issues.

4.3.3.4.5. Critical Design Review (CDR)

The CDR is a multi-disciplined technical review to ensure that the system under review can proceed into system fabrication, demonstration, and test; and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints. Generally this review assesses the system final design as captured in product specifications for each configuration item in the system (product baseline), and ensures that each product in the product baseline has been captured in the detailed design documentation. Product specifications for hardware enable the fabrication of configuration items, and may include production drawings. Product specifications for software (e.g., Software Design Documents) enable coding of a Computer Software Configuration Item. Configuration items may consist of hardware and software elements, and include items such as airframe, avionics, weapons, crew systems, engines, trainers/training, etc. Completion of the CDR should provide:

(1) An established system product baseline;

(2) An updated risk assessment for System Development and Demonstration;

(3) An updated Cost Analysis Requirements Description (CARD) (or CARD-like document) based on the system product baseline;

(4) An updated program development schedule including fabrication, test, and software coding critical path drivers; and

(5) An approved Product Support Plan with updates applicable to this phase.

For complex systems, the program manager may conduct a CDR for each subsystem or configuration item. These individual reviews would lead to an overall system CDR. When individual reviews have been conducted, the emphasis of the overall system CDR should focus on configuration item functional and physical interface design, as well as overall system detail design requirements. The CDR determines whether the hardware, human, and software final detail designs are complete, and whether the Integrated Product Team is prepared to start system fabrication, demonstration, and test.

The subsystem detailed designs are evaluated to determine whether they correctly and completely implement all system requirements allocated to the subsystem, and whether the traceability of final subsystem requirements to final system detail design is maintained. At this review, the Integrated Product Team also reviews the results of peer reviews on requirements and final detail design documentation, and ensures that the latest estimates of cost (development, production, and support) are consistent with the detail design. A successful review is predicated on the Integrated Product Team's determination that the subsystem requirements, subsystem detail design, results of peer reviews, and plans for testing form a satisfactory basis for proceeding into system fabrication, demonstration and test.

The program manager should tailor the review to the technical scope and risk of the system, and address the CDR in the Systems Engineering Plan.

Typical CDR success criteria include affirmative answers to the following exit questions:

(1) Does the status of the technical effort and design indicate operational test success (operationally suitable and effective)?

(2) Does the detailed design, as disclosed, satisfy the Capability Development Document or any available draft Capability Production Document?

(3) Has the system product baseline been established and documented to enable hardware fabrication and software coding to proceed with proper configuration management?

(4) Has the detailed design satisfied Human Systems Integration (HSI) requirements?

(5) Are adequate processes and metrics in place for the program to succeed?

(6) Are the risks known and manageable for developmental testing and operational testing?

(7) Is the program schedule executable (technical/cost risks)?

(8) Is the program properly staffed?

(9) Is the program executable with the existing budget and the approved product baseline?

(10) Is the detailed design producible within the production budget?

(11) Is the updated CARD consistent with the approved product baseline?

(12) Are all Critical Safety Items and Critical Application Items identified?

(13) Does the updated cost estimate fit within the existing budget?

(14) Is the software functionality in the approved product baseline consistent with the updated software metrics and resource-loaded schedule?

(15) Have key product characteristics having the most impact on system performance, assembly, cost, reliability, or safety been identified?

(16) Have the critical manufacturing processes that impact the key characteristics been identified and their capability to meet design tolerances determined?

(17) Have process control plans been developed for critical manufacturing processes?

The program manager should conduct the CDR when the "build-to" baseline has been achieved, allowing production and coding of software deliverables to proceed. A rule of thumb is that 75% to 90% of (manufacturing quality) product drawings and associated instructions should be complete, and that 100% of all airworthiness critical component (Critical Safety Items and Critical Application Items) drawings are complete.

4.3.3.5. Outputs of the Systems Engineering Processes/Inputs to the Design Readiness Review

The outputs of the systems engineering processes in System Integration become the inputs to the Design Readiness Review. These inputs include the following measures of design maturity:

- The number of subsystem and system technical reviews successfully completed;
- The percentage of drawings completed;
- Planned corrective actions to hardware/software deficiencies;
- Adequate development testing;
- An assessment of environment, safety and occupational health risks;
- A completed failure modes and effects analysis;
- The identification of key system characteristics and critical manufacturing processes; and
- An estimate of system reliability based on demonstrated reliability rates; etc.

4.3.3.6. Purpose of Systems Engineering in System Demonstration

Successful completion of the Design Readiness Review and successful demonstration of the system in prototypes or engineering development models end System Integration work effort. The program will normally continue in the System Development and Demonstration phase with the System Demonstration effort. System Demonstration demonstrates the ability of the system to operate in a useful way consistent with the approved key performance parameters. Through the use of systems engineering, a system is demonstrated in its intended environment, using the selected prototype. When the necessary industrial capabilities are reasonably available, the system satisfies approved requirements, and the system meets or exceeds exit criteria and Milestone C entrance requirements, the System Demonstration effort may end. Key to the System Demonstration effort is acceptable performance in developmental test and evaluation and early operational assessments, and the use of modeling and simulation to support test design and the demonstration of satisfactory system integration.

4.3.3.7. Inputs to the Systems Engineering Processes in System Demonstration

The results of the Design Readiness Review provide the principal inputs to the systems engineering processes during System Demonstration. The Capability Production Document, finalized after the Design Readiness Review, provides additional input.

4.3.3.8. Key SE Activities During System Demonstration

Figure 4.3.3.8.1. illustrates the steps during the System Demonstration part of the System Development and Demonstration phase. Further detail on each step is contained in the paragraphs below.

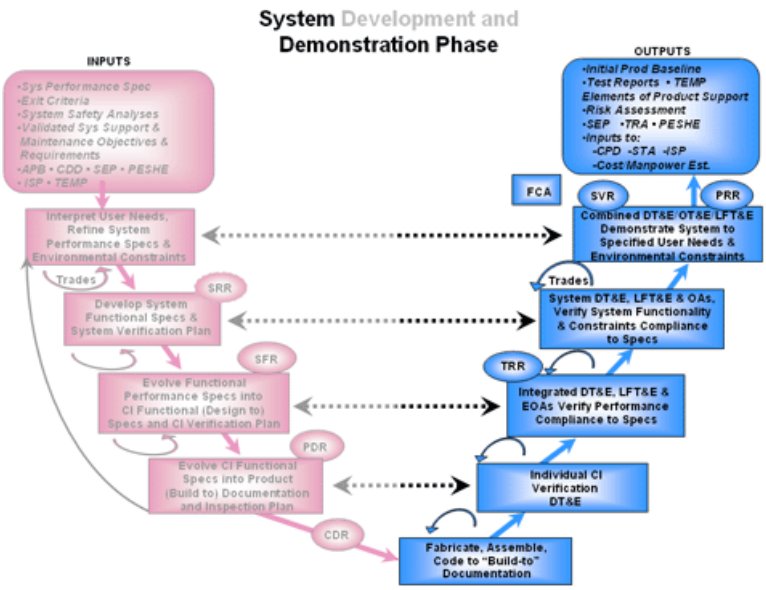

Figure4.3.3.8.1. Systems engineering-related steps during the System Demonstration effort of System Development and Demonstration.

4.3.3.8.1. Developmental Test and Evaluation verifies Individual Configuration Items

Demonstrate, according to the verification and validation plans, the physical, electrical, software, and other characteristics of the components to be integrated. Begin unit testing of hardware and independent verification and validation of software. Special attention should be placed on the integration and testing of commercial components. Ensure the components and any assemblies of them meet their requirements and function in the environment of their intended use. Developmental test and evaluation is conducted on the configuration items to assess technical progress against critical technical parameters. Continue to monitor risk, cost, and schedule. Design issues that arise as a result of the Integration, Verification, or Validation processes should feed back into the Design Solution process for refinement to the design. Early component level test may not require the same level of review as the final system level tests.

4.3.3.8.2. Integrated Developmental Test and Evaluation, Live Fire Test and Evaluation, and Early Operational Assessments verify Performance Compliance to Specifications

Verify subsystem hardware and software performance against their defined subsystem design requirements. Demonstrate subsystem hardware and software in their intended environment. Early operational assessments and developmental test and evaluation are conducted at the subsystem level, and risk, cost, and schedule continue to be monitored.

The Test Readiness Review occurs after this activity. The program manager determines the "formality" and scope of the Test Readiness Review for each assembly or subsystem.

The program manager also conducts the Functional Configuration Audit to verify that the actual performance of the configuration item meets specification requirements.

4.3.3.8.3. System Developmental Test and Evaluation, Live Fire Test and Evaluation, and Operational Assessments verify System Functionality and Constraints Compliance to Specifications

Integrate the subsystems into the defined system and demonstrate the integrated system under its operational environment constraints. This verifies that the system meets performance and functionality requirements, and validates the use of the system in its intended environment. This step includes developmental test and evaluation, any live fire test and evaluation, and operational assessments on the integrated system. All integration and interface issues must be resolved. Monitor and analyze risks as they pertain to the cost, schedule, and performance of the integrated system.

4.3.3.8.4. Combined Developmental Test and Evaluation, Operational Test and Evaluation, and Live Fire Test and Evaluation Demonstrate System to Specified User Needs and Environmental Constraints

Verify and validate the integrated system against the specified operational requirements within the required operational environment(s) to ensure the system can satisfy operational expectations. The developmental and operational test environments and scenarios must be defined, and cost, schedule, and performance considerations must be continually addressed. This involves interoperability and interfaces for the system within any system of systems in which it operates. Any interface and interoperability issues for the system must be resolved for the system to achieve its interoperability certification in the next phase. Operational supportability should be confirmed at this time. In preparation for the Production Readiness Review, this step should confirm that the manufacturing processes are under control and that there are no significant manufacturing risks. Technical risk must be addressed, characterized, and mitigated.

4.3.3.9. Technical Reviews During System Demonstration

4.3.3.9.1. Test Readiness Review (TRR)

The TRR is a multi-disciplined technical review to ensure that the subsystem or system under review is ready to proceed into formal test. The TRR assesses test objectives, test methods and procedures, scope of tests, and safety and confirms that required test resources have been properly identified and coordinated to support planned tests. The TRR verifies the traceability of planned tests to program requirements and user needs. The TRR determines the completeness of test procedures and their compliance with test

plans and descriptions. The TRR assesses the system under review for development maturity, cost/ schedule effectiveness, and risk to determine readiness to proceed to formal testing. In addition to adequate planning and management, to be effective the program manager should follow-up with the outcomes of the TRR.

Test and evaluation is an integral part of the systems engineering processes of Verification and Validation. Test and evaluation should permeate the entire life cycle of an acquisition program.

Test and evaluation is also an important tool to identify and control risk.

This discussion principally addresses the TRR to support the readiness for a system to proceed into system-level Developmental Test. However, the program manager could utilize the TRR process to support all tests in all phases of an acquisition program, including testing within a system of systems context. A robust test program should enhance the program manager's ability to identify and manage risk. The program managers and Test and Evaluation Working-level Integrated Product Team should tailor any TRR to the specific acquisition phase, the specific planned tests, and the identified level of risk within the program. The scope of the review is directly related to the risk level associated with performing the planned tests and the importance of the test results to overall program success. The program manager should address the scope of the TRR(s) in the Systems Engineering Plan.

The level of specific risk and risk level will vary as a system proceeds from component level, to system level, to systems of systems level testing. Early component level test may not require the same level of review as the final system level tests. Sound judgment should dictate the scope of a specific test or series of tests.

Readiness to convene a TRR is predicated on the program manager's and Test and Evaluation Working-level Integrated Product Team's determination that preliminary testing, functional testing, and pre-qualification testing results form a satisfactory basis for proceeding with a TRR and subsequent initiation of formal, system-level Developmental Test.

As a practical matter, the program manager should carefully plan and properly resource test events.

Regardless of stage of development or the level of the testing (component, subsystem, or system), the basic tenets of this discussion about the TRR should apply.

The TRR should answer the following questions:

(1) Why are we testing? What is the purpose of the planned test? Does the planned test verify a requirement that is directly traceable back to a system specification or other program requirement?

(2) What are we testing (subsystem, system, system of systems, other)? Is the configuration of the system under test sufficiently mature, defined, and representative to accomplish planned test objectives and or support defined program objectives?

(3) Are we ready to begin testing? Have all planned preliminary, informal, functional, unit level, subsystem, system, and qualification tests been conducted, and are the results satisfactory?

(4) What is the expected result and how can/do the test results affect the program?

(5) Is the planned test properly resourced (people, test article or articles, facilities, data systems, support equipment, logistics, etc.)?

(6) What are the risks associated with the tests and how are they being mitigated?

(7) What is the fall-back plan should a technical issue or potential showstopper arise during testing?

Typical TRR success criteria include:

(1) Completed and approved test plans for the system under test;

(2) Completed identification and coordination of required test resources;

(3) The judgment that previous component, subsystem, and system test results form a satisfactory basis for proceeding into planned tests; and

(4) Identified risk level acceptable to the program leadership.

Test and evaluation is critical to evaluating the system. The TRR ensures that the testing to be conducted properly evaluates the system and that the system is ready to be tested.

4.3.3.9.2. System Verification Review (SVR)

The SVR is a multi-disciplined product and process assessment to ensure that the system under review can proceed into Low-Rate Initial Production and Full-Rate Production within cost (program budget), schedule (program schedule), risk, and other system constraints. Generally this review is an audit trail from the Critical Design Review. It assesses the system final product, as evidenced in its production configuration, and determines if it meets the functional requirements (derived from the Capability Development Document and draft Capability Production Document) documented in the Functional, Allocated, and Product Baselines. The SVR establishes and verifies final product performance. It provides inputs to the Capability Production Document. The SVR is often conducted concurrently with the Production Readiness Review. A Functional Configuration Audit may also be conducted concurrently with the SVR, if desired.

Typical SVR success criteria include affirmative answers to the following exit questions:

(1) Does the status of the technical effort and system indicate operational test success (operationally suitable and effective)?

(2) Can the system, as it exists, satisfy the Capability Development Document/draft Capability Production Document?

(3) Are adequate processes and metrics in place for the program to succeed?

(4) Are the risks known and manageable?

(5) Is the program schedule executable within the anticipated cost and technical risks?

(6) Are the system requirements understood to the level appropriate for this review?

(7) Is the program properly staffed?

(8) Is the program's Non Recurring Engineering requirement executable with the existing budget?

(9) Is the system producible within the production budget?

4.3.3.9.3. Production Readiness Review (PRR)

The PRR examines a program to determine if the design is ready for production and if the producer has accomplished adequate production planning. The review examines risk; it determines if production or production preparations incur unacceptable risks that might breach thresholds of schedule, performance, cost, or other established criteria. The review evaluates the full, production-configured system to determine if it correctly and completely implements all system requirements. The review determines whether the traceability of final system requirements to the final production system is maintained.

At this review, the Integrated Product Team should review the readiness of the manufacturing processes, the Quality Management System, and the production planning (i.e., facilities, tooling and test equipment capacity, personnel development and certification, process documentation, inventory management, supplier management, etc.). A successful review is predicated on the Integrated Product Team's determination that the system requirements are fully met in the final production configuration, and that production capability forms a satisfactory basis for proceeding into Low-Rate Initial Production and Full-Rate Production.

The program manager should convene a PRR of the prime contractor *and* major subcontractors, as applicable. The PRR(s) should be conducted in an iterative fashion, concurrently with other technical reviews, such as the System Functional Review, the Preliminary Design Review, and the Critical Design Review, during the System Development and Demonstration phase. Periodic production readiness assessments should be conducted during the System Demonstration work effort to identify and mitigate risks as the design progresses. The "*final*" PRR should occur at the completion of the System Development and Demonstration phase and the start of the Production and Deployment Phase. The final PRR should assess the manufacturing and quality risk as the program proceeds into Low-Rate Initial Production and Full-Rate Production.

The program manager should tailor the PRR to the technical scope and risk associated with the system. The program manager should address the PRR in the Systems Engineering Plan.

Typical PRR success criteria include affirmative answers to the following exit questions:

(1) Has the system product baseline been established and documented to enable hardware fabrication and software coding to proceed with proper configuration management?

(2) Are adequate processes and metrics in place for the program to succeed?

(3) Are the risks known and manageable?

(4) Is the program schedule executable (technical/cost risks)?

(5) Is the program properly staffed?

(6) Is the detailed design producible within the production budget?

A follow-on, tailored, PRR may be appropriate in the Production and Deployment phase for the prime contractor and major subcontractors if:

(1) Changes from the System Development and Demonstration phase and during the production stage of the design, in either materials or manufacturing processes, occur;

(2) Production start-up or re-start occurs after a significant shutdown period;

(3) Production start-up with a new contractor; or

(4) Relocation of a manufacturing site.

4.3.3.9.4. Technology Readiness Assessment (TRA)

The program manager should normally conduct a second TRA prior to Milestone C. The TRA may be held concurrently with other technical reviews, specifically System Requirements Review, Critical Design Review, System Verification Review, or Production Readiness Review. Completion of this TRA should provide:

(1) An evaluation of system technology maturity based on the Work Breakdown Structure;

(2) An objective scoring of the level of technological maturity; and

(3) Mitigation plans for achieving acceptable maturity prior to milestone decision dates.

4.3.3.10. Outputs of the Systems Engineering Processes in System Development and Demonstration

- Initial Product Baseline;
- Test Reports;
- Test and Evaluation Master Plan;
- Elements of Product Support;
- Risk Assessment;
- Systems Engineering Plan;
- Technology Readiness Assessment;
- Programmatic Environment, Safety, and Occupational Health Evaluation;
- Inputs to the Capability Production Document;
- Inputs to System Threat Assessment;

- Inputs to the Information Support Plan; and
- Inputs to Cost and Manpower Estimate;

4.3.4. Production and Deployment Phase

The Production and Deployment Phase commences at Milestone C and encompasses Operations and Support. During the Production and Deployment Phase, the system should achieve operational capability that satisfies mission needs.

Two work efforts, separated by the Full-Rate Production Decision Review, comprise the Production and Deployment Phase: Low-Rate Initial Production and Full-Rate Production and Deployment.

4.3.4.1. Purpose of Systems Engineering in Production and Deployment

As the integrated components develop into a system, the test and evaluation processes frequently reveal issues that require improvements or redesign. As the testing environment more closely approaches that of the users needs, the required improvements might be complex and/or subtle. The initial manufacturing process may also reveal issues that were not anticipated. It may be discovered that changing the product somewhat may provide enhancements in the manufacturing or other supporting processes. Low-Rate Initial Production should result in completion of manufacturing development. The systems engineering effort in Full-Rate Production and Deployment delivers the fully-funded quantity of systems and supporting materiel and services for the program or increment. During this effort, units attain Initial Operational Capability.

4.3.4.2. Inputs to the Systems Engineering Processes in Production and Deployment

- Test Results;
- Exit Criteria to leave the Production and Deployment phase and enter the Operations and Support phase;
- Acquisition Program Baseline;
- Capability Development Document and Capability Production Document;
- Systems Engineering Plan;
- Test and Evaluation Master Plan;
- Programmatic Environment, Safety, and Occupational Health Evaluation; and
- Product Support Package.

4.3.4.3. Key Systems Engineering Activities During Production and Deployment

Figure 4.3.4.3.1. illustrates the steps during the Production and Deployment phase. Some activities and reports are shown outside of the systems engineering V-shaped model that was used in describing the other phases. The following paragraphs, 4.3.4.3.1. through

4.3.4.3.3, contain further detail on each step. The Test Readiness Review and Physical Configuration Audit are covered in Sections 4.3.3.9.1 and 4.3.4.4.3, respectively.

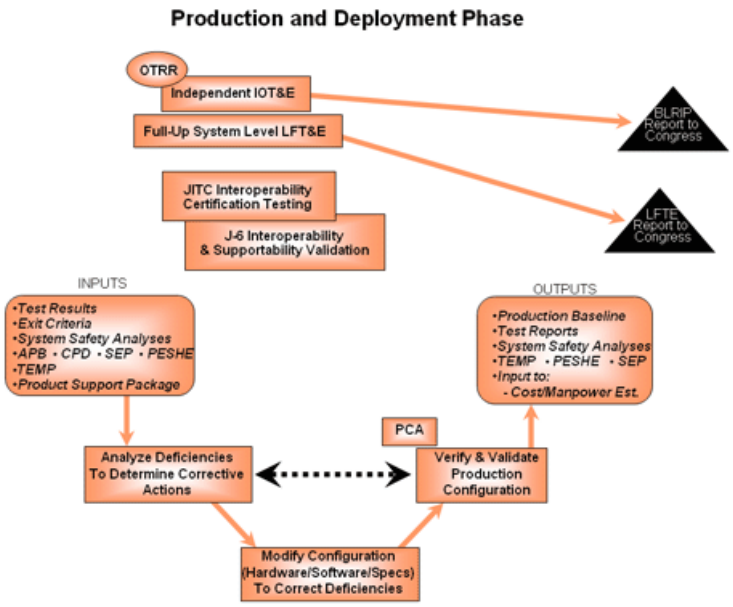

Figure 4.3.4.3.1. Systems Engineering Activities During Production and Deployment.

4.3.4.3.1. Analyze Deficiencies to Determine Corrective Actions

Using the aggregation of all inputs available at this stage of the program (test results, maintenance reports, exit criteria from System Development and Demonstration, Capability Production Document, Systems Engineering Plan, Test and Evaluation Master Plan, as well as associated support and maintenance concepts), known deficiencies are analyzed. A solution is proposed through the employment of Systems Engineering processes. A plan to build/modify/verify, and test the proposed solution is formulated and approved.

4.3.4.3.2. Modify Configuration (Hardware, Software, and Specifications) to Correct Deficiencies

The proposed solution to the deficiency is translated to the appropriate hardware/software or specification changes. Modifications are created, incorporated, and verified in accordance with the approved plan. This product change may include retrofit, since the

production process has begun. The impact on system cost, schedules, and performance should also be considered when addressing production incorporation.

4.3.4.3.3. Verify and Validate Production Configuration

The proposed solution to the system deficiency should be verified and tested. This process may require the spectrum from laboratory through full operational system testing. These test, analyze and fix activities may have to be repeated to resolve deficiencies or further improve the system solution. These approved changes should be incorporated into the final production configuration baseline.

4.3.4.4. Technical Reviews During Production and Deployment

4.3.4.4.1. Integrated Baseline Review (IBR)

The program manager may convene an additional IBR to support the Low-Rate Initial Production contract. Section 4.3.2.4.2. of this Guidebook discusses the systems engineering considerations associated with an IBR. Section 11.3.4. describes an IBR in detail. The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, in cooperation with industry has also prepared an IBR handbook.

Completion of IBR at this stage of the life cycle should result in the assessment of risk and the degree to which the six criteria described in 4.3.2.4.2 are met.

4.3.4.4.2. Operational Test Readiness Review (OTRR)

The program manager may conduct another TRR prior to Initial Operational Test and Evaluation. The OTRR is a multi-disciplined product and process assessment to ensure that the "production configuration" system can proceed into Initial Operational Test and Evaluation with a high probability of successfully completing the operational testing. Successful performance during operational test generally indicates that the system is suitable and effective for service introduction. The Full Rate Production Decision may hinge on this successful determination. The understanding of available system performance to meet the Capability Production Document is important to the OTRR. The OTRR is complete when the Service Acquisition Executive evaluates and determines materiel system readiness for Initial Operational Test and Evaluation.

4.3.4.4.3. Physical Configuration Audit (PCA)

The PCA is conducted around the time of the full rate production decision. The PCA examines the actual configuration of an item being produced. It verifies that the related design documentation matches the item as specified in the contract. In addition to the standard practice of assuring product verification, the PCA confirms that the manufacturing processes, quality control system, measurement and test equipment, and training are adequately planned, tracked, and controlled. The PCA validates many of the supporting processes used by the contractor in the production of the item and verifies other elements of the item that may have been impacted/redesigned after completion of the System Verification Review (SVR). A PCA is normally conducted when the government plans to control the detail design of the item it is acquiring via the Technical Data Package. When the government does not plan to exercise such control or purchase

the item's Technical Data Package (e.g., performance based procurement) the contractor should conduct an internal PCA to define the starting point for controlling the detail design of the item and establishing a product baseline. The PCA is complete when the design and manufacturing documentation match the item as specified in the contract. If the PCA was not conducted prior to the full rate production decision, it should be performed as soon as production systems are available.

4.3.4.5. Outputs of the Systems Engineering Processes in Production and Deployment

- Production Baseline;
- Test Reports;
- Test and Evaluation Master Plan;
- Risk Assessment;
- Programmatic Environment, Safety, and Occupational Health Evaluation;
- NEPA Compliance Schedule (as required);
- Systems Engineering Plan; and
- Inputs to Cost and Manpower Estimate

4.3.5. Operations and Support Phase

The objective of this phase is the execution of a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its total life cycle. When the system reaches the end of its useful life, the Department must dispose of it. These two work efforts, Sustainment and Disposal, comprise the Operations and Support Phase.

4.3.5.1. Purpose of Systems Engineering in Operations and Support

During the Sustainment effort of the Operations and Support Phase, systems engineering processes support in-service reviews, trade studies, and decision making on modifications, upgrades, and future increments of the system. Interoperability or technology improvements, parts or manufacturing obsolescence, aging aircraft (or system) issues, premature failures, changes in fuel or lubricants, Joint or service commonality, etc. may all indicate the need for a system upgrade(s).

System disposal is not a systems engineering activity. However, systems engineering processes that inject disposal requirements and considerations into the earlier design processes ultimately address and impact disposal.

4.3.5.2. Inputs to the Systems Engineering Processes in Operations and Support

- Service Use Data;
- User feedback;

- Failure reports;
- Discrepancy reports;
- Programmatic Environment, Safety, and Occupational Health Evaluation; and
- Systems Engineering Plan.

4.3.5.3. Key Systems Engineering Activities During Operations and Support

Figure 4.3.5.3.1. illustrates the steps during the Operations and Support phase. Further detail on each step is contained in paragraphs 4.3.5.3.1. through 4.3.5.3.7. Systems engineering should continue during operation and support of the system, and be used to continuously assess fielded system technical health against documented performance requirements and effectiveness, suitability, and risk measures. In-service systems engineering provides the program manager with an integrated technical assessment of system trends and sustainment alternatives, and then is used to oversee development and implementation of the selected alternative.

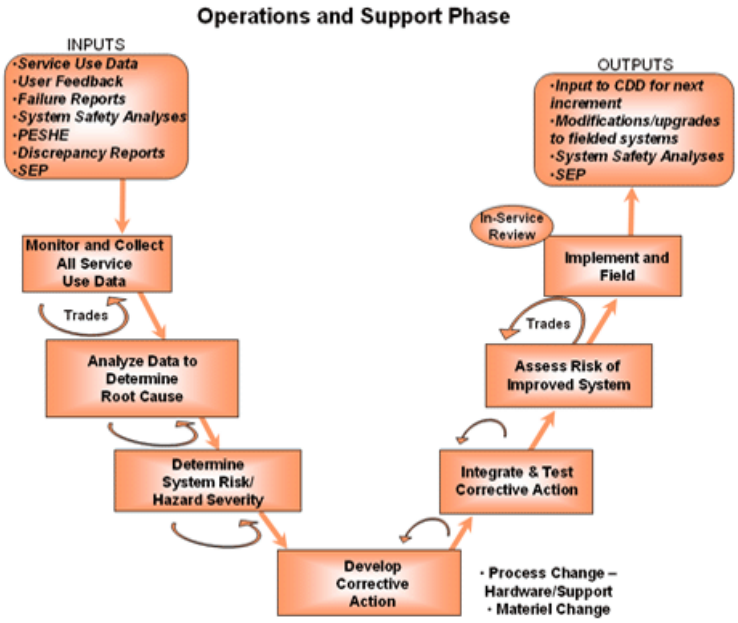

Figure 4.3.5.3.1. Systems Engineering Activities During Operations and Support.

4.3.5.3.1. Monitor and Collect All Service Use Data

The aggregation of all data inputs available at this stage of the program (service use data, maintenance discrepancy reports, user feedback, system/component failure reports, and the Systems Engineering Plan) provides the life cycle basis for many O&S decisions that will be made throughout the operational life of the system. Historically, many fielded systems remain in service much longer than originally planned. The type of data retrieved may change as the operational understanding of the system matures.

4.3.5.3.2. Analyze Data to Determine Root Cause of Problem

As problems arise in the fielded system, the systems engineering processes determine the cause of the problem and may lead to a solution. The retrieved data is key to this determination, and should be thoroughly analyzed for causes and potential solutions. These analyses may ascertain whether deficiencies exist in the system as designed/built, or whether the system has been operated differently, or in a different environment, than that for which it was designed.

4.3.5.3.3. Determine the System Risk/Hazard Severity

Risk assessment techniques and principles, as well as systems engineering processes, determine the hardware/software safety hazards and identify the readiness, program, and cost risks associated with the identified problems and/or deficiencies.

4.3.5.3.4. Develop Corrective Action

Corrective actions may include process, hardware, software, support, materiel, or maintenance changes. The systems engineering process is utilized to develop appropriate corrective actions.

4.3.5.3.5. Integrate and Test Corrective Action

Integrate the proposed corrective process, hardware, software, support, materiel, and/or maintenance changes; and methodically test the resultant prototype. Adequate testing (regression, durability, functional, interoperability, etc.) should be completed to ensure the proposed corrective action is suitable for fielding.

4.3.5.3.6. Assess Risk of Improved System

Once the functionality of the proposed corrective action is demonstrated, long-range system ramifications should be addressed. The appropriate systems engineering process is a risk assessment, which involves in-depth (regression, durability, structural, interoperability, support, etc.) system analyses. Additionally, the support, training, documentation, configuration control, and maintenance aspects of the improvements should be considered. All of these elements have an impact on system life cycle costs, which should be meticulously calculated in order to justify the required funding.

4.3.5.3.7. Implement and Field

The system corrective action/improvement may be authorized, implemented, and fielded once the correction/improvement is thoroughly understood and tested, and adequate supplies, support, training, and maintenance procedures are provided. Documentation

and configuration control should be thorough and meticulous. These data are utilized during periodic In-Service Reviews (ISRs) to document in-service health, operational system risk, system readiness, costs, trends, aging equipment and out of production issues.

4.3.5.4. Technical Reviews During Operations and Support

4.3.5.4.1. In-Service Review (ISR)

The ISR is a multi-disciplined product and process assessment to ensure that the system under review is operationally employed with well-understood and managed risk. This review is intended to characterize the in-service technical and operational health of the deployed system. It provides an assessment of risk, readiness, technical status, and trends in a measurable form. These assessments substantiate in-service support budget priorities. The consistent application of sound programmatic, systems engineering, and logistics management plans, processes, and sub-tier in-service stakeholder reviews will help achieve the ISR objectives. Example support groups include the System Safety Working Group and the Integrated Logistics Management Team. A good supporting method is the effective use of available government and commercial data sources. In-service safety and readiness issues are grouped by priority to form an integrated picture of in-service health, operational system risk, system readiness, and future in-service support requirements.

The ISR should provide:

(1) An overall System Hazard Risk Assessment;

(2) An operational readiness assessment in terms of system problems (hardware, software, and production discrepancies); and

(3) Status of current system problem (discrepancy) report inflow, resolution rate, trends, and updated metrics. The metrics may be used to prioritize budget requirements.

Successful completion of this review should provide the program manager and other stakeholders with the integrated information they need to establish priorities and to develop execution and out year budget requirements.

Typical success outcomes include:

(1) System problems have been categorized to support the O&S requirements determination process.

(2) Required budgets (in terms of work years) have been established to address all system problems in all priority categories.

(3) Current levels of System Operational Risk and System Readiness have been quantified and related to current O&S and procurement budgets.

(4) Future levels of System Operational Risk and System Readiness have been quantified and related to future year O&S and procurement budgets.

4.3.5.5. Outputs of the SE Processes in Operations and Support

- Input to Capability Development Document for next increment of the system;
- Modifications and upgrades to fielded systems;
- System Safety Analyses
- Programmatic Environment, Safety, and Occupational Health Evaluation;
- NEPA Compliance Schedule (as required); and
- Systems Engineering Plan.

4.3.6. Evolutionary Acquisition Programs

Programs with an evolutionary acquisition strategy undergo additional reviews (e.g., a MS B decision for each increment). The systems engineering activities and reviews are repeated as appropriate to ensure the same level of program insight is achieved within Evolutionary Acquisition Programs.

4.4. Systems Engineering Decisions: Important Design Considerations

The program manager faces a myriad of considerations and management tools to translate the user's desired capabilities (regardless of phase in the acquisition cycle) into a structured system of interrelated design specifications. This is clearly not a trivial task. It is an iterative task, performed within the framework of Systems Engineering to achieve the "best value" for the user.

The "best value" solution is not an easy solution to define. Many requirements and design considerations cannot fully coexist in a single design - hence, the need for rigorous systems engineering processes with trade offs. The systems engineering processes detailed in Section 4.2 and applied in each acquisition phase as detailed in Section 4.3 will enable the program manager to manage expectations of the user across the spectrum of requirements and design. The systems engineering management tools discussed in Section 4.5 give the program manager the methodology to examine the specific characteristics of his/her own program against a myriad of often-conflicting design considerations. This section discusses a number of these considerations and how they contribute to program performance. Each will have a different, "optimal" solution depending on the capabilities required of the program. Some "design considerations" will take the form of design constraints (e.g., weight, volume, power, cooling, etc.) that are derived requirements and need to be closely managed through a rigorous trades process. Some constraints may form system-wide budgets and require close tracking as the design matures. The challenge for the program manager is to apply systems engineering to achieve balance across all of the considerations and constraints.

The program manager should be aware that some considerations are mandated by law and others will be mandated by the user in the program's capability document. *These mandates must be preeminent in the program manager's design considerations balancing act.*

Figure 4.4.1. provides a framework for how these design considerations fit into an affordable systems operational effectiveness framework.

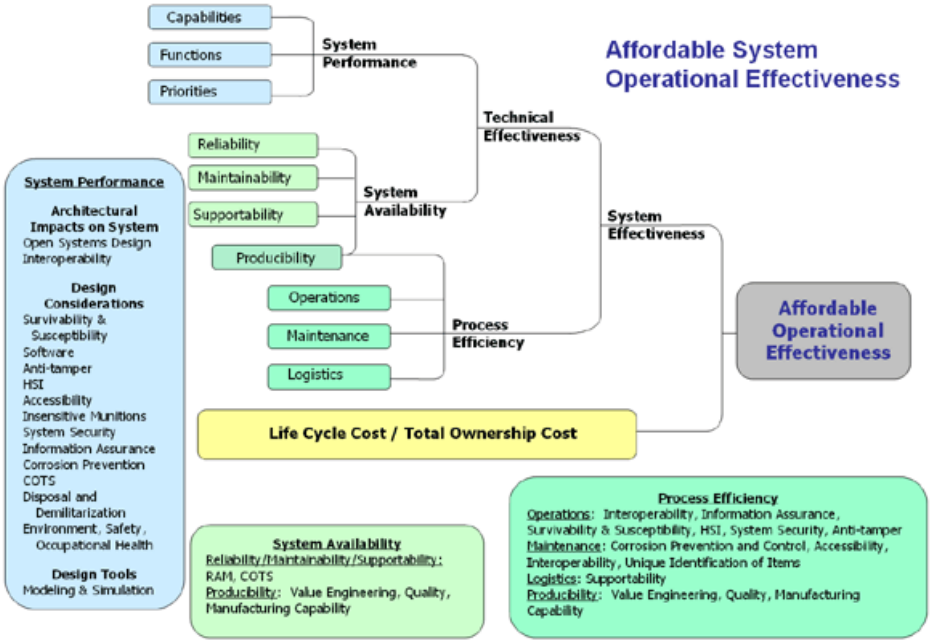

Figure 4.4.1. Affordable System Operational Effectiveness Diagram

4.4.1. Open Systems Design

An open system is a system that employs modular design tenets, uses widely supported and consensus-based standards for its key interfaces, and is subject to validation and verification tests to ensure the openness of its key interfaces. An open systems design is a design approach for developing an affordable and adaptable open system. It derives inputs from both the technical management processes and technical processes undertaken within the systems engineering and other Life-cycle processes, and in turn impacts these processes. The open systems design strategy should be implemented as part of the program's overall technical approach and must become an integral part of the program's SEP.

Program managers should employ an open systems design strategy only after careful analysis of required capabilities and strategies for technology development, acquisition, test and evaluation, and product support. They should also analyze the impacts of information assurance, systems safety and security, commercial, off-the-shelf availability, and other design considerations before finalizing their open systems design strategy. For example, programs should ensure that required capabilities lend themselves to the application of open systems design and do not impose premature design-specific solutions. Program managers should also evaluate the appropriateness of an open systems design in light of environmental constraints such as very high temperature, excessive

humidity, and safety and security needs of the system. The bottom line is that program managers should make a business case for using the open systems design through the application of trade studies, dynamic cost models, and market research aimed at analyzing technology and open standard trends and the degree of market support for needed technologies and standards.

Program managers should employ an open systems design strategy within the context of implementing their overall plan for Modular Open Systems Approach (MOSA) implementation. Within the MOSA context, programs should design their system based on adherence to the following five MOSA principles:

- **Establish an Enabling Environment.** This principle lays the foundation for successful implementation of subsequent principles. To adhere to this principle, the program manager must establish supportive requirements, business practices, and technology development, acquisition, test and evaluation, and product support strategies needed for effective development of open systems. Assigning responsibility for MOSA implementation, ensuring appropriate experience and training on MOSA, continuing market research, and proactive identification and overcoming of barriers or obstacles that can potentially slow down or even, in some cases, undermine effective MOSA implementation are among the supportive practices needed for creating an enabling MOSA environment.
- **Employ Modular Design.** Effective modular design is contingent upon adherence to four major modular design tenets. These tenets determine the degree to which modules are cohesive (contain well-focused and well-defined functionality); encapsulated (hide the internal workings of a module's behavior and its data); self-contained (do not constrain other modules); and highly binned (use broad modular definitions to enable commonality and reuse). By following these tenets, each module will be designed for change and the interface to each module is defined in such a way as to reveal as little as possible about its inner workings which facilitate the standardization of modular interfaces.
- **Designate Key Interfaces.** To effectively manage hundreds, and in some cases thousands, of interfaces that exist within and among systems, designers should group interfaces into key and non-key interfaces. Such distinction enables designers and configuration managers to distinguish among interfaces that exist between technologically stable and volatile modules, between highly reliable and more frequently failing modules, between modules that are essential for net-centricity and those that do not perform net-centric functions, and between modules that pass vital interoperability information and those with least interoperability impact.
- **Use Open Standards.** In order to take full advantage of modularity in design, interface standards must be well defined, mature, widely used, and readily available. Moreover, standards should be selected based on maturity, market acceptance, and allowance for future technology insertion. As a general rule, preference is given to the use of open interface standards first, the de facto interface standards second, and finally government and proprietary interface standards. Basing design strategies on widely supported open standards increases

the chance that future changes will be able to be integrated in a cost effective manner.

- **Certify Conformance.** Openness of systems is verified, validated, and ensured through rigorous and well-established assessment mechanisms, well-defined interface control and management, and proactive conformance testing. The program manager, in coordination with the user, should prepare validation and verification mechanisms such as conformance certification and test plans to ensure that the system and its component modules conform to the external and internal open interface standards allowing plug-and-play of modules, net-centric information exchange, and re-configuration of mission capability in response to new threats and evolving technologies. Open systems verification and validation must become an integral part of the overall organization change and configuration management processes. They should also ensure that the system components and selected commercial products avoid utilization of vendor-unique extensions to interface standards and can easily be substituted with similar components from competitive sources. Program managers should either use their own tool or preferably the MOSA PART developed by the Open Systems Joint Task Force to assess the compliance with open systems policies and ensure that their programs are properly positioned to reap the open systems benefits.

Adherence to these principles is needed to ensure access to the latest technologies and products, achieve interoperability, and facilitate affordable and supportable modernization of fielded assets. Such adherence is also needed to ensure delivery of technologically superior, sustainable and affordable increments of militarily useful capability within an evolutionary acquisition strategy context. For more information and detailed guidance on using MOSA and open systems design please see Chapter 2, Section 2.3.15. and review the Open Systems Joint Task Force detailed guidance.

4.4.2 . Interoperability

All acquisition programs are required to satisfactorily address interoperability and integration. These requirements span the complete acquisition life cycle for all acquisition programs. Interoperability and supportability of information technology (IT) and National Security System (NSS) acquisition programs, are required to comply with DoD Directive 4630.5, DoD Instruction 4630.8, CJCS Instruction 3170.01, CJCS Manual 3170.01, CJCSI 6212.01), Public Law 104-106 (1996), and 44 U.S.C. 3506.

4.4.3. Standardization

Standardization advances interoperability through commonality of systems, subsystems, components, equipment, data, and architectures. The program manager balances decisions to use standard systems, subsystems, and support equipment against specific capabilities (including corresponding information system elements that perform critical, essential, or support functions within each joint functional capability), technology growth, and cost effectiveness.

Program managers should consider compliance with international standardization agreements, such as the NATO Standardization Agreements, or the agreements of the Air

and Space Interoperability Council (formerly known as the Air Standards Coordinating Committee) or American-British-Canadian-Australian Armies Standardization Program. The program manager should identify any international standardization agreements or U.S. implementing documents that apply to the program early in the design process to ensure interoperability with combined and coalition systems and equipment.

4.4.4. Software

The following best practices for software systems also apply in general to any system:

- Viewing the software "content," particularly complex algorithms and functional flows, as enabling technologies requiring maturation and risk reduction prior to MS B;
- Developing architectural-based software systems that support open system concepts;
- Exploiting commercial, off-the-shelf (COTS) computer systems products;
- Allowing incremental improvements based on modular, reusable, extensible software;
- Identifying and exploiting, where practicable, Government and commercial software reuse opportunities before developing new software;
- Selecting the programming language in context of the systems and software engineering factors that influence system performance, overall Life-cycle costs, risks, and the potential for interoperability;
- Using DoD standard data and following data administrative policies in DoD Directive 8320.1;
- Selecting contractors with domain experience in developing comparable software systems; with successful past performance; and with a mature software development capability and process;
- Assessing information operations risks (see DoD Directive S-3600.1) using techniques such as independent expert reviews;
- Preparing for Lifecycle software support or maintenance by developing or acquiring the necessary documentation, host systems, test beds, and computer-aided software engineering tools consistent with planned support concepts;
- Preparing for Lifecycle software support or maintenance by planning for transition of fielded software to the support/maintenance activity; and
- Tracking COTS software purchases and maintenance licenses.

The program manager should structure a software development process to recognize that emerging capabilities and missions will require modification to software over the life cycle of the system. In order to deliver truly state-of-the-software, this process should allow for periodic software enhancements.

Additionally, the program manager should apply the following security considerations to software design and management (see DoD Directive 5000.1):

- A documented impact analysis statement, which addresses software reliability and accompanies modifications to existing DoD software;
- Formal software change control processes;
  - Software quality assurance personnel monitor the software change process;
  - An independent verification and validation team provides additional review;
- Analyze the technical risks and vulnerabilities of the software that could be exploited, and identify mitigation strategies;
- A change control process indicating whether foreign nationals, in any way, participated in software development, modification, or remediation;
- Each foreign national employed by contractors/subcontractors to develop, modify, or remediate software code specifically for DoD use has a security clearance commensurate with the level of the program in which the software is being used;

Primary vendors on DoD contracts that have subcontractors who employ cleared foreign nationals work only in a certified or accredited environment (DoD Instruction 5200.40);

- DoD software with coding done in foreign environments or by foreign nationals is reviewed for malicious code by software quality assurance personnel;
- When employing commercial, off-the-shelf (COTS) software, preference is given during product selection and evaluation to those vendors who can demonstrate that they took efforts to minimize the security risks associated with foreign nationals who developed, modified, or remediated the COTS software being offered; and
- Software quality assurance personnel review software sent to locations not directly controlled by the DoD or its contractors for malicious code when it is returned to the DoD contractor's facilities.

4.4.5. Commercial-off-the-Shelf Items (COTS)

Use of commercial items offers significant opportunities for reduced development time, faster insertion of new technology, and lower life cycle costs, owing to a more robust industrial base. Maximum use of mature technology provides the greatest opportunity to hold fast to program cost, schedule, and performance requirements and is consistent with an evolutionary acquisition strategy. However, no matter how much of a system is provided by commercial items, the program manager still should engineer, develop, integrate, test, evaluate, deliver, sustain, and manage the overall system. Particular attention should be paid to the intended usage environment and understanding the extent to which this differs from (or is similar to) the commercial usage environment; subtle differences in usage can have significant impact on system safety, reliability, and durability.

When acquiring COTS software products or other commercial items, the program manager still implements systems engineering processes. In this context, integration encompasses the amalgamation of multiple COTS components into one deployable system or the assimilation of a single COTS product (such as an enterprise resource

planning system). In either case, the program manager should ensure that the system co-evolves with essential changes to doctrine (for combat systems) or reengineered business processes (for combat support and information technology systems) and apply commercial item best practices in the following areas:

- Adapting to commercial business practices;
- COTS evaluation;
- Relationship with vendors;
- Life-cycle planning; and
- Test and evaluation of COTS items.

Adapting to Commercial Business Practices. When purchasing a commercial item, the program manager should adopt commercial business practice(s). The extent to which the DoD business practices match the business practices supported by commercial items determines the likelihood that the items will meet DoD needs, yet still realize the intended cost savings. It is likely, however, that a gap will exist, and the gap may be large. Negotiation, flexibility, and communication on the part of the stakeholders, the commercial vendors, and the program manager are required.

COTS Evaluation. The program manager should plan for and implement evaluations to assist in fully identifying commercial capabilities, to choose between alternate architectures and designs, to determine whether new releases continue to meet requirements, and to ensure that the commercial items function as expected when linked to other system components. In addition, evaluation provides the critical source of information about the trade studies that should be made between the capabilities of the system to be fielded and the system architecture and design that makes best use of commercial capabilities. Evaluating commercial items requires a focus on mission accomplishment and matching the commercial item to system requirements.

For COTS software, program managers are encouraged to use code-scanning tools, within the scope and limitations of the licensing agreements, to ensure both COTS and Government off-the-shelf software do not pose any information assurance or security risks. Section 7.10 of this Guidebook discusses the considerations for COTS software solutions.

For COTS devices that use the electromagnetic spectrum (e.g., spectrum-dependent), program managers should be aware that COTS devices that are authorized to operate within the United States and Its Possessions are not automatically authorized to operate in foreign countries outside the United States and Its Possessions. Examples of such COTS devices include radio frequency identification systems, wireless local-area-networks, baby monitors, and garage door openers. Chapter 7 lists the policy documents relating to electromagnetic spectrum management and describes the procedures for obtaining spectrum supportability.

Life-Cycle Planning. The program manager should establish a rigorous change management process for life-cycle support. Systems that integrate multiple commercial items require extensive engineering to facilitate the insertion of planned new commercial technology. This is not a "one time" activity because unanticipated changes may drive

reconsideration of engineering decisions throughout the life of the program. Failure to address changes in commercial items and the marketplace will potentially result in a system that cannot be maintained as vendors drop support for obsolete commercial items.

Relationship with Vendors. The program manager needs to remain aware of and influence product enhancements with key commercial item vendors to the extent practical and in compliance with Federal Advisory Committee Act. As vendors are different from contractors and subcontractors, different practices and relationships are needed. Vendors react to the marketplace, not the unique needs of DoD programs. To successfully work with vendors, the program manager may need to adopt practices and expectations that are similar to other buyers in the marketplace. Traditional DoD acquisition and business models are not sufficient for programs acquiring commercial items, as they do not take into account the marketplace factors that motivate vendors.

T&E of COTS Items. The program manager should develop an appropriate test and evaluation strategy for commercial items to include evaluating potential commercial items in a system test bed, when practical; focusing test beds on high-risk items; and testing commercial-item upgrades for unanticipated side effects in areas such as security, safety, reliability, and performance. It is essential to integrate this test strategy with Life-cycle planning as described above.

4.4.6. Manufacturing Capability

4.4.6.1. Producibility

Producibility is the degree to which the design of the system facilitates the timely, affordable, and optimum-quality manufacture, assembly, and delivery of the system to the customer and should be a development priority. Design engineering efforts concurrently develop producible and testable designs, capable manufacturing processes, and the necessary process controls to satisfy requirements and minimize manufacturing costs. The program manager should use existing manufacturing processes whenever possible. When the design requires new manufacturing capabilities, the program manager needs to consider process flexibility (e.g., rate and configuration insensitivity).

Full rate production of a system necessitates a stable design, proven manufacturing processes, and available or programmed production facilities and equipment.

4.4.6.2. Manufacturing Readiness Levels

Engineering and Manufacturing Readiness Levels are a means of communicating the degree to which a technology is producible, reliable, and affordable. Their use is consistent with efforts to include the consideration of engineering, manufacturing, and sustainment issues early in a program. More information can be found in the Manager's Guide to Technology Transition in an Evolutionary Acquisition Environment. Application of EMRLs should be tightly integrated with the technical reviews detailed in Section 4.3.

4.4.7. Quality

The quality of products or services is determined by the extent they meet (or exceed) requirements and satisfy the customer(s), at an affordable cost. Quality is a composite of material attributes, including performance and product/service features and characteristics that satisfy a customer's requirement. A key to success is to incorporate systems engineer/design quality into the product by defining the product or service quality requirements from the beginning and then providing the contractor with the maximum degree of flexibility to meet these requirements.

The contractor is responsible for the quality of its products. The program manager should allow contractors to define and use their preferred quality management system that meets required program support capabilities. International quality standards ISO 9001-2000, *Quality Management Systems - Requirements*, or AS 9100:2001, *Quality Management Systems - Aerospace Requirements*, define process-based quality management systems and are acceptable for use on contracts for complex or critical items per FAR 46.202-4, Higher-Level Contract Quality Requirements.

A contractor's quality management system should be capable of the following key activities:

- Monitor, measure, analyze, control, and improve processes;
- Reduce product variation;
- Measure/verify product conformity;
- Establish mechanisms for field product performance feedback; and
- Implement an effective root-cause analysis and corrective action system.

Many companies pursue quality registration of their quality management systems as a goal in itself, rather than setting continuous quality improvement as a goal or using their quality management systems to help develop capable processes. There have been instances where a supplier has been ISO 9001 registered, and the supplier’s product was deficient or life threatening. The program manager will not require ISO registration of a supplier’s quality program. ISO compliance is just one means that a program manager uses to distinguish between multiple bidders. Past performance is another example. Contractors who apply Six Sigma tools and achieve reduced variation in their production processes could be analyzed for oversight reduction.

4.4.8. Reliability, Availability, and Maintainability (RAM)

The program manager should establish RAM objectives early in the acquisition cycle and address them as a design parameter throughout the acquisition process. The program manager develops RAM system requirements based on the Initial Capabilities Document or Capability Development Document and total ownership cost (TOC) considerations, and states them in quantifiable, operational terms, measurable during DT&E and OT&E. RAM system requirements address all elements of the system, including support and training equipment, technical manuals, spare parts, and tools. These requirements are derived from and support the user's system readiness objectives. Reliability requirements address mission reliability and logistics reliability. The former addresses the probability of carrying out a mission without a mission-critical failure. The latter is the ability of a system to perform as designed in an operational environment over time without any

failures. Availability requirements address the readiness of the system. Availability is a function of the ability of the system to perform without failure (reliability) and to be quickly restored to service (a function of both maintainability and the level and accessibility of support resources). Maintainability requirements address the ease and efficiency with which servicing and preventive and corrective maintenance can be conducted; i.e., the ability of a system to be repaired and restored to service when maintenance is conducted by personnel of specified skill levels and prescribed procedures and resources.

Application of RAM and producibility activities during design, development, and sustainment is guided by a concise understanding of the concept of operations, mission profiles (functional and environmental), and desired capabilities. These are, in turn, invaluable to understanding the rationale behind RAM and producibility activities and performance priorities and paves the way for decisions about necessary trade studies between system performance, availability, and system cost, with impact on the cost effectiveness of system operation, maintenance, and logistics support. The focus on RAM should be complemented by emphasis on system manufacturing and assembly, both critical factors related to the production and manufacturing, and to the sustainment cost of complex systems.

The program manager plans and executes RAM design, manufacturing development, and test activities so that the system elements, including software, that are used to demonstrate system performance before the production decision reflect a mature design. IOT&E uses production representative systems, actual operational procedures, and personnel with representative skill levels. To reduce testing costs, the program manager should utilize M&S in the demonstration of RAM requirements, wherever appropriate. (See DoD 3235.1-H.)

An additional challenge associated with RAM is the stochastic nature of the performance parameter. Typically, a large proportion of system requirements is deterministic and can be easily and repeatedly measured; e.g., the weight of an item is easily measured and can be repeated on a consistent basis. By contrast, a test of the reliability of an item is an evaluation of a sample, from which the population performance is inferred. The item may be performing to its average reliability requirement as specified, but the sample may return a higher or lower value. Repeated or more extensive samples would provide greater information about the underlying performance. The true reliability of the item is never really known until the item has completed its service. Until that point, the performance may be sampled, and confidence bounds determined for the population performance. Development of RAM requirements and the associated demonstration methods need to consider the stochastic nature of these parameters. Additional RAM guidance can be found in the DoD RAM Guide and in the Reliability and Maintainability Continuous Learning Module (CLM) at https://learn.dau.mil/html/clc/Clc.jsp and then click on CLE301.

4.4.9. Supportability

The program manager should conduct supportability activities throughout the system life cycle. When using an evolutionary acquisition strategy, supportability activities address performance and support requirements for both the total life cycle of the system and for

each capability increment, and consider and mitigate the impact of system variants or variations. The supportability of the design(s) and the acquisition of systems should be cost-effective and provide the necessary infrastructure support to achieve peacetime and wartime readiness requirements. Supportability considerations are integral to all trade-off decisions, as required in DoDD 5000.1, E1.29:

> *PMs shall consider supportability, life cycle costs, performance, and schedule comparable in making program decisions. Planning for Operation and Support and the estimation of total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system life cycle.*

Supportability is the inherent quality of a system - including design for reliability and maintainability, technical support data, and maintenance procedures - to facilitate detection, isolation, and timely repair/replacement of system anomalies. This includes factors such as diagnostics, prognostics, real-time maintenance data collection, 'design for support' and 'support the design' aspects, corrosion protection and mitigation, reduced logistics footprint, and other factors that contribute to optimum environment for developing and sustaining a stable, operational system. To minimize the logistics footprint, the supportability posture of defense systems should be designed-in. The "footprint problem" has an engineering solution.

4.4.9.1. Supportability Analyses

The program manager conducts supportability analyses as an integral part of the systems engineering process throughout the system life cycle. The results of these analyses form the basis for the related design requirements included in the system performance specification and in the documentation of logistics support planning. The results also support subsequent decisions to achieve cost-effective support throughout the system life cycle. For systems, this includes all increments of new procurements and major modifications and upgrades, as well as reprocurement of systems, subsystems, components, spares, and services that are procured beyond the initial production contract award. The program manager should permit broad flexibility in contractor proposals to achieve program supportability objectives.

4.4.9.2. Support Concepts

The program manager establishes logistics support concepts (e.g., organic, two-level, three-level, contractor, partnering) early in the program, and refines the concepts throughout program development. Total ownership cost plays a key role in the overall selection process. Support concepts for all systems provide cost effective, total-life-cycle, logistics support.

Support concepts include the following:

- Embedded Diagnostics and Prognostics;
- Embedded Training and Testing;
- Serialized Item Management;
- Automatic Identification Technology;

- Iterative Technology Refreshment;
- Data Syntax and Semantics; and
- Unique Identification.

4.4.9.3. Support Data

Contract requirements for deliverable support and support-related data should be consistent with the planned support concept and represent the minimum essential requirements to cost-effectively maintain the fielded system and foster source of support competition throughout the life of the fielded system. The program manager coordinates Government requirements for these data across program functional specialties to minimize redundant contract deliverables and inconsistencies.

4.4.9.4. Support Resources

The support resources needed, for both the total system over its expected life and for each increment of introduced capability, are inherent to "full fundin" calculations. Therefore, support resource requirements are a key element of program reviews and decision meetings. During program planning and execution, logistics support products and services are competitively sourced. The program manager should consider embedded training and maintenance techniques to enhance user capability and reduce Lifecycle costs.

The program manager generally uses automatic test system (ATS) families or COTS components that meet defined ATS capabilities to meet all acquisition needs for automatic test equipment hardware and software. Critical hardware and software elements define ATS capabilities. The program manager considers diagnostic, prognostic, system health management, and automatic identification technologies and bases ATS selection on a cost and benefit analysis over the complete system life cycle. Consequently, the program manager is seeking to minimize the introduction of unique types of ATS into the DoD field, depot, and manufacturing operations.

4.4.10.Human Systems Integration (HSI)

Per DoD Directive 5000.1, the program manager shall apply HSI to optimize total system performance and minimize total ownership cost. To do this, the program manager shall work with the manpower, personnel, training, safety, and occupational health, habitability, survivability, and human factors engineering (HFE) communities to translate and integrate the HSI thresholds and objectives contained in the capabilities documents into quantifiable and measurable system requirements (see DoD Instruction 5000.2). The program manager then includes these requirements in specifications, the Test and Evaluation Master Plan (TEMP), and other program documentation, as appropriate, and uses them to address HSI in the statement of work and contract. The program manager identifies any HSI-related schedule or cost issues that could adversely impact program execution; the system's support strategy should identify responsibilities, describe the technical and management approach for meeting HSI requirements, and summarize major elements of the associated training system (see 6.4.5.2.1.). See also MIL STD 1472F, Human Engineering. HSI topics include:

- Human Factors Engineering (DoD Instruction 5000.2 and Guidebook section 6.3);
- Habitability and Personnel Survivability (DoD Instruction 5000.2 and Guidebook sections 4.4.12, 6.2.6, 6.2.7.);
- Manpower Initiatives (DoD Instruction 5000.2 and Guidebook section 6.2.1);
- Personnel Initiatives (DoD Instruction 5000.2 and Guidebook section 6.2.2); and
- Training (DoD Instruction 5000.2, DoD Directive 1430.13, *Training Simulators and Devices*, and Guidebook section 6.2.3).

4.4.11.Environment, Safety and Occupational Health (ESOH)

As part of the program's overall cost, schedule, and performance risk reduction, the program manager shall prevent ESOH hazards, where possible, and manage ESOH hazards where they cannot be avoided (see 6.2.4.1, 6.2.5.2., and 6.2.5.3.). More specifically, DoD Instruction 5000.2 establishes requirements for program managers to manage ESOH risks for their system's life cycle. The program manager is required to have a PESHE document at MS B (or Program Initiation for ships) that describes

- The strategy for integrating ESOH considerations into the systems engineering risk management process using the methodologies described in the government-industry standard, *Standard Practice for System Safety,* MIL-STD-882D;
- The schedule for completing the National Environmental Policy Act (NEPA) (42 U.S.C. 4321-4370d) and Executive Order 12114 documentation;
- The status of ESOH risk management. The Acquisition Strategy, includes a summary of the PESHE;
- From MS B on, the PESHE document serves as a repository for top-level management information on ESOH risk; and
- Identification, assessment, mitigation, residual risk acceptance, and on-going evaluations of mitigation effectiveness and on NEPA compliance.

The ESOH systems engineering activities are described in further detail in the following sections:

- Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE);
- ESOH Risk Management; and
- Review and update Designated Science and Technology Information, the Security Classification Guide, and the Counterintelligence Support Plan.

Additional detailed guidance, processes and tools are available at the ESOH Special Interest Area on the Acquisition Community Connection web site, and at the DAU-hosted System Safety in Systems Engineering continuous learning module at https:learn.dau.mil/html/clc/Clc.jsp (click on CLE009).

4.4.11.1. Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE)

There is no specific format for the PESHE. The program manager documents the PESHE in whatever manner is most useful to the program and best communicates to decision makers what Environment, Safety, and Occupational Health (ESOH) issues affect the program. The PESHE transitions from an initial planning document at Milestone B into an ESOH risk management tool as the program matures.

The PESHE includes the following:

- Strategy for integrating ESOH considerations into the systems engineering process;
- Identification of who is responsible for implementing the ESOH strategy;
- Approach to identifying ESOH risks, reducing or eliminating the risks, and implementing controls for managing those ESOH risks where the program cannot avoid them;
- Identification, assessment, mitigation, and acceptance of ESOH risks. DoD Instruction 5000.2, E7.7 establishes the acceptance authorities for residual risks as: the DoD Component Acquisition Executive for high risks, the Program Executive Office-level for serious risks, and the program manager for medium and low risks as defined in MIL-STD-882D;
- Method for tracking progress in the management and mitigation of ESOH risks and for measuring the effectiveness of ESOH risk controls;
- Compliance schedule for completing National Environmental Policy Act (NEPA)/ Executive Order 12114 documentation;
- Identification of hazardous materials (HAZMAT), including energetics, used in the system;
- Approach for, and progress in, integrating HAZMAT, energetics, and other ESOH considerations (e.g., environmental impacts, personnel safety, regulatory compliance) into system demilitarization and disposal planning (see 4.4.14); and
- Approach for, and progress in, integrating ESOH into test and evaluation (T&E) planning and reporting.

DoD Instruction 5000.2 does not require that the PESHE supersede or replace other ESOH plans, analyses, and reports (e.g., System Safety Management Plan/Assessments, HAZMAT Management Plan, Pollution Prevention Plan, Health Hazard Assessments, etc.); the program manager incorporates these documents by reference, as appropriate. However, to the maximum extent possible, the program manager should minimize duplication of effort and documentation and give preference to recording ESOH information in the PESHE, as opposed to maintaining a series of overlapping, redundant documents. Human Systems Integration also addresses many of the safety and health ESOH areas. The PESHE describes the linkage between ESOH and HSI and how the program avoids duplication of effort.

The required compliance schedule for completing NEPA/E.O. 12114 documentation, as detailed in the PESHE and summarized in the Acquisition Strategy, includes the following:

- Events or proposed actions (to include T&E and fielding/basing activities) throughout the life cycle of the program that may require preparation of formal NEPA documentation;
- Proponent for each proposed action having the lead to prepare the formal NEPA documentation;
- The anticipated initiation date for each proposed action;
- The anticipated type of NEPA/E.O. 12114 document (e.g., Categorical Exclusion, Environmental Assessment and Finding of No Significant Impact, or Environmental Impact Statement and Record of Decision) which the proponent should complete prior to the proposed action start date;
- The anticipated start and completion dates for the final NEPA/E.O. 12114 document; and
- The specific approval authority for the documents. DoD Instruction 5000.2, E7.7 establishes the DoD Component Acquisition Executive or designee (for joint programs, the DoD Component Acquisition Executive of the Lead Executive DoD Component) as the approval authority for system-related NEPA/E.O. 12114 documentation.

Networks and automated system programs, including those using commercial, off-the-shelf solutions, are not exempt from the statutory and regulatory requirements (discussed above) to manage ESOH considerations as part of the systems engineering process. These systems are required to document those management efforts in a PESHE. The Automated Information System program manager should perform the ESOH analyses appropriate for the scope of the acquisition program (e.g., software; acquisition of hardware; installation of facilities, fiber optic cables, radio antennae, etc.). Automated Information System Programs that primarily deal with new or modified software applications should focus the PESHE on software system safety processes, procedures, and results. The PESHE for an Automated Information System Program that also involves hardware and/or facilities should also address ESOH considerations such as man-machine interface, identification of hazardous materials, preparation of required NEPA documentation, demilitarization planning, and disposal in accordance with hazardous waste laws and regulations.

4.4.11.2. Environment, Safety, and Occupational Health (ESOH) Risk Management

Balancing the elimination or reduction of ESOH risk with an informed and structured residual risk acceptance process is essential for positively contributing to a program's efforts in meeting cost, schedule, and performance requirements. ESOH risks are part of each program's overall cost, schedule, and performance risks, and the program manager should review them from within that overall context. Risk acceptance and implementation of effective mitigating measures/controls is necessary to avoid loss of life or serious injury to personnel; serious damage to facilities or equipment resulting in large dollar loss; failures with adverse impact on mission capability, mission operability, or public opinion; and harm to the environment and the surrounding community.

The ESOH risk management process uses ESOH risk analysis matrices, based on the guidance in MIL STD 882D. The risk matrices should use clearly defined probability and severity criteria (either qualitative or quantitative) to categorize ESOH risks. Program managers elect to either establish a single consolidated ESOH risk matrix or use individual environmental, safety, and occupational health matrices.

The three basic types of ESOH risks are

- Potential ESOH impacts and adverse effects from routine system development, testing, training, operation, sustainment, maintenance, and demilitarization/disposal;
- Potential ESOH and mission readiness impacts from system failures or mishaps, including critical software failures; and
- Potential impacts to program Lifecycle cost, schedule, and performance from ESOH compliance requirements.

The scope of potential risks includes all ESOH regulatory compliance requirements associated with the system throughout its life cycle, such as, but not limited to, the following:

- HAZMAT use and hazardous waste generation;
- Demilitarization and disposal requirements;
- Safety (including explosives safety, ionizing and non-ionizing radiation);
- Human health (associated with exposure to chemical, physical, biological, or ergonomic hazards, etc.);
- Environmental and occupational noise; and
- Impacts to the natural environment (e.g., air, water, soil, flora, fauna).

ESOH risk information should include the following:

- Description of the risk/hazard;
- Preliminary risk assessment;
- Necessary mitigation measures to eliminate or reduce the risk;
- Residual risk assessment;
- Residual risk acceptance document; and
- Mitigation measure effectiveness.

Programs begin the process of identifying ESOH risks using lessons learned from the following sources of information:

- Legacy systems that the new system will replace, to include mishap and lost time rates associated with any legacy system;
- Similar systems;
- Pre-system acquisition activities (e.g., the Technology Development Strategy);

- Demilitarization and disposal of similar systems; and
- ESOH regulatory issues at potential locations for system testing, training, and fielding/basing.

In addition to standard ESOH risk management data, HAZMAT (to include energetics) risk information includes:

- The locations and quantities of HAZMAT on the system, where applicable;
- Energetic qualification information for each energetic material used in the system;
- Reasonably anticipated hazardous byproducts/discharges and expected quantities of hazardous waste generated during normal use/maintenance, in addition to those anticipated in emergency situations (e.g., exhaust, fibers from composite materials released during accidents, etc.); and
- Special HAZMAT training and handling.

The preferred mitigation strategy is source reduction or elimination of the hazards, also referred to as pollution prevention when dealing with potential environmental impacts. The program manager should strive to eliminate or reduce ESOH risks as part of the system's total Lifecycle risk reduction strategy. For systems containing energetics, source reduction consists of minimizing the use of the energetic materials and developing system designs that reduce the possibility and consequences of an explosive mishap. This includes complying with the insensitive munitions criteria (per DoD Directive 5000.1) and pursuing hazard classifications and unexploded ordnance liabilities that minimize total ownership cost (see section 4.4.16).

If effectively executed, ESOH risk management sets the stage for addressing National Environmental Policy Act (NEPA)/Executive Order 12114 requirements by identifying system-specific ESOH risk information. The program manager combines these data with the geographic/site specific environmental conditions and requirements, to prepare formal NEPA analysis documents. In addition, the program manager is responsible to provide system specific ESOH risk data in support of NEPA analysis by other action proponents. This approach streamlines the overall NEPA/E.O. 12114 analysis process, reducing cost and schedule impacts. The program manager should integrate into the ESOH risk management data any additional ESOH risks or additional mitigation measures identified during the formal NEPA/E.O. 12114 analysis process.

The program manager should monitor and assess the effectiveness of mitigation measures (i.e., tracking ESOH progress in terms of regulatory compliance) to determine whether additional control actions are required. The program manager then documents the effectiveness of mitigation measures in the PESHE. Relevant information can include any related mishap data, adverse health effects, and significant environmental impacts from system development, testing, training, operation, sustainment, maintenance, and demilitarization/disposal. Programs can also convey information about the effectiveness of their risk management efforts with metrics, achievements, success stories, etc.

4.4.11.3. Networks and Automated Information System ESOH Management

As noted in Table E3.T1 and paragraph E7.1.6 of DoDI 5000.2, networks and automated system programs, including those using COTS solutions, are not exempt from the DoD 5000 requirements to manage ESOH considerations as part of the systems engineering process and are required to document those efforts in a PESHE. The AIS PM should perform the ESOH analyses appropriate for the scope of the acquisition program (e.g., software; acquisition of hardware; installation of facilities, fiber optic cables, radio antennae, etc.). AIS programs that primarily deal with new or modified software applications should focus the PESHE on software system safety processes, procedures, and results. The PESHE for an AIS program that also involves hardware and/or facilities should also address ESOH considerations such as man-machine interface, identification of hazardous materials, preparation of required NEPA documentation, demilitarization planning, and disposal in accordance with hazardous waste laws and regulations.

4.4.12. Survivability and Susceptibility

The program manager should fully assess system and crew survivability against all anticipated threats at all levels of conflict early in the program, but in no case later than entering System Demonstration and Demonstration. This assessment also considers fratricide and detection. If the system or program has been designated by the Director, Operational Test and Evaluation (DOT&E), for Live Fire Test and Evaluation (LFT&E) oversight, the program manager should integrate the test and evaluation (T&E) used to address crew survivability issues into the LFT&E program supporting the Secretary of Defense LFT&E Report to Congress.

The program manager should address Nuclear, Biological and Chemical and High Altitude Electromagnetic Pulse cost-effective survivability techniques and plan for the validation and confirmation of NBC and HEMP survivability.

The program manager should establish and maintain a survivability program throughout the system life cycle to attain overall program objectives. The program should stress early investment in survivability enhancement efforts that improve system operational readiness and mission effectiveness by:

- Providing threat avoidance capabilities (low susceptibility);
- Incorporating hardening and threat tolerance features in system design (low vulnerability);
- Providing design features to reduce personnel casualties resulting from damage to or loss of the aircraft (casualty reduction);
- Maximizing wartime availability and sortie rates via operationally compatible threat damage tolerance and rapid reconstitution (reparability) features;
- Minimizing survivability program impact on overall program cost and schedule; and
- Ensuring protection countermeasures and systems security applications are defined for critical component's vulnerability to validated threats for systems survivability, including conventional or nuclear advanced technology weapons; nuclear, biological, or chemical contamination; and electronic warfare threats.

Unless waived by the Milestone Decision Authority, mission-critical systems, including crew, regardless of acquisition category, should be survivable to the threat levels anticipated in their projected operating environment as portrayed in the System Threat Assessment. Design and testing ensure that the system and crew can withstand man-made hostile environments without the crew suffering acute chronic illness, disability, or death.

The program manager should ensure that system susceptibility is addressed as a design consideration. Electromagnetic compatibility (EMC) and electromagnetic interference (EMI) should be addressed against the planned operational environment and the effects they may have on the system. Additionally, EMC/EMI should be a consideration within the system to understand unintended electromagnetic coupling across and among system components under various operational and maintenance scenarios. MIL-STD-461 or similar procedures can provide a basis for the technical design and certification approach for EMC/EMI. Section 7.6 contains additional detail about spectrum management considerations.

4.4.13. Corrosion Prevention and Control

The program manager should consider and implement corrosion prevention and mitigation planning to minimize the impact of corrosion and material deterioration throughout the system life cycle (see the Corrosion Prevention and Control Planning Guidebook). Corrosion prevention and mitigation methods include, but are not limited to, the use of effective design practices, material selection, protective finishes, production processes, packaging, storage environments, protection during shipment, and maintenance procedures. The program manager establishes and maintains a corrosion prevention and mitigation reporting system for data collection and feedback and uses it to adequately address corrosion prevention and mitigation logistic considerations and readiness issues. Corrosion prevention and mitigation considerations are integral to all trade-off decisions for Performance Based Logistics (see section 5.3.) as required in DoD Directive 5000.1:

> *<u>Performance-Based Logistics.</u> PMs shall develop and implement performance-based logistics strategies that optimize total system availability while minimizing cost and logistics footprint. Trade-off decisions involving cost, useful service, and effectiveness shall consider corrosion prevention and mitigation. Sustainment strategies shall include the best use of public and private sector capabilities through government/industry partnering initiatives, in accordance with statutory requirements.*

4.4.14.Disposal and Demilitarization

During systems engineering as part of the program manager's Total Life Cycle Systems Management responsibilities, the program manager should consider materiel demilitarization and disposal. The program manager should coordinate with DoD Component logistics and explosive safety activities and the Defense Logistics Agency, as appropriate, to identify and apply applicable demilitarization requirements necessary to eliminate the functional or military capabilities of assets (DoD 4140.1-R and DoD

4160.21-M-1) and to determine reutilization and hazardous-property disposal requirements for system equipment and by-products (DoD 4160.21-M).

For a munitions program, the program manager shall document the parts of the system that will require demilitarization and disposal and address the inherent dangers associated with ammunition and explosives (DoD Instruction 5000.2). This documentation should be in place before the start of developmental test and evaluation and before the program manager releases munitions or explosives to a non-military setting. The documentation provides the following:

- Render safe step-by-step procedures for disassembling the munitions item(s) to the point necessary to gain access to or to remove the energetic and hazardous materials; and
- Identification of all energetics and hazardous material, and the associated waste streams produced by the preferred demilitarization/disposition process.

Open burn and open detonation are not to be considered as the primary methods of demilitarization or disposal.

4.4.15.Information Assurance (IA)

The program manager should incorporate information assurance requirements into program design activities to ensure availability, integrity, authentication, confidentiality, and non-repudiation of critical system information (see DoD Directive 5000.1). DoD policy for information assurance of information technology, including National Security Systems (NSS), appears in DoD Directive 8500.1, *Information Assurance (IA) Implementation,* DoD Instruction 8580.1, *Information Assurance in the Defense Acquisition System,* and implementing instructions in DoD Instruction 8500.2, *Information Assurance (IA)* . Because the requirements for IA vary greatly across acquisition programs, it is essential that a program manager examine his/her acquisition program carefully to identify applicable IA requirements. Sections 7.5 and 8.3.3 of this Guidebook provide additional guidance on the extent and elements of IA that should be considered.

4.4.16.Insensitive Munitions

The ultimate objective when making design decisions on munitions is to develop and field munitions that have no adverse reaction to unplanned stimuli. All munitions and weapons, regardless of Acquisition Category (ACAT) level, should conform to insensitive munitions (unplanned stimuli) criteria and use materials consistent with safety and interoperability requirements. The Joint Capabilities Integration and Development System validation process determines insensitive munitions requirements and keeps them current throughout the acquisition cycle. Munitions insensitivity is certified per CJCS Instruction 3170.01. Waivers for munitions/weapons, regardless of ACAT level, require Joint Requirements Oversight Council (JROC) approval.

All submunitions and weapon submunitions, regardless of ACAT, should conform to the policy of reducing overall unexploded ordnance through a process of improving the submunitions system reliability - the desire is to field future submunitions with a 99% or higher functioning rate (SecDef Memorandum, 10 Jan 01, subject: DoD Policy on

Submunition Reliability). The JROC approves any waivers for this policy for "future" Acquisition Category I and II submunitions weapons programs. A future submunitions weapon is one that will reach Milestone C in fiscal year 2005 and beyond.

4.4.17.Anti-Tamper Provisions

Anti-tamper activities encompass the system engineering activities intended to prevent or delay exploitation of critical technologies in U.S. systems. These activities involve the entire life cycle of systems acquisition, including research, design, development, testing, implementation, and validation of anti-tamper measures. Properly employed, anti-tamper measures will add longevity to a critical technology by deterring efforts to reverse-engineer, exploit, or develop countermeasures against a system or system component.

The program manager should develop and implement anti-tamper measures in accordance with the determination of the Milestone Decision Authority (Milestone Decision Authority), as documented in the Anti-Tamper Annex to the Program Protection Plan (see DoD 5200.1-M, Acquisition Systems Protection Program) and DoDD 5200.39, Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection). Anti-tamper capability, if determined to be required for a system, is reflected in the systems specifications, integrated logistics support plan, Systems Engineering Plan, and other program documents and design activities. Because of its function, anti-tamper should not be regarded as an option or a system capability that may later be traded off without a thorough operational and acquisition risk analysis. To accomplish this, the program manager identifies, Critical Program Information and system vulnerabilities and, with assistance from counter-intelligence organizations, performs threat analyses on the critical technologies. Additionally, the program manager researches anti-tamper measures and determines which best fit the performance, cost, schedule, and risk of the program.

The program manager should also plan for post-production anti-tamper validation of end items. The Department's Anti-Tamper Executive Agent may develop and execute a validation plan and report results to the Milestone Decision Authority and Component Acquisition Executive.

4.4.18.System Security

The program manager should consider security, survivability, and operational continuity (i.e., protection) as technical performance parameters as they support achievement of other technical performance aspects such as accuracy, endurance, sustainability, interoperability, range, etc., as well as mission effectiveness in general. The program manager includes these considerations in the risk benefit analysis of system design and cost. Users are familiar with critical infrastructure protection and space control requirements, and account for necessary hardening, redundancy, backup, and other physical protection measures in developing system and system-of-systems capability documents and architectures.

4.4.18.1. Research and Technology Protection (RTP)

A component of overall system security, research and technology protection, identifies and safeguards selected DoD research and technology anywhere in the Research,

Development, Test and Evaluation or acquisition processes to include associated support systems (e.g., test and simulation equipment). This involves integrating all security disciplines, counterintelligence, intelligence, and other defense methods to protect critical science and technology from foreign collection or unauthorized (see also Chapter 8).

4.4.18.2. System Security Engineering (SSE)

System security engineering is an important element of Research and Technology Protection (RTP) and the vehicle for integrating RTP into a system during the design process. Not only does security engineering address potential unauthorized collection or disclosure, it also considers the possible capture of the system by an adversary during combat or hostile action and what security countermeasures are important during design to prevent reverse engineering. A discretionary Systems Security Management Plan documents recommended formatting, contents, and procedures for the SSE manager and contractors implementing SSE. Guidance for SSE assessments and preparation of the SSE management plan are contained in Military Handbook 1785, *System Security Engineering*.

4.4.19.Accessibility

The program manager must ensure that electronic and information technology acquisitions comply with Section 508 of the Rehabilitation Act of 1973. Unless an exception at Federal Acquisition Regulation 39.204 applies, acquisitions of electronic and information technology supplies and services must meet the applicable accessibility standards at Title 36 Code of Federal Regulations Section 1194. To avoid unnecessary costs and delays, the program manager should consider what accessibility requirements, if any, are applicable to the program early and throughout the system life cycle.

4.4.20.Unique Identification of Items

DoD Unique Identification (UID) permanently identifies an individual item. The serialized item is then distinct from all other individual items that the DoD buys or owns. With UID, the DoD can associate valuable business intelligence to an item throughout its life cycle. The UID system accurately captures and maintains data for valuation and tracking of items.

The DoD UID program places a minimum set of globally unique and unambiguous data markings on each identified item. The robust system ensures data integrity throughout the life of the item, and supports multi-faceted business applications and users.

The following sources provide useful information about UID:

- An Acting Under Secretary of Defense (Acquisition, Technology, and Logistics) Memorandum dated July 29, 2003. The memo contains the basic UID requirements and makes UID a mandatory requirement for all solicitations issued on or after 1 January 2004 by the Department;
- A DoD UID guide containing Frequently Asked Questions and a set of UID business rules, available at http://www.acq.osd.mil/uid;

- DFARS 211.274, *Item Identification and Valuation*, and DFARS 252.211-7003, *Item Identification and Valuation*; and
- Guide to Uniquely Identifying Items that specifies Identification Marking of U.S. Military Property.

4.4.21.Critical Safety Items

Critical Safety Items (CSIs) are parts whose failure would cause loss of life, permanent disability or major injury, loss of a system, or significant equipment damage. In particular, Pub. L. 108-136, sec. 802 (codified in 10 U.S.C. 2319) defines aviation critical safety items (CSIs) as parts, assemblies, installation equipment, launch equipment, recovery equipment or support equipment for an aircraft or aviation weapon systems, the failure, malfunction or absence of which could cause a catastrophic loss or critical failure resulting in loss or serious damage to an aircraft or weapon system, an unacceptable risk of personal injury or loss of life, or an uncommanded engine shutdown. CSIs represent less than five (5%) of the total population of replenishment parts used in aviation systems, but the implications of failure require they be identified and carefully managed from design through to disposal. The statute requires the Secretary of Defense to prescribe policy for the quality control of aviation CSIs. Specifically, it requires that 1) Design Control Activities establish a process to identify and manage aviation CSIs; 2) aviation CSIs be purchased only from sources approved by the Design Control Activity; and 3) delivered aviation CSIs meet requirements established by the Design Control Activity. As defined by the Authorization Act, the Design Control Activity is the systems command of a military department specifically responsible for ensuring the airworthiness of an aviation system or equipment in which aviation CSIs will be used.

Because of concerns regarding proper identification and life-cycle management of aviation CSIs, the Joint Aeronautical Commanders' Group (JACG) issued guidance for identifying, acquiring, ensuring quality, managing, and disposing CSIs. This guidance established standardized practices and terminology across Services, the Defense Logistics Agency (DLA), the Defense Contract Management Agency (DCMA), and Federal agencies for life-cycle management of aviation CSIs. Section C8.5 of DoD 4140.1-R on the DoD Supply Chain Materiel Management further establishes procedures for the life-cycle management of aviation CSIs.

4.5. Systems Engineering Execution: Key Systems Engineering Tools and Techniques

This section describes many of the systems engineering techniques and tools for management, oversight, and analysis and provides some general knowledge management resources.

4.5.1. Systems Engineering Plan

The Systems Engineering Plan (SEP) is a detailed formulation of actions that should guide all technical aspects of an acquisition program. Program managers should establish the SEP early in program formulation and update it at each subsequent milestone. It is intended to be a living document, tailored to the program, and a roadmap that supports

program management by defining comprehensive systems engineering activities, addressing both government and contractor technical activities and responsibilities. The SEP should be consistent with and complementary to the Test and Evaluation Strategy or Test and Evaluation Master Plan, as appropriate. This chapter of the Guidebook, in its entirety, should be taken as guidance for preparation of a SEP. Other SEP guidance materials include the following:

- SEP Frequently Asked Questions;
- SEP Preparation Guide; and
- SEP Focus Areas for Technical Planning.

The SEP describes the program's overall technical approach, including systems engineering processes; resources; and key technical tasks, activities, and events along with their metrics and success criteria. Integration or linkage with other program management control efforts, such as integrated master plans, integrated master schedules, technical performance measures, and earned value management, is fundamental to successful application.

There is no prescribed format for the SEP. However, it should address how systems engineering will support the translation of system capability needs into an effective, suitable product that is sustainable at an affordable cost. Specifically, a well-prepared SEP will address the integration of the technical aspects of the program with the overall program planning, systems engineering activities, and execution tracking to include:

- The systems engineering processes to be applied in the program (e.g., from a standard, a capability maturity model, or the contractor's process). Describe how the processes will be implemented and how they will be tailored to meet individual acquisition phase objectives. Describe how the systems engineering processes will support the technical and programmatic products required of each phase. Sections 4.2 (process) and 4.3 (process application to SE phase) provide a "roadmap" of how SE processes can be applied to an acquisition program.
- The system's technical baseline approach. Describe how the technical baseline will be developed, managed, and used to control system requirements, design integration, verification, and validation. Include a discussion of metrics (e.g., technical performance measures) for the technical effort and how these metrics will be used to measure progress.
- Event-driven timing, conduct, success criteria, and expected products of technical reviews, and how technical reviews will be used to assess technical maturity, assess technical risk, and support program decisions. SEP updates shall include results of completed technical reviews. Section 4.3 of this guide, as well as other reference material on technical reviews, should form a basis for the program's approach.
- The integration of systems engineering into the program's integrated product teams (IPTs). Describe how systems engineering activities will be integrated within and coordinated across IPTs; how the IPTs will be organized; what SE tools they will employ; and their resources, staffing, management metrics, and

integration mechanisms. Describe how systems engineering activities are integrated in the program's overall integrated schedules (4.5.2 and 4.5.3).

- For programs that are part of a system of systems or family of systems, the synchronization with related systems to achieve the desired mission capability as the system evolves. The relative contribution of each system to the overall mission capability in terms of performance and effectiveness should be identified to ensure that the combination of systems is appropriately integrated together.

In addition to describing required program activities, the SEP addresses the who, what, when, where, why, and how of the applied systems engineering approach.

Participants in the SE Process (Who) - Ideally, the SEP should detail roles and responsibilities of the systems engineering effort across the acquirer (government) and supplier (contractor) boundaries. Roles of the Chief Engineer, lead Systems Engineer, IPT SEs, Systems Engineering and Integration Teams, etc., need to be explicitly defined. Vertical and horizontal integration, team communications, and scope of decision-making authority are key elements of the plan, especially as these relate to management of technical baselines and reviews. SE staffing (planned vs. actual) should be included in this discussion together with (required vs. actual) discussion of domain experience of the staff.

SE Processes (What) - There are many ways to accomplish SE. Critical to the plan is which of these many ways will the program select and implement. There is a difference between complexity and uncertainty. While SE is complex, it should not be uncertain. The SEP should serve as a vehicle for minimizing process uncertainty. Optimally, a program team should use a single set of common SE processes. For large programs having multiple organizations, this may be an impractical goal. In these cases, the program manager should strive to "rationalize" or link the different process implementations across the program team so that process inputs and outputs integrate.

Facilities Enabling SE (Where) - The SEP should address development and use of SE facilities, including verification and validation facilities. Since these facilities can be complex hardware and software systems in their own right, the issue of integration facilities can be a significant challenge, particularly as relating to modeling and simulation development requirements.

SE Event Timing (When) - Systems engineering is an event-driven process. As such, the SEP should discuss the timing of events in relation to other SE and program events. While the initial SEP and Integrated Master Schedule will have the expected occurrence in the time of various milestones (such as overall system CDR), the plan should accommodate and be updated to reflect changes to the actual timing of SE activities, reviews, and decisions.

SE Decision Rationale (Why) - SE includes a continuous evolution of requirements (from high end to detail level) and trade offs (to best balance the design across often-conflicting design considerations). Rationale as to how these requirements and trades will be balanced should be included in the SEP. Decision criteria, such as entry and exit criteria for technical reviews, should be detailed.

Tools Enabling SE (How) -- Systems engineering makes use of a number of tools, toolsets, and enablers, such as modeling and simulation. The capability, variety, and dynamics of modern SE tools demand that they be fully integrated with the overall approach and discussion of SE application. Since adaptation of tools often occurs on programs, continual update of the SEP is required.

For programs where the USD(AT&L) or the ASD(NII) is the Milestone Decision Authority, components shall submit the SEP at least 30 days before the scheduled Defense Acquisition Board or ITAB milestone review. The Milestone Decision Authority is the approval authority for the SEP (see USD(AT&L) SE Policy Memo of 20 Feb 04). The Director, Defense Systems, and members of the OSD staff will assess the SEP and other required milestone documents, identify and help resolve issues, and make a recommendation on the program's readiness to proceed to the Defense Acquisition Board or ITAB.

4.5.2. Integrated Master Plan

The program manager should use event-driven schedules and the participation of all stakeholders to ensure that all tasks are accomplished in a rational and logical order and to allow continuous communication with customers. Necessary input conditions to complete each major task are identified, and no major task is declared complete until all required input conditions and component tasks have been satisfied. When documented in a formal plan and used to manage the program, this event-driven approach can help ensure that all tasks are integrated properly and that the management process is based on significant events in the acquisition life cycle and not on arbitrary calendar events.

One way of defining tasks and activities is the use of an integrated master plan, which provides an overarching framework against which all work is accomplished. It documents all the tasks required to deliver a high quality product and facilitate success throughout the product's life cycle. Cost, schedule (specific dates), and non-essential tasks are not included in this plan. During the initial stages of a program, the integrated plan is preliminary, and its purpose is to provide an understanding of the scope of work required and the likely structure of the program. It is constructed to depict a likely progression of work through the remaining phases, with the most emphasis on the current or upcoming phase (especially the period to be contracted for next). The integrated plan also serves to identify dependencies, which may be performed by different organizations.

As the program is defined, the integrated master plan is iterated several times, each time increasing the level of detail and confidence that all essential work has been identified. The specific format for this plan is not critical; however, it usually reflects an Event/Accomplishment/Criteria hierarchical structure--a format that greatly facilitates the tracking and execution of the program. Functional and Lifecycle inputs are required to integrate the product and associated processes produced by the program. Without formal documentation, such as an integrated master plan, these inputs may be lost when personnel change. Such a plan also defines and establishes the correct expectations.

Deriving the program schedule presents an opportunity to identify critical risk areas. As the times to complete specific tasks are estimated, events that may cause delays will

become apparent. These events are potential areas of risk that the program manager should consider for further analysis.

4.5.3. Integrated Master Schedule

Unlike event-based planning, time-based planning uses a calendar or detailed schedule to demonstrate how work efforts will support tasks and events. One way to produce such a schedule is to develop an integrated master schedule based on an integrated master plan. With an integrated master plan, the integrated master schedule further helps the program manager understand the links and interrelationships among the various teams. The integrated schedule begins as an integrated master plan with dates--the starting points are the events, accomplishments, and criteria that make up the plan. At a minimum, an integrated master schedule shows the expected start and stop dates for each criterion in the plan, but each criterion may be broken down into lower-level tasks that will be used to manage the program on a day-to-day basis. The schedule can be expanded downward to the level of detail appropriate for the scope and risk of the program. Programs with high risk show much lower levels of detail in the integrated master schedule in order to give the visibility to manage and control risk. The more detailed the integrated master schedule, however, the greater the cost to track and update the schedule. The dates in the integrated master schedule usually are not made contractually binding in order to allow the flexibility to take full advantage of event-driven scheduling.

Each of the work products requires different levels of effort, personnel, resources, and time to complete, with some being more difficult to complete than others. Critical Path Analysis is used to help identify which tasks, or sets of tasks, will be more difficult or costly to complete. As many of the tasks are inter-related and as work products typically require the completion of all lower level tasks before the higher-level work product can be completed, the early identification of critical tasks is essential for ensuring that schedule and cost goals are maintained for the program.

4.5.4. Value Engineering

The DoD value engineering program, per 41 U.S.C. 432, reduces cost, increases quality, and improves mission capabilities across the entire spectrum of DoD systems, processes, and organizations. It employs a simple, flexible, and structured set of tools, techniques, and procedures that challenge the status quo by promoting innovation and creativity. Furthermore, it incentivizes government participants and their industry counterparts to increase their joint value proposition in achieving best value solutions as part of a successful business relationship. Where appropriate, program managers should engage in a broad and rigorous application of the value engineering methodology. In addition, program managers should be receptive to Value Engineering Change Proposals (VECPs) made by contractors as a way of sharing cost savings and should also ensure that implementation decisions are made promptly. Additional Value Engineering training is available as a Defense Acquisition University learning module at https://learn.dau.mil/html/clc/Clc.jsp (click on CLE001).

4.5.5. Technical Performance Measurement

Systems engineering uses technical performance measurements to balance cost, schedule, and performance throughout the life cycle. Technical performance measurements compare actual versus planned technical development and design. They also report the degree to which system requirements are met in terms of performance, cost, schedule, and progress in implementing risk handling. Performance metrics are traceable to user-defined capabilities.

4.5.6. Trade Studies

Trade studies are conducted among operational capabilities, functional, and performance requirements, design alternatives and their related manufacturing, testing, and support processes; program schedule; and Lifecycle cost. Such trade studies are made at the appropriate level of detail to support decision making and lead to a proper balance between system performance and cost. Requirements come from many sources and unfortunately can conflict with each other. Trade studies are used for the resolution of these conflicts.

4.5.7. Modeling and Simulation

As the Department of Defense continues its transformation, it increasingly relies on network-centric operations and on individually-complex systems linked together in complex systems-of-systems. This transformation increases the dependency on seamless interoperability. Interoperability is needed between systems across military service and national boundaries, and requires effective performance by each individual system. The systems engineering process must exploit modeling and simulation to rapidly field improved capabilities with sufficient confidence that the fielded capabilities will perform effectively in the system-of-systems joint mission environment.

Modeling and simulation is an essential element of the systems engineering process. Modeling and simulation can represent the system-of-systems environment as a context for systems engineering to properly design, develop, and test individual systems. The cost and complexity of modern weapon systems, particularly within a family-of-systems or system-of-systems, preclude the development of full-scale prototypes to merely provide proof of concept. Similarly, the cost of testing events limits the number of tests that can be practically conducted. Modeling and simulation supports the systems engineering decision process by supporting systems design, trade studies, financial analysis, sustainment, and performance assessments.

The following paragraphs describe the contributions of modeling and simulation by phase.

4.5.7.1. Modeling and Simulation (M&S) in Concept Refinement

A technical framework, including essential architecture products, is necessary for a program manager to initiate the systems engineering process to allow interoperability with legacy, current, and future systems. M&S tools exist that can help define the technical framework to be part of the Capability Development Document. A prudent process includes development of a distributed collaborative environment accessible by all the stakeholders. M&S is a tool to support the collaborative process, to exchange data,

consider alternatives (such as operational concepts, conceptual designs, cost, and technology strategies), and view potential resulting capabilities.

M&S will allow a program manager to conduct rapid virtual prototyping with all stakeholders playing a role in the system as part of a family-of-systems or systems-of-systems. A distributed collaborative environment will support authoritative information exchange and rapid refinement of the design or concept due to changing circumstances such as technological advancements and changing threats, tactics, or doctrine.

Characteristics of a collaborative environment will entail models and simulations at multiple locations that are run and operated by subject matter experts and connected by wide area networks on an as needed basis. As changes are made to define a system that meets the needed capability, all stakeholders in the system's life cycle will have an active role in the changes being made.

When a needed capability is identified, M&S can be used in the collaborative environment to examine and explore alternatives and variations to proposed concepts. Rigorous examination, by all of the stakeholders, of proposed and alternative concepts applied through the effective use of M&S can help identify enabling technologies, constraints, costs, and associated risks. This rigor early in the concept refinement process is vital because the resulting decisions made in this early phase have repercussions throughout the system's life cycle that drive the ultimate life-cycle costs of the system.

Outputs of the Concept Refinement Phase include the Systems Engineering Plan (SEP) which should include M&S support throughout the acquisition life cycle and address M&S roles of both the government and industry. Of particular importance are configuration management, data rights and access, and responsibilities for life-cycle maintenance of data and models by industry and government. Appropriate standards to assure M&S interoperability and reuse of models and data should be addressed. Further, the Test and Evaluation Strategy should be defined with the role that M&S will play in augmenting and focusing the testing and evaluation process. Of vital importance is a strategy to continuously improve the veracity of the suite of M&S based on results from testing. The cyclical process of "model-test-fix-mode" is applicable to assure M&S remains on the cutting edge of validity.

Key to successful simulation support to the systems engineering process is the recognition that M&S employed during the concept refinement stage can be leveraged throughout successive phases of the acquisition cycle. Ideally, the same architecture, scenarios, data, and M&S exercised in the collaborative environment during concept refinement will be reused in support of the analysis during the Technology Development.

4.5.7.2. Modeling and Simulation (M&S) in Technology Development

M&S can be used during the Technology Development phase to help reduce technology risk and determine an appropriate set of technologies to integrate into a full system. With the establishment of the collaborative environment the same architecture, scenario, data, HWIL, SWIL, infrastructure, and some of the same M&S can be used to examine new technologies. M&S used in the development and demonstration of new technologies for Advanced Technology Demonstrations (ATDs) and Advanced Concept Technology Demonstrations (ACTDs) can be incorporated into the collaborative environment to

determine how to interface the new technologies with legacy systems and determine the likelihood of their successful transition to support a needed capability.

A variety of M&S tools can be used to examine reliability, maintainability, transportability, provisioning (spares, support equipment, manpower), cost implications, and human-machine interface design considerations for any new designs or technologies that can be applied to specific capability needs. The program manager should make use of physics-of-failure and finite element analysis M&S for stress analysis, structural dynamics, mass properties, structural design materials, fatigue, loads, shock isolation, and acoustics. These M&S tools should be incorporated and made accessible through the established collaborative environment.

Cost models should also be employed to determine projected life-cycle costs of the system. As part of the cost estimate, M&S tools for manpower estimates can be employed. Alternatives to the traditional cost estimation techniques need to be considered because legacy cost models tend not to adequately address costs associated with information systems, FoS, and SoS.

Testing of new capabilities needs to include test and evaluation throughout the technology and system development process rather than solely relying on a single "pass-fail" test to move into production. The role of M&S in the testing process must be documented in the Test and Evaluation Master Plan (TEMP). With the assistance and proper application of M&S and the early coordination with operational testers, the operational tests can be integrated throughout the development process and incorporated with the developmental tests. As part of the developmental testing process, a program manager should identify data needed from the tests to further validate the M&S used in the collaborative environment.

Before hardware prototypes are built, virtual prototypes should be developed, evaluated, redesigned as appropriate, and then reevaluated. The "model-test-fix-mode" process should be used under a spiral development paradigm to help identify an achievable capability with an ultimate goal of demonstrating capability in a virtual context before considering a hardware demonstration.

Outputs of the Technology Development phase include system performance specifications, the TEMP, an updated SEP, validated systems support, Lifecycle cost estimates, and manpower requirements. M&S should play a significant role in all of these outputs during this phase of the acquisition process.

4.5.7.3. Modeling and Simulation (M&S) in Systems Development and Demonstration

A key aspect of the systems Development and Demonstration phase is the integration of the new technologies with legacy, current, and future systems. With the establishment of the architecture for the collaborative environment, many of the systems interface requirements should already be satisfied. This will be particularity true for any new systems developed utilizing the same architecture. In any case, M&S can be used in conjunction with HWIL, real world C4ISR systems, and other simulated systems to identify the required interface requirements in order to be an integral part of a family of systems or system of systems.

Verified and validated M&S, supported by validated test data, can be used to support the testing process to evaluate the performance and maturity of the technology under development. The program manager can make effective use of M&S to help focus T&E of hardware prototypes to maximize the highest pay off of the T&E investments. M&S can assist the T&E process by assessing a system in scenarios and areas of the mission space or performance envelope where testing cannot be performed, is not cost effective, or additional data are required. M&S must play a significant role in testing a system that is part of a family-of-systems (FOS) or systems-of-systems (SoS). It is cost prohibitive and unrealistic to bring together all assets of a FoS or SoS to conduct live tests and evaluations of the systems' interactions. These systems' interactions can, however, be examined in a simulated environment where all or selective assets of FoS or SoS can be simulated.

Through the use of M&S, a system's capabilities and contributions to a FoS or SoS can demonstrated. Computerized representations of the system's human-machine interfaces can be provided to end-users to obtain final ergonomic modifications to the design. Making design changes in the computerized representations will be much less costly than making the same changes in hardware prototypes. Consideration should be given to using or modifying these same computerized representations to start training end-users on the new system. In such a simulated environment, final design trades and modifications can be made before going into production.

The M&S incorporated into the established collaborative environment supports transition to production. The digital design data associated with the system can be electronically transferred directly to the manufacturing floor, minimizing ambiguity in the systems specifications.

4.5.7.4. Modeling and Simulation (M&S) in Production

The M&S used during the systems engineering process allows system designs to be electronically transmitted to the manufacturing shop floor to make the manufacturing process more streamlined and efficient. M&S can be used to not only produce detailed designs of a system; they can also be used to define the production and support processes for the system. M&S should be considered in designing manufacturing facilities, defining production flows to meet planned production rates, and eliminating production bottlenecks.

Before a new system goes into production, a program manager should examine the possibilities of modifying the computerized prototypes of the system to create virtual trainers. A virtual trainer could be used to start training end-users on the new system before it rolls off of the production line.

4.5.7.5. Modeling and Simulation (M&S) in Operations and Support

As systems are fielded, end-user innovation and feedback on the operational performance of a system and its role in a family-of-systems (FoS) or system-of-system (SoS) may necessitate design modifications. Operational maintenance and repairs can be compared to the projections made by the logistical models and simulations so that the models can be revalidated and modified. The end-user feedback can be incorporated into existing

M&S tools used in the system's established collaborative environment to examine redesign alternatives. The Operations and Support Phase can be considered the beginning of the acquisition cycle because this is when needed capabilities and new requirements are identified.

The M&S applied to the system's acquisition process has potential to be re-used as course-of-action, decision support, and training tools. Additionally, the program manager has an M&S repository that represents the system at multiple levels of fidelity that can be used to represent the system in other M&S FoS and SoS environments. Therefore, it is incumbent for a program manager to plan for maintaining the M&S used throughout the development of the system during Operations and Support.

M&S plays an important role in all aspects of the acquisition process. This is especially true in designing and developing a capability that is part of a FoS or SoS. Today's systems and associated interactions are complex M&S can assist the process by controlling the desired variables to provide a repeatable audit trail that can assist in the acquisition decision processes.

4.5.7.6. Modeling and Simulation (M&S) Resources

Properly implemented, M&S can ensure that schedules are met, costs and production constraints are identified and quantified, and system requirements and key performance parameters are achieved. The following documents are provided for additional guidance. Additionally each service has a modeling and simulation office, which provides support to program offices.

Documents:

- DoD Directive 5000.59, Modeling and Simulation Management
- DoD 5000.59-M, Glossary of Modeling and Simulation Terms
- DoD 5000.59-P, Modeling and Simulation (M&S) Master Plan
- DoD Instruction 5000.61, Verification, Validation and Accreditation

Standards:

- IEEE 1278 (Series), IEEE Standard for Distributed Interactive Simulation (DIS)
- IEEE 1516 (Series), IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)

Websites:

- Defense Modeling and Simulation Office: www.dmso.mil
- Army Model and Simulation Office: www.amso.army.mil
- Navy Modeling and Simulation Management Office: www.navmsmo.hq.navy.mil
- Air Force Agency for Modeling and Simulation: www.afams.af.mil
- Simulation Interoperability Standards Organization: www.sisostds.org
- Institute of Electrical and Electronics Engineers: www.ieee.org

4.5.8. Summary of Technical Reviews

Technical reviews are an important oversight tool that the program manager can use to review and evaluate the state of the system and the program, re-directing activity after the review if found necessary. The commonly used reviews during most acquisition programs are the following:

- Initial Technical Review
- Alternative Systems Review
- System Requirements Review
- System Functional Review
- Preliminary Design Review
- Critical Design Review
- Test Readiness Review
- Production Readiness Review
- System Verification Review
- Operational Test Readiness Review

To learn more about the role of technical reviews in technical management throughout the program's lifecycle, consider taking the Technical Reviews continuous learning module offered by DAU at https://learn.dau.mil/html/clc/Clc.jsp and then click on CLE003.

NOTE: The technical reviews listed above and described in Section 4.3 are detailed reviews conducted between the program management office and contractor personnel to assist the program manager and contractor in assessing technical progress of the program. Unlike these technical reviews, a Design Readiness Review (DoD Instruction 5000.2) and Full-Rate Production Decision Review (DoD Instruction 5000.2) are Milestone Decision Authority-led management oversight reviews intended to provide an assessment (cost, schedule, and performance) of a program's readiness to progress further through the acquisition life cycle.

4.5.9. General Knowledge Tools

4.5.9.1. Best Practices

- The General Accounting Office has conducted several studies (A and B) on best practices
- The Systems Engineering Community of Practice
- The Systems Engineering Process Office within the Science, Technology, and Engineering Department of the Space and Naval Warfare Systems Center in San Diego, CA, is a resource for systems engineering and software engineering best practices. http://sepo.spawar.navy.mil

4.5.9.2. Case Studies

- The Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics), Office of Systems Engineering, has published several Integrated Product and Process Development case studies, including
    - Integrated Product/Process Development in the New Attack Submarine Program: A Case Study
    - Ford Motor Company's Investment Efficiency Initiative: A Case Study
    - Integrated Product/Process Development in Upgrade and Mod Programs.
- The Air Force Center for Systems Engineering has several case studies underway:
    - C-5
    - F-111
    - Theater Battle Management Core System
    - The Hubble Space Telescope.
- Case studies are also being planned for missile defense, DoD space-based systems, and commercial systems. http://cse.afit.edu/page.cfm?page=49
- Reliability, Availability and Maintainability Primer Case Studies

4.5.9.3. Lessons Learned

Lessons learned are a tool that the program manager may use to help identify potential areas of risk associated with the system by reviewing the experiences encountered in past programs. Lessons learned databases document what worked and what did not work in past programs, in the hopes that future programs can avoid the same pitfalls. Lessons learned can be found at all levels of the program, including: managerial, system, sub-system, and component.

Lessons learned are most effective when analogous programs and systems are identified, and the lessons learned are applied with discretion and proper judgment, as opposed to non-applicable lessons being blindly followed.

Ideally, a program manager searches lessons learned databases for analogous systems, enabling the program manager to be better prepared to defuse potential problems before they become real problems or to see what solutions to similar problems worked well in the past. However, because lessons learned databases are currently highly decentralized, it is often difficult to efficiently and effectively find applicable lessons learned in a form that is useful.

There are many organizations that produce lessons learned. Links to some of these organizations and databases from within and outside the DoD are given below.

- Center for Army Lessons Learned
- Air Force Center for Knowledge Sharing Lessons Learned Note: Access to this site is limited to government computers.
- Center for Systems Engineering at the Air Force Institute of Technology

- Air Force Knowledge Management
- Navy Lessons Learned System
- Joint Center for Lessons Learned
- Department of Energy Lessons Learned
- NASA Lessons Learned Information System

4.6. Systems Engineering Resources

4.6.1. Standards and Models

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15288, System Life Cycle Processes
- ISO/IEC 12207, Software Life Cycle Processes
- Electronic Industry Alliance (EIA)/Institute of Electrical and Electronic Engineers (IEEE) J-STD-016, Software Development
- American National Standards Institute (ANSI)/EIA 632, Processes for Engineering a System
- ANSI/EIA 649, National Consensus Standard for Configuration Management
- ANSI/EIA 748A, Earned Value Management Systems
- EIA 859, Consensus Standard for Data Management
- IEEE 1220, Application Management of the Systems Engineering Process
- EIA 731, Systems Engineering Capability Model
- CMMI SWE/SE/IPPD/SS, Capability Maturity Model-Integration, Software Engineering, Systems Engineering, Integrated Product and Process Development and Supplier Sourcing
- Best Manufacturing Practices Center of Excellence. www.bmpcoe.org/library/books/se%20model/00000482.html

4.6.2. Handbooks and Guides

- Guidance for the Use of Robust Engineering in Air Force Acquisition Programs
- Navy Systems Engineering Guide
- INCOSE Handbook
- MIL-HDB-61, *Configuration Management*
- MIL-HDBK 881, *Work Breakdown Structure*
- MIL-HDBK 1785, Systems Security Engineering
- NASA SE Handbook
- DSMC Systems Engineering Fundamentals

- DAU Risk Management Handbook
- Product Support for the 21st Century: A Program Manager's Guide to Buying Performance
- Designing and Assessing Supportability in DoD Weapon Systems: A Guide to Increased Reliability and Reduced Logistics Footprint
- DoD Template for Application of Total Life Cycle Systems Management (TLCSM) and Performance Based Logistics (PBL) In the Weapon System Life Cycle
- DoD Guide for Uniquely Identifying Items
- The Reliability Analysis Center is a DoD Information Analysis Center, a Center of Excellence, and a technical focal point for information, data, analysis, training and technical assistance in the engineering fields of Reliability, Maintainability, Supportability, and Quality. Their web site is http://rac.alionscience.com/
- ISO/IEC TR 19760, *Systems Engineering – A guide for the application of ISO/IEC 15288 (System Life Cycle Processes)*, First Edition, 2003-11-15
- Best Manufacturing Practices Center of Excellence. www.bmpcoe.org/library/books/se%20model/00000482.html

CHAPTER 5

Life Cycle Logistics (LCL)

5.0. Overview

5.0.1. Purpose

This chapter provides program managers with a description of Life-Cycle Logistics (LCL) and its application in the acquisition and sustainment phases. A fundamental change in DoD policy is the designation of the program manager as the life cycle manager (Total Life Cycle Systems Management (TLCSM)), responsible for effective and timely acquisition and sustainment of the system throughout its life cycle. The program manager is responsible for providing the needed product support capability to maintain the readiness, sustainment and operational capability of a system. Emphasis is placed on increasing reliability and reducing logistics footprint in the systems engineering process, and providing for effective product support using performance based logistics (PBL) strategies. Performance Based Logistics strategies may be applied at the system, subsystem, or major assembly level depending upon program unique circumstances and appropriate business case analysis. This approach is depicted in Figure 5.0.1.1.

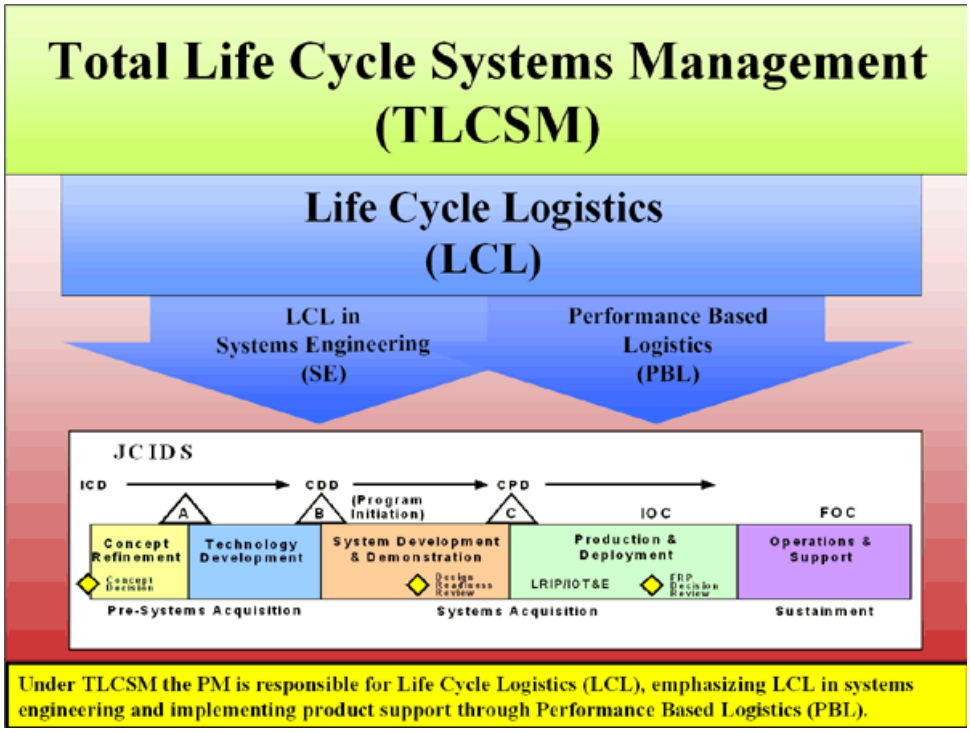

Figure 5.0.1.1. Overview

5.0.2. Contents

The first four sections of this chapter correspond to the elements depicted in Figure 5.0.1.1 :

Section 5.1, Life-Cycle Logistics (LCL), describes LCL, explains its role under Total Life Cycle Systems Management, and identifies the Program Manager's main LCL responsibilities. It also identifies DoD's overall logistics goals, providing context for the conduct of all LCL related activities.

Section 5.2, LCL in Systems Engineering, discusses LCL in Systems Engineering, focusing primarily on achieving affordable systems operational effectiveness. LCL considerations are addressed in the Joint Capabilities Integration and Development System process, demonstrated in Test and Evaluation, and implemented in fielding and Sustainment of the system. The concept of "design for support, support the design" is presented in this section.

Section 5.3, Performance Based Logistics, discusses DoD's preferred approach to product support, Performance Based Logistics, and provides a step-by-step process for implementing Performance Based Logistics. Performance Based Agreements and Source of Support are also discussed.

Section 5.4, Key LCL Activities in the System Life Cycle, identifies key LCL activities in each phase of a program, whether it is a major new system, a modification to a fielded system, or a redesign of a product support system. This section applies the concepts and actions discussed in the previous sections, placing them sequentially in the Defense Acquisition Management Framework to demonstrate when LCL-related activities take place.

In addition, Section 5.5, LCL Tools and References, provides LCL tools and references. These tools and references provide further explanation of critical items discussed in the chapter, as well as examples, templates, and other useful tools for LCL implementation.

5.1. Lifecycle Logistics (LCL)

This section discusses LCL in the context of Total Life Cycle Systems Management and DoD's strategic logistics goals, and identifies the program manager's LCL responsibilities. Subsequent sections discuss the program manager's primary means of fulfilling those LCL responsibilities: the inclusion of LCL considerations in systems engineering and implementation of Performance Based Logistics in Product Support.

5.1.1. Total Life Cycle Systems Management (TLCSM)

TLCSM is the implementation, management, and oversight, by the designated Program Manager, of all activities associated with the acquisition, development, production, fielding, sustainment, and disposal of a DoD weapon or materiel system across its life cycle (DoD Directive 5000.1). (See also 2.3, 11.7) TLCSM bases major system development decisions on their effect on life cycle operational effectiveness and logistics affordability. TLCSM encompasses, but is not limited to, the following:

- Single point of accountability for accomplishing program logistics objectives including sustainment.

- Evolutionary acquisition strategies, including product support.
- An emphasis on LCL in the systems engineering process.
- Supportability as a key element of performance.
- Performance-based logistics strategies.
- Increased reliability and reduced logistics footprint.
- Continuing reviews of sustainment strategies.

Implementation of the TLCSM business approach means that all major materiel alternative considerations, and all major acquisition functional decisions demonstrate an understanding of their effects on operations and sustainment phase system effectiveness and affordability (see section 4.1).

In addition, TLCSM assigns the program manager responsibility for effective and timely acquisition, product support, availability, and sustainment of a system throughout its life cycle.

5.1.2. Lifecycle Logistics (LCL)

LCL is the planning, development, implementation, and management of a comprehensive, affordable, and effective systems support strategy. Under Total Life Cycle Systems Management, Lifecycle Logistics has a principal role during the acquisition and operational phases of the weapon or materiel system life cycle. LCL should be carried out by a cross-functional team of subject matter experts to ensure that supportability requirements are addressed comprehensively and consistently with cost, performance, and schedule during the life cycle. Affordable, effective support strategies must meet goals for operational effectiveness, optimum readiness, and the facilitation of iterative technology enhancements during the weapon system life cycle.

LCL also includes the planning, development, and implementation of Performance Based Logistics initiatives as the preferred approach to systems support (DoD Directive 5000.1). Examples of these initiatives include: managing performance agreements, integrating support strategies, and employing diagnostics, prognostics, and logistics chain management approaches to achieve operational effectiveness, system affordability, and reduced logistics footprint. LCL should be an integral part of the systems engineering process to insure that supportability considerations are implemented during the design, development, production, and sustainment of a weapon system.

DoD Strategic Intent: LCL fully supports DoD's strategic goals for acquisition and sustainment logistics as stated in the most recent Quadrennial Defense Review (QDR), Joint Vision 2020, and the Focused Logistics Campaign Plan (FLCP). DoD goals include:

- Project and sustain the force with minimal footprint (per QDR).
- Implement Performance-Based Logistics.
- Reduce cycle times to industry standards (per QDR).

LCL supports achievement of these goals within the context of Total Life Cycle Systems Management.

5.1.3. The Program Manager's Life-Cycle Logistics (LCL) Responsibilities

The Program Manager is the life cycle manager. Program managers examine and implement appropriate, innovative, alternative logistics support practices, including best public sector and commercial practices and technology solutions. (See DoD Directive 5000.1 paragraphs E1.29 and E1.17.) The choice of alternative logistics support practices is based on the program manager's documented assessment that such actions can satisfy joint needs in a manner that is fully interoperable within DoD's operational and logistics systems, improve schedules, performance, or support; or reduce weapon system support costs. Regardless of the chosen support strategy, program managers, in collaboration with other key stakeholders, especially the warfighter, establish logistics support program goals for cost, customer support, and performance parameters over the program life cycle. Decisions are made to satisfy formal criteria, resulting in systems that are interoperable and meet Joint Capabilities Integration and Development System and Joint Capabilities Integration and Development System-related performance capabilities needs.

LCL is a critical component in two of the program manager's key program management deliverables: the acquisition strategy, which includes the product support strategy; and the acquisition program baseline, which identifies program metrics.

Acquisition Strategy. As part of the acquisition strategy discussed in section 2.3, the program manager develops and documents a **Product Support Strategy** for Lifecycle sustainment and continuous improvement of product affordability, reliability, and supportability, while sustaining readiness (see section 5.4.1.2.1). This effort ensures that system support and Lifecycle affordability considerations are addressed and documented as an integral part of the program's overall acquisition strategy. The product support strategy defines the supportability planning, analyses, and trade-offs conducted to determine the optimum support concept for a materiel system and strategies for continuous affordability improvement throughout the product life cycle. The support strategy continues to evolve toward greater detail, so that by Milestone C, it contains sufficient detail to define how the program will address the fielding and support requirements that meet readiness and performance objectives, lower life cycle cost (LCC), reduce risks, reduce logistics footprint, and avoid harm to the environment and human health. The support strategy should address all applicable support requirements to include, but not be limited to, the following elements:

- Product Support (including software) (5.1.3.1);
- Interoperability (5.1.3.2);
- Data Management (DM) (5.1.3.3);
- Integrated Supply Chain Management (5.1.3.4);
- Life Cycle Cost Optimization (5.1.3.5);
- Logistics Footprint Minimization (5.1.3.6);
- Life Cycle Assessment (5.1.3.7);

- Demilitarization and Disposal (5.1.3.8);
- Environment, Safety, and Occupational Health (ESOH) (5.2.1.6 and 4.4.11);
- Human Systems Integration (HSI) (5.2.1.6 and Chapter 6); and
- Review and update Designated Science and Technology Information, the Security Classification Guide, and the Counterintelligence Support Plan.

The Product Support Guide provides detailed information for developing product support strategies and related activities (see DUSD(LMR) Memorandum, November 2001, Product Support Guide).

Acquisition Program Baseline (APB). As discussed in section 2.1.1 of this Guidebook, the program manager and user prepare the APB at program initiation. Updates follow subsequent milestone reviews, program restructurings, and unrecoverable program deviations. The APB core is a transcription of the Joint Capabilities Integration and Development System' formal requirements for performance capability, schedules, and total program cost. The program manager can ensure effective consideration of Lifecycle logistics factors by emphasizing supportability factors in the APB.

5.1.3.1. Product Support

Product support is a package of logistics support functions necessary to maintain the readiness, sustainment, and operational capability of the system.

The overall product support strategy, documented in the acquisition strategy, should include Lifecycle support planning and address actions to assure sustainment and continually improve product affordability for programs in initial procurement, reprocurement, and post-production support.

Support concepts satisfy user specified requirements for sustaining support performance at the lowest possible life cycle cost for each evolutionary increment of capability to be delivered to the user, including:

- Availability of support to meet warfighter-specified levels of combat and peacetime performance.
- Logistics support that sustains both short and long-term readiness
- Minimal total Lifecycle cost to own and operate (i.e., minimal total ownership cost).
- Maintenance concepts that optimize readiness while drawing upon both organic and industry sources.
- Data management and configuration management that facilitates cost-effective product support throughout the system life cycle.

Performance Based Logistics is the preferred DoD approach to product support (see section 5.3), which serves to consolidate and integrate the support activities necessary to meet these objectives (see Product Support Guide).

5.1.3.2. Interoperability

Interoperability is a key LCL facilitator, which allows the program manager to take advantage of joint capabilities in designing and implementing a product support strategy. A modular open systems approach (MOSA) allows the logistician to apply risk mitigation analyses earlier in the system development process to reduce the required resources and overall life cycle costs. The life cycle logistician assists the program management team in the application of MOSA to provide interoperability, maintainability, and compatibility when developing the support strategy and follow-on logistics planning for sustainment. Materiel and operational interoperability for LCL should be considered throughout the systems engineering process.

In carrying out their product support responsibilities, the program manager should be mindful of the benefits of drawing support from other DoD Components and Allies. Acquisition cross-servicing agreements are a means of exploiting those potential benefits.

Acquisition and Cross-Servicing Agreements (ACSAs). Per DoD Instruction 5000.2, the program manager should be aware of and understand the legal authority for the acquisition and reciprocal transfer of logistic support, supplies, and services from eligible countries and international organizations. The program manager should explicitly consider the long-term potential of ACSAs in developing the support strategy. Further guidance on this subject is available in section 11.2.3 of this Guidebook and DoDD 2010.9.

5.1.3.3. Data Management (DM)

Under Total Life Cycle Systems Management, the program manager is responsible for Data Management for the system throughout its life cycle. Data Management is an important part of Life-Cycle Logistics. In that context, Data Management consists of the disciplined processes and systems that plan for, acquire and/or access, manage, and use data throughout the total system life cycle. Data Management in Systems Engineering is discussed in 4.2.3.7.

Data Management is defined as the process of applying policies, systems and procedures for identification and control of data requirements; for the timely and economical acquisition of such data; for assuring the adequacy of data; for the access, distribution or communication of the data to the point of use; and for analysis of data use. Data is defined as recorded information regardless of the form or method of recording. This section concentrates on technical, product, and logistics data in support of the development, production, operation, sustainment, improvement, demilitarization and disposal of a system. This includes both government and contractor created data.

The program manager should develop a long-term strategy that integrates data requirements across all functional disciplines to include logistics. A performance-based approach should be used to identify the minimal data required to cost-effectively operate, maintain and improve the fielded system and to foster source of support competition throughout the system life cycle. Data should be available in a format that is compatible with the intended user's environment and a quality assurance program should be implemented to guarantee the accuracy and completeness of the data.

In many cases, leaving Government acquired data in the physical possession of the contractor and having access to the contractor's data system is the ideal solution. In

addition to data access, the requirement for Government use, reproduction, manipulation, altering or transfer of possession of data should be part of the data acquisition and management strategy. The contract should specify appropriate Government rights to the data acquired, in addition to requirements for delivery or access. Data, whenever it is delivered to the government, should be formatted in accordance with accepted data standards to ensure usability by the government. A list of data standard examples can be found in section 4.2.3.7, of this document. These decisions should be made early in the acquisition life cycle to avoid unexpected costs to procure, reformat and deliver data.

Whether the data is stored and managed by the government or by industry, the program manager is responsible for protecting system data. Policy applicable to data protection, marking, and release can be found in the following: DoD Directive 5230.24, *Distribution Statements on Technical Documents*; DoD Directive 5230.25, *Withholding of Unclassified Technical Data From Public Disclosure*; DoD 5400.7-R, *DoD Freedom of Information Act Program*; and Defense Federal Acquisition Regulations Supplement (DFARS) Part 252.227-7013 & 7014.

Industry standards, such as GEIA, ISO and ANSI, provide high level principles to guide integrated data management planning, and implementation. GEIA Standard, GEIA-859, *Data Management* is a guide that may be helpful for program managers and data managers. This standard and the emerging Handbook outline principles and processes for the management of data including data interoperability & longevity, best practices, and long term electronic storage, use, and recovery of data.

The Data Management strategy should be supported by an integrated data system that meets the needs of both the warfighter and the support community. Data systems supporting acquisition and sustainment should be connected, real-time or near real-time, to allow logisticians to address the overall effectiveness of the logistics process in contributing to weapon system availability and life cycle cost factors. Melding acquisition and sustainment data systems into a true total life cycle integrated data environment provides the capability needed to reduce the logistics footprint and plan effectively for sustainment, while also insuring that acquisition planners have accurate information about total life cycle costs.

As discussed in Chapter 7, an integrated data management system:

- Facilitates technology insertion for affordability improvements during re-procurement and post-production support.
- Supports configuration management processes.
- Maintenance and sustainment analyses;
- Contract service risk assessments over the life of the system

5.1.3.4. Integrated Supply Chain Management

DoD Components operate an integrated, synchronized, total-system, Lifecycle logistics chain to meet user requirements for information and materiel. The objective is to promote user confidence in the logistics process by building a responsive, cost-effective capacity

to ensure that warfighters get the materiel that they need, when they need it, with complete status information.

Under the Lifecycle Logistics approach, the program manager is ultimately responsible for satisfying the user's request, regardless of who is executing the integrated logistics and supply chain action. The DoD logistics chain, however, emphasizes commodity management, rather than weapon system optimization, with multiple hand-offs through various links in the supply chain. As discussed in section 5.3 below, program managers can use a Performance Based Logistics strategy to address these limitations. Because Performance Based Logistics arrangements are weapon system-based, support is focused on the customer and conflicting commodity priorities are mitigated or eliminated. In summary, Performance Based Logistics enables the program manager to exploit supply chain processes and systems to provide flexible and timely materiel support response during crises and joint operations.

The program manager ensures that user support is based on collaborative planning, resulting in realistic performance expectations established through Performance Based Agreements (see 5.3.2). These agreements should be negotiated in conjunction with the product support integrator, support providers, and the service providers, e.g. distribution centers and transportation providers. Performance Based Agreements Templates and Guidance are available for use (see 5.5.5). Most of these supply chain activities are governed by DoD 4140.1-R, released 23 May 2003.

Although it is important in all aspects of Life-Cycle Logistics, integrated supply chain management places a premium on user collaboration.

User Collaboration. Implementation of the Lifecycle Logistics approach, especially integrated supply chain management, requires program managers to collaborate with users, e.g. the force providers in conjunction with the Combatant Commands and the DoD Components of those commands, to determine optimal logistics strategies tailored to meet the users' needs and expectations, and produce a performance based agreement that codifies the negotiated user requirements and performance expectations (DoD Directive 5000.1). These agreements should be negotiated in conjunction with the product support integrator, support providers, and the service providers (e.g. distribution centers and transportation providers).

5.1.3.5. Life Cycle Cost Optimization

The program manager's overriding program objective is to maximize system effectiveness from the perspective of the warfighter. Given a resource-constrained environment; however, trade-offs are inevitable among performance, availability, process efficiency, and cost. The program manager should think in both the short- and long-terms. Short-term pressures to achieve system performance and schedule imperatives are very real, and cannot be ignored. In any program there will always be financial constraints and unforeseen financial contingencies.

System long-term readiness and affordability are, however, equally important program elements to be maximized. Program success is also determined by executing the performance parameter threshold for "operational cost as a military requirement, with threshold values." (CJCS Instruction 3170.01) The focus should be taking a Total Life

Cycle Systems Management approach to program resources and source selection weight decisions, as applied to operational cost effectiveness.

Defense system Life Cycle Cost (LCC) is the total cost to the Government of acquisition and ownership of a system over its useful life. It includes the cost of development, acquisition, support, and disposal. LCC should be considered in all program decisions, especially in trade-offs affecting Life-Cycle Logistics. (See DoD Directive 5000.1, E1.4, E1.18, and E1.29.) The Cost Analysis Requirements Description (see 3.4.2.1) reflects all significant Life-Cycle Logistics requirements for purposes of preparing the LCC estimate.

The program manager addresses these issues using the system operational effectiveness (SOE) model (5.2.2) – balancing consideration of performance, cost, schedule, system availability, and process efficiency components. A system that meets performance requirements but is not reliable, maintainable, and supportable is a liability to the warfighter. Ultimately, over the system life cycle, balancing this composite of long-term objectives will clearly provide greater benefit to the warfighter and to DoD.

Cost as an Independent Variable (CAIV). "Cost" is first treated as a formal military requirement via Joint Capabilities Integration and Development System cost-related performance parameters. Supportability-related cost performance criteria, such as O&S cost-per-operating-hour, should influence CAIV principles; as applied to program investment and prioritization intended to affect life cycle cost effectiveness and affordability. (See DoD Directive 5000.1 and this Guidebook section 3.2.4)

5.1.3.6. Logistics Footprint Minimization

In addition to minimizing costs, the program manager must also strive to minimize the logistical burden that a system will place on deployed forces. As stated in the QDR, an overarching DoD goal is to project and sustain the force with minimal logistics footprint. The 'footprint problem' is an engineering problem (see section 5.2.1.1), which is best addressed early in the life cycle. Program managers ensure that footprint metrics appropriate to the system and its operational environment are considered throughout the life cycle.

5.1.3.7. Life Cycle Assessment

While the greater part of the program manager responsibilities discussed above are first addressed in early, pre-deployment phases of the life cycle, Total Life Cycle Systems Management also requires the program manager to provide continuing support and assessment to deployed systems, and to manage the demilitarization and disposal of old systems.

The product support strategy addresses how the program manager and other responsible organizations will carry out ongoing assessment of the fielded system. Life cycle assessment identifies and properly addresses performance, readiness, ownership cost, and support issues. It includes both pre- and post-deployment evaluations to assess system performance and the support strategy, and to support technology insertion for continuous modernization and product affordability improvements. Life cycle assessment should be consistent with the written charter of the program manager's authority, responsibilities,

and accountability for accomplishing approved program objectives. Post-deployment evaluations are the primary means of providing program manager life cycle assessment.

Post Deployment Review (PDR). The program manager uses post-deployment reviews of the system, beginning at IOC, to verify whether the fielded system continues to meet or exceed thresholds and objectives for cost, performance, and support parameters approved at full-rate production. DoD policy requires that, "The Services shall conduct periodic assessments of system support strategies vis-à-vis actual vs. expected levels of performance and support. These reviews occur nominally every three to five years after IOC or when precipitated by changes in requirements/design or performance problems, and should include, at minimum:

- Product Support Integrator/Provider performance.
- Product improvements incorporated.
- Configuration control.

Modification of performance based logistics agreements as needed based on changing war fighter requirements or system design changes." (USD(ATL) Memorandum, March 2003, TLCSM& PBL, p. 9)

Post-deployment reviews continue as operational support plans execute (including transition from organic to contract support and vice versa, if applicable), and should be regularly updated depending on the pace of technology. The program manager should use existing reporting systems and operational feedback to evaluate the fielded system whenever possible

5.1.3.8. Demilitarization and Disposal

Given that the program manager is the total life cycle manager, it is important that program managers are aware, from the very beginning of a program, that they must consider and plan for the ultimate demilitarization and disposal of the system once it is no longer militarily useful.

The program manager considers materiel demilitarization and disposal during systems engineering. The program manager minimizes the Department of Defense's liability due to information and technology security, and Environment, Safety, and Occupational Health issues. The program manager carefully considers the impacts of any hazardous material component requirements in the design stage to minimize their impact on the life cycle of the end item regarding item storage, packaging, handling, transportation, and disposition. The program manager coordinates with DoD Component logistics activities and DLA, as appropriate, to identify and apply applicable demilitarization requirements necessary to eliminate the functional or military capabilities of assets (DoD 4140.1-R and DoD 4160.21-M-1). The program manager coordinates with DLA to determine property disposal requirements for system equipment and by-products (DoD 4160.21-M). The Chief of Naval Operations N43 and NAVSEA/Supervisor of Shipbuilding act as managers for ship disposal and recycling.

5.2. Life-Cycle Logistics (LCL) in Systems Engineering (SE)

Program management teams manage programs "through the application of a systems engineering approach that optimizes total system performance and minimizes total ownership costs" (DoD Directive 5000.1). Due to the nature of evolutionary acquisition and incremental/spiral development strategies, there is no longer a clear and definable line between design, development, deployment, and sustainment. Effective sustainment of weapons systems begins with the design and development of reliable and maintainable systems through the continuous application of a robust systems engineering methodology that focuses on total system performance.

LCL should be considered early and iteratively in the design process, and life cycle supportability requirements are an integral part of the systems engineering process. A detailed discussion of the systems engineering process can be found in section 4.2 of this Guidebook. Also see Designing and Assessing Supportability in DoD Weapon Systems: A Guide to Increased Reliability and Reduced Logistics Footprint (the 'Supportability Guide'). Additional discussion of LCL activities by acquisition phase can be found in section 5.4 of this Guidebook.

Demonstration of assured supportability and Lifecycle affordability should also be an entrance criterion for the Production and Deployment Phase. The specific requirements associated with integrating the support strategy into the system engineering process can be accomplished through IPPD.

This section first provides a list of LCL Considerations for systems engineering. Next it focuses on the achievement of affordable system operational effectiveness during Pre-Acquisition and Acquisition, including Joint Capabilities Integration and Development System analyses, design, Test and Evaluation, and Production (Design for Support). Finally, it briefly discusses LCL during Sustainment, to include Deployment, Operations, and Support (Support the Design).

5.2.1. Life-Cycle Logistics (LCL) Considerations for Systems Engineering

The following are recommended considerations in managing Life-Cycle Logistics-related systems engineering activities, including Joint Capabilities Integration and Development System, design, test and evaluation, fielding, and sustainment.

5.2.1.1. Logistics Footprint Reduction

Program management teams can best support evolving military strategy by providing US forces with the best possible system capabilities while minimizing the logistics footprint. Program management teams are responsible for achieving program objectives throughout the Lifecycle, from development through sustainment, while minimizing cost and logistics footprint (see DoD Directive 5000.1, E1.17 and E1.29). To minimize the logistics footprint, a deployed system must lessen the quantity of support resources required, including personnel, supplies, and support equipment. To achieve these goals, the supportability posture of weapon systems needs to be designed-in. The "footprint problem" is resolved through effective and early systems engineering – the opportunities for decreasing the logistics footprint decline significantly as the system evolves from design to production to deployment. See also 4.4.9 and The Supportability Guide.

5.2.1.2. Condition Based Maintenance Plus (CBM+)

Program managers are required to "optimize operational readiness through affordable, integrated, embedded diagnostics and prognostics, … automatic identification technology; and iterative technology refreshment" (DoD Instruction 5000.2). It is also Department of Defense policy that Condition Based Maintenance (CBM) be "implemented to improve maintenance agility and responsiveness, increase operational availability, and reduce life cycle total ownership costs" (DUSD(LMR) Memorandum, November 2002, CBM+). The goal of CBM is to perform maintenance only upon evidence of need. CBM tenets include: designing systems that require minimum maintenance; need-driven maintenance; appropriate use of embedded diagnostics and prognostics through the application of RCM; improved maintenance analytical and production technologies; automated maintenance information generation; trend based reliability and process improvements; integrated information systems providing logistics system response based on equipment maintenance condition; and smaller maintenance and logistics footprints. Condition Based Maintenance Plus (CBM+) expands on these basic concepts, encompassing other technologies, processes, and procedures that enable improved maintenance and logistics practices. CBM+ can be defined as a set of maintenance processes and capabilities derived, in large part, from real-time assessment of weapon system condition, obtained from embedded sensors and/or external tests and measurements. Ultimately, these practices can increase operational availability and readiness at a reduced cost throughout the weapon system life cycle. The design specifications should identify early teaming with systems engineering to clearly define and understand the operating envelope in order to design in Built-In-Test (BIT) and Built-In-Self-Test (BIST) mechanisms including false alarm mitigation.

Diagnostics: Applicable and effective on-board monitoring/recording devices and software, e.g. built-in test (BIT), that provide enhanced capability for fault detection and isolation, thus optimizing the time to repair. Emphasis must also be on accuracy and minimization of false alarms (DoD Instruction 5000.2).

Prognostics: Applicable and effective on-board monitoring/recording devices and software, e.g. BIT, that monitor various components and indicate out of range conditions, imminent failure probability, and similar proactive maintenance optimization actions (DoD Instruction 5000.2).

5.2.1.3. Serialized Item Management

Effective serialized item management programs provide accurate and timely item-related data that is easy to create and use, and their use is required (DoD Instruction 5000.2). Serialized item management is pursued to identify populations of select items (parts, components, and end items), to mark all items in the population with a universally Unique Item Identifier, to enable the generation, collection and analysis of maintenance data about each specific item. As a minimum, it is appropriate to consider selecting item populations from within the following categories:

- repairable items down to and including sub-component repairable unit level,
- life-limited, time-controlled, or items with records (e.g., logbooks, aeronautical equipment service records, etc.), and
- items that require technical directive tracking at the part number level.

For additional information and guidance, see DoD policy memorandum, September 4, 2002, Serialized Item Management.

Automatic Identification Technology. Automatic identification technology (AIT), also required, is considered an integral element of serialized item management programs and supporting supply and maintenance management information systems (DoD Instruction 5000.2). Items selected for serialized item management should be marked with AIT-compliant identification numbers. Item markings and accompanying AIT capabilities allow paperless identification, automatic data entry, and facilitate digital retrieval of maintenance-related information. For additional information and guidance, see DoD policy memorandum, July 29, 2003, Policy for Unique Identification (UID) of Tangible Items-New Equipment, Major Modifications, and Reprocurement of Equipment and Spares; and DoD policy memorandum, November 26, 2003, Update to Policy for Unique Identification (UID) of Tangible Items – New Equipment, Major Modifications, and Reprocurements of Equipment and Spares.

Radio Frequency Identification. Radio Frequency Identification is an integral part of the DoD plan to enhance supply chain management (USD(AT&L) Memorandum, July 2004, Radio Frequency Identification (RFID) Policy). Specifically, by providing real-time updates, radio frequency identification will enhance movement and timely positioning of materiel within the logistics node. The implementation of radio frequency identification will transform DoD supply chains externally and internally, and should be addressed in the SCM strategy.

5.2.1.4. Configuration Management

Configuration Management (CM) is a process for establishing and maintaining the consistency of a product's physical and functional attributes with its design and operational information throughout its life. program managers are required to "base configuration management decisions on factors that best support implementing performance-based strategies throughout the product life cycle" (DoD Directive 5000.1). Integral to successful CM is the development of a CM plan. The program manager can find detailed guidance for documenting the CM plan in ANSI/EIA-649 *Configuration Management*.

The following are attributes of the Configuration Management Process:

A. Configuration Identification - uniquely identifying the functional and physical characteristics of an item

B. Configuration Change Management- controlling changes to a product using a systemic change process

C. Configuration Status Accounting - capturing and maintaining the configuration of an item throughout the lifecycle

D. Configuration Verification and Audit- ensuring product design is accurately documented and achieves agreed upon performance requirements.

The program manager should consider industry standards and best practices. Those standards are documented in the following:

- ANSI/EIA 649A, *Configuration Management,* located on the GEIA website http://www.geia.org/ click on STANDARDS
- ISO 10007, *Quality Management – Guidelines for configuration management*
- EIA 836, *Configuration Management Data Exchange and Interoperability,* located on the GEIA website http://www.geia.org/ click on STANDARDS
- HDBK 649, *Configuration Management* – (in development, expected 12/05)

Program managers establish and maintain a configuration control program, and are required to "base configuration management decisions on factors that best support implementing performance-based strategies throughout the product life cycle" (DoD Directive 5000.1). The approach and activity that has responsibility for maintaining configuration control will depend on a number of program specific factors such as design rights, design responsibility, support concept, and associated costs and risk. Nominally the government maintains configuration control of the system design specification and the contractor(s) performs configuration management for the design. As such the Government retains the authority/responsibility for approving any design changes that impact the system's ability to meet specification requirements. The contractor(s) has the authority/responsibility to manage other design changes. The Government maintains the right to access configuration data at any level required to implement planned or potential design changes and support options. Configuration management of legacy systems should be addressed on a case by case basis as design changes are contemplated. (See also 4.2.3.6, EIA-649, and MIL HDBK 61A)

5.2.1.5. Continuous Technology Refreshment and Obsolescence

The program manager engineers the system architecture and establishes a rigorous change management process for life cycle support. Systems that integrate multiple commercial items can require extensive engineering to facilitate the insertion of planned new commercial technology. This is not a "one time" activity because unanticipated changes may drive reconsideration of engineering decisions throughout the life of the program.

Successful parts management addresses diminishing manufacturing sources and material shortages in the proposal, design, and maintenance phases of a product – that is, throughout the product's life cycle. For further discussion see the Supportability Guide.

As discussed in section 5.3, Performance Based Logistics support arrangements give significant latitude to the Product Support Integrator to manage technology refreshment. Product Support Integrators have responsibility for performance outcomes and are incentivized to maintain currency with state-of-the-art technology, maximize the use of commercial off-the-shelf items, and generally use readily available items to avoid the high cost of diminishing manufacturing sources and material shortages over the life of the system.

5.2.1.6. Other Life-Cycle Logistics (LCL) Related Considerations

Risk Management. The acquisition strategy addresses risk management, which should include LCL related risk.

Interoperability and Joint Architecture. Interoperability, which is required (DoD Directive 5000.1), is also important to LCL considerations such as supportability, maintainability, and footprint. For further discussion of interoperability see 5.1.3.2, 4.4.2, and Chapter 7.

Interoperability and Business Enterprise Architecture. The Business Enterprise Architecture for Logistics (BEA-Log) exists in the context of DoD's Business Enterprise Architecture (BEA) (DoD Directive 5000.1). For further information see http://www.bea-log.com.

Human Systems Integration. The program manager pursues HSI initiatives to optimize total system performance and minimize total ownership costs. For further discussion see Chapter 6.

Environment, Safety and Occupational Health (ESOH). A support program, as defined in DoD Instruction 5000.2, includes ESOH (to include explosives safety), which must be addressed throughout the acquisition process (DoD Directive 5000.1). As part of the program's overall cost, schedule, and performance risk reduction, the program manager shall prevent ESOH hazards, where possible, and shall manage ESOH hazards where they cannot be avoided. (See also section 4.4.11)

A program manager's best means of insuring a system will meet its LCL goals and satisfy user supportability needs is to insure that these LCL considerations are infused in all phases of the program's life cycle. It is especially important that LCL considerations are included in Pre-Acquisition and Acquisition activities, including the Joint Capabilities Integration and Development System process and Test and Evaluation. (LCL related activities become prominent as a program moves into Production and Deployment, and Sustainment.

5.2.2. Pre-Acquisition and Acquisition (Design for Support)

As discussed in section 4.4.9 and in the Supportability Guide, designing for optimal System Operational Effectiveness (SOE) requires balance between System Effectiveness and Life Cycle Cost. The emphasis is not only on the reliability and maintainability of the prime mission system or equipment to execute mission capability, but also on human factors engineering along with the cost-effective responsiveness and relevance of the support system and infrastructure. The key here is to smoothly integrate the DoD 5000 Defense Acquisition Management Framework (including its defined phases and milestones), together with the systems engineering and design maturation processes.

SOE is the composite of performance, availability, process efficiency, and total ownership cost. The objectives of the SOE concept can best be achieved through influencing early design and architecture, and through focusing on the supportability outputs. Reliability, reduced logistics footprint, and reduced system life cycle cost are most effectively achieved through inclusion from the very beginning of a program - starting with the definition of required capabilities. This process is depicted in Figure 5.2.2.1.

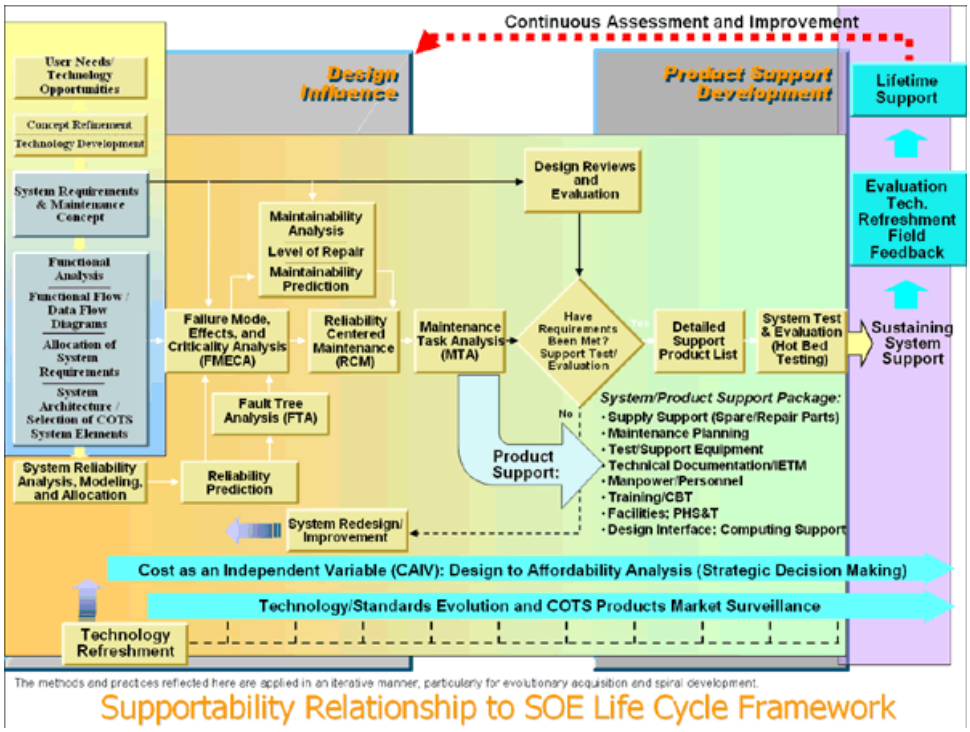

Figure 5.2.2.1. Supportability Relationships

As Figure 5.2.2.1. illustrates, reliability, maintainability and supportability methods, practices, and processes must be integrated throughout the systems engineering process to facilitate the supportability assessment of a design, from conception through deployment and sustainment. As such, the concept of operations must be defined to provide the basis for defining both the top-level system requirements and capabilities, and the initial definition of the system maintenance and support concept. Formulating the system architecture and performing all associated trade studies with attention to system maintenance ensures a balanced and symbiotic relationship between the system and the associated support system.

Implementation of this disciplined approach, including systems engineering activities such as Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), and Reliability Centered Maintenance (RCM), will produce a Maintenance Task Analysis (MTA) directly linked to the system's Reliability Maintainability and Supportability (RMS). The technical input and MTA process identifies support tasks, which are then assessed for affordability and supportability. This in turn produces a Total System Product Support Package that identifies support requirements based upon the inherent reliability and maintainability of the system. This Total System Product Support Package provides detailed descriptions of the:

- Supply Support (Spare/Repair Parts)

- Maintenance Planning
- Test/Support Equipment
- Technical Documentation/Interactive Electronic Technical Manuals
- Manpower & Training/Computer Based Training
- Facilities
- Packaging Handling Storage & Transportation
- Design Interface/Computing Support

Continuous assessment of in-service system performance will identify needs for system improvements to enhance reliability, obsolescence, corrosion, or other Life-Cycle Logistics attributes.

The colored boxes in Figure 5.2.2.1.correspond to the phases of the Defense Acquisition Management Framework (Figure 5.4.1.) and link to the appropriate discussion in section below: yellow/blue = Concept Refinement and Technology Development (Pre-Acquisition), tan/green = Systems Development and Demonstration (Acquisition), and Production and Deployment, and purple = Operations and Support (Sustainment). The gray box on the left links to Pre-Acquisition and Acquisition (Design for Support). The gray box on the right links to Sustainment (Support the Design). It is important to note, however, that these processes are typically iterative and overlapping - thus the boxes overlap. They are not necessarily carried out in a linear progression. Under evolutionary acquisition and incremental/spiral development, systems engineering and Life-cycle logistics processes will often be repeated in progressive loops throughout the program life cycle.

Designing for optimal SOE provides balance. The emphasis is not only on the reliability and maintainability of the prime mission system or equipment to execute mission capability ('Design for Support'), but also on the cost-effective responsiveness and relevance of the support system and infrastructure ('Support the Design').

Achieving Affordable System Operational Effectiveness (SOE). The concept of SOE explains the dependency and interplay between system performance, availability (reliability, maintainability, and supportability), process efficiency (system operations, maintenance, and logistics support), and system life cycle cost. (See the Supportability Guide, Section 2.1.) This overarching perspective provides a context for the "trade space" available to a program manager along with the articulation of the overall objective of maximizing the operational effectiveness of weapon systems. SOE requires proactive, coordinated involvement of organizations and individuals from the requirements, acquisition, logistics, and user communities, along with industry. This applies equally to new weapon systems as well as to major modifications and opportunistic upgrading of existing, fielded systems. In all cases, full stakeholder participation is required in activities related to 'designing for support,' 'designing the support,' and 'supporting the design.' These factors and relationships are depicted in Figure 5.2.2.2. :

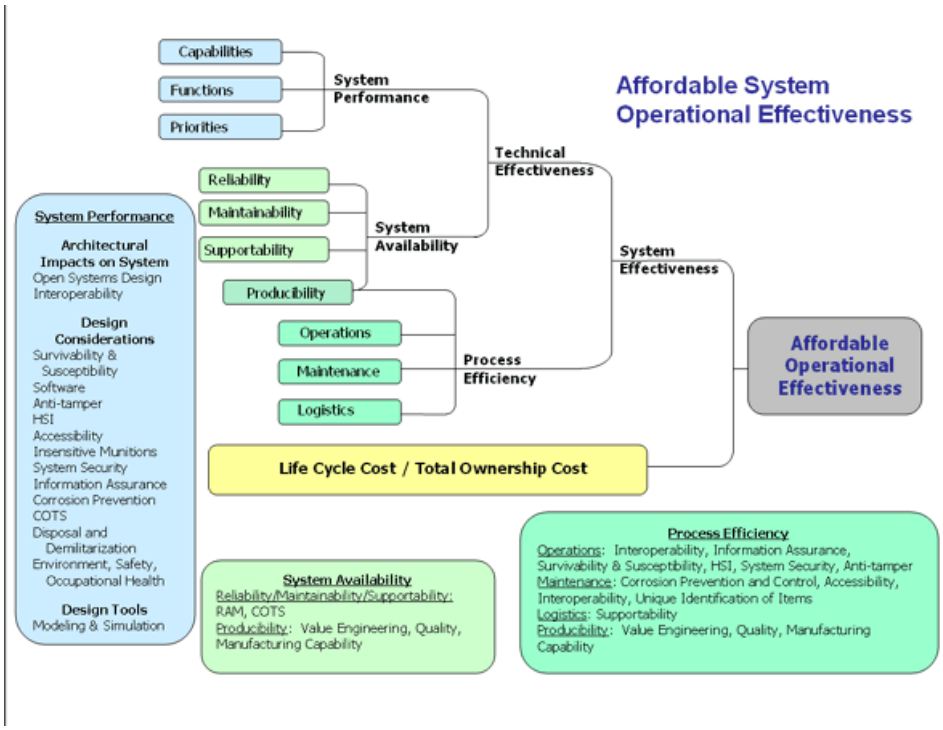

Figure 5.2.2.2. Affordable System Operational Effectiveness

System Performance. System performance is realized through designed-in system ***capabilities*** and ***function*** . In this context, the term ***capabilities*** refers to the various desired performance attributes and measures of the system, such as maximum speed, range, altitude, or weapons delivery accuracy. The term ***functions*** refers to the desired mission capabilities and mission scenarios that the system must be capable of executing in an operational environment. (See the Supportability Guide, section 2.2.1)

Technical Effectiveness. Technical effectiveness reflects the inherent balance between system performance and system availability. These two aspects of the system must be designed- in synergistically and with full knowledge of the expected system missions in the context of a proposed system maintenance concept. (See the Supportability Guide, section 2.2.4)

System Effectiveness. System effectiveness reflects the balance achieved between the technical effectiveness and the process efficiency of the system. In this context, process efficiency is constituted by the system operational, maintenance, and logistics processes. System effectiveness reflects a holistic view of the real mission capability delivered to the field. (See the Supportability Guide, section 2.2.5)

System Availability. The components of system availability are defined to include: reliability, maintainability, supportability (RMS) (see section 4.4.8), and producibility, defined as follows:

- Reliability: The ability of a system to perform as designed in an operational environment over time without failure.
- Maintainability: The ability of a system to be repaired and restored to service when maintenance is conducted by personnel using specified skill levels and prescribed procedures and resources.
- Supportability: The inherent quality of a system - including design, technical support data, and maintenance procedures - to facilitate detection, isolation, and timely repair/replacement of system anomalies. This includes factors such as diagnostics, prognostics, real-time maintenance data collection, 'design for support' and 'support the design' aspects, corrosion protection and mitigation, reduced logistics footprint, and other factors that contribute to an optimum environment for developing and sustaining a stable, operational system (see section 4.4.9). Supportability also includes the degree to which a system's design and planned logistics resources support its readiness requirements and wartime utilization. Unlike reliability or maintainability, supportability includes activities and resources (such as fuel) that are necessary for system operation. It also includes all resources that contribute to the overall support cost (e.g. personnel, equipment, technical data, etc.).
- Producibility: The degree to which the design of the system facilitates the timely, affordable, and optimum-quality manufacture, assembly, and delivery of the system to the customer. Producibility is closely linked to other elements of availability and to costs. Items that feature design for producibility are also normally easier to maintain and have lower life cycle costs. (See section 4.4.6.1.)

Reliability-Centered Maintenance (RCM). RCM is an analytical process, first and foremost, to reduce life cycle cost and is also used to determine preventive maintenance tasks as well as provide recommendations for other actions necessary to maintain a required level of safety, maximize equipment availability, and minimize operating cost. SAE JA1011 (Evaluation Criteria for RCM Programs) and SAE JA1012 (A Guide to the RCM Standard) are illustrative commercial standards for this method. (Supportability Guide)

Process Efficiency. Process Efficiency reflects how well the system can be produced, operated and maintained, and to what degree the logistics infrastructure and footprint have been reduced to provide an agile, deployable, and operationally effective system. Achieving process efficiency requires early and continuing emphasis on producibility, maintenance, and the various elements of logistics support. (See the Supportability Guide, Section 2.2.3)

5.2.3. Sustainment (Support the Design)

The program manager should apply the systems engineering processes for designing and assessing supportability not only during acquisition, but throughout the entire life cycle. These processes should be applied for all modifications including configuration changes resulting from evolutionary acquisition and spiral development. Supportability assessments, coordinated with systems engineering, may identify redesign opportunities for fielded systems that would enhance weapon system operational effectiveness. These

assessments can also identify sub-optimal performers in the fielded product support system, which can be corrected through rebalanced logistics elements or changes to the maintenance program. Designing-in and subsequent continuing assessment of supportability throughout the life cycle is essential to maintaining the effectiveness of fielded systems, and are responsibilities of the program manager.

While acquisition phase activities are critical to designing and implementing a successful and affordable sustainment strategy, the ultimate measure of success is application of that strategy after the system has been deployed for operational use. Warfighters require operational readiness and operational effectiveness – systems accomplishing their missions in accordance with their design parameters in a mission environment. Systems, regardless of the application of design for supportability, suffer varying stresses during actual operational deployment and use.

Accordingly, the DoD Components conduct periodic assessments of system support strategies vis-à-vis actual vs. expected levels of performance and support. Modification of Performance Based Logistics agreements are made as needed, based on changing warfighter requirements or system design changes. When assessing and revising agreements and support strategies, the process should encompass all previous configuration/block increments, and also include elements of System Development and Demonstration phase activities, with an emphasis on not only 'adding on' new support as required, but also on addressing the support strategy in total across the entire platform and range of deployed configurations. This task requires close coordination with appropriate systems engineering IPTs.

5.3. Performance-Based Logistics (PBL)

Performance-Based Logistics (PBL) is DoD's preferred approach for product support implementation (DoD Directive 5000.1). As noted in section 5.1, program managers should establish a Performance Based Logistics approach in fulfilling their product support, integrated supply chain management, and other Life-Cycle Logistics responsibilities. Performance Based Logistics utilizes a performance-based acquisition strategy that is developed, refined, and implemented during the systems engineering process. Performance Based Logistics can help program managers optimize performance and cost objectives through the strategic implementation of varying degrees of Government-Industry partnerships. (See also - Implementing a Performance-Based Business Environment.)

This section discusses Performance Based Logistics and presents a basic methodology for implementing Performance Based Logistics. It then provides detailed discussion of key aspects of PBL: Performance Based Agreements, and Source of Support, which includes Maintenance, Supply, Transportation, and a brief note regarding contractor logistics support.

Performance Based Logistics is the purchase of support as an integrated, affordable, performance package designed to optimize system readiness and meet performance goals for a weapon system through long-term support arrangements with clear lines of authority and responsibility. Application of Performance Based Logistics may be at the system, subsystem, or major assembly level depending on program unique circumstances and

appropriate business case analysis. Additional guidance to help program managers apply Performance Based Logistics is contained in the Product Support Guide, Chapter 1.

The essence of Performance Based Logistics is buying performance outcomes, not the individual parts and repair actions. This is accomplished through a business relationship that is structured to meet the warfighter's requirements. Performance Based Logistics support strategies integrate responsibility for system support in the Product Support Integrator, who manages all sources of support. Source of support decisions for Performance Based Logistics do not favor either organic or commercial providers. The decision is based upon a best-value determination, evidenced through a business case analysis (BCA), of the provider's product support capability to meet set performance objectives. This major shift from the traditional approach to product support emphasizes what level of support program manager teams buy, not who they buy from. Instead of buying set levels of spares, repairs, tools, and data, the new focus is on buying a predetermined level of availability to meet the warfighter's objectives.

One of the most significant aspects of Performance Based Logistics is the concept of a negotiated agreement between the major stakeholders (e.g. the program manager, the force provider(s), and the support provider(s)) that formally documents the performance and support expectations, and commensurate resources, to achieve the desired Performance Based Logistics outcomes. Per DoD Instruction 5000.2, "the program manager shall work with the users to document performance and support requirements in performance agreements specifying objective outcomes, measures, resource commitments, and stakeholder responsibilities." The term 'performance agreements,' as cited in DoD 5000-series policy, is an overarching term suitable for policy guidance. In actual Performance Based Logistics implementation guidance, the more specific term 'performance based agreements' is used to ensure clarity and consistency. Additional discussion of Performance Based Agreements can be found in section 5.3.2, and in DUSD(LMR) Memorandum, March 2003, Implementing the Future Logistics Enterprise End-to-End Customer Support.

Tailoring. It is important to note that each Performance Based Logistics arrangement is unique and will vary from other Performance Based Logistics arrangements. A Performance Based Logistics arrangement may take many forms. There is no one-size-fits-all approach to PBL.

Earned Value Management (EVM). EVM is a valuable program management tool that can be extremely useful in Performance Based Logistics implementation. Please see 11.3.1 for a detailed discussion of EVM.

The Force Provider/Program Manager/Support Provider relationship and Performance Based Agreement linkages are depicted in Figure 5.3.1.

The following are considerations for the program manager in implementing performance based logistics and developing performance based agreements.

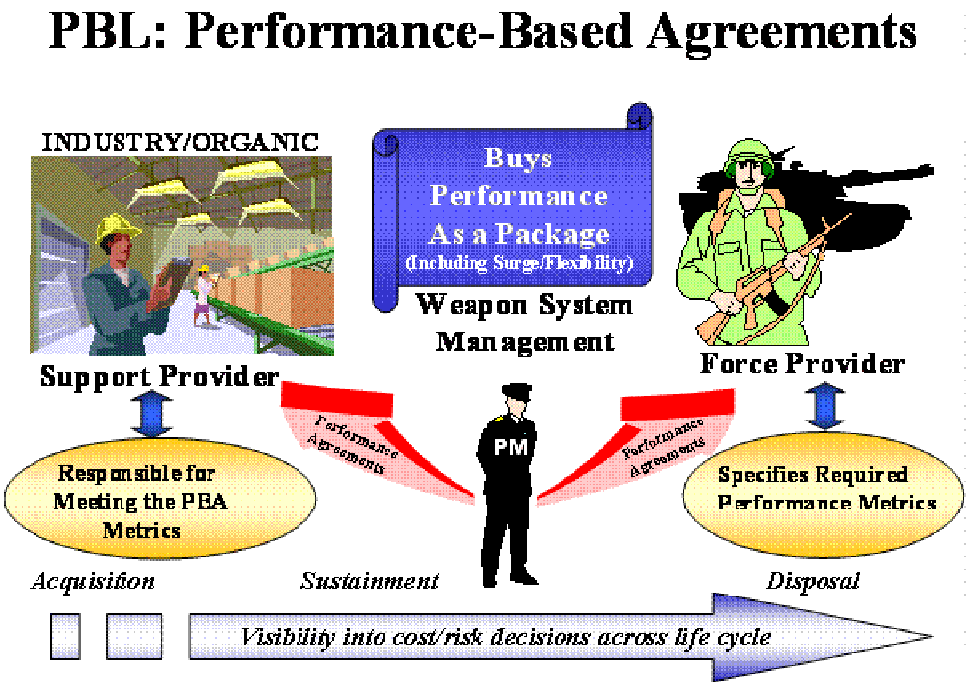

Figure 5.3.1. Performance Based Agreements (Performance Based Agreement)

5.3.1. Methodology for Implementing PBL

Methodology for Implementing Performance Based Logistics (Performance Based Logistics)

The Performance Based Logistics methodology, which is further detailed in the Product Support Guide, is a twelve step process that can be applied to new, modified, or legacy systems:

1. Integrate Requirements and Support. (5.3.1.1)
2. Form the Performance Based Logistics Team. (5.3.1.2)
3. Baseline the System. (5.3.1.3)
4. Develop Performance Outcomes. (5.3.1.4)
5. Select the Product Support Integrator(s). (5.3.1.5)
6. Develop a Workload Allocation Strategy. (5.3.1.6)
7. Develop a Supply Chain Management Strategy. (5.3.1.7)
8. Perform a Performance Based Logistics Business Case Analysis. (5.3.1.8)
9. Establish Performance Based Agreements. (5.3.1.9)

10. Award Contracts. (5.3.10)

11. Employ Financial Enablers. (5.3.11)

12. Implement and Assess. (5.3.12)

This Performance Based Logistics implementation process is not intended to be rigid and inflexible. The program management team should apply the steps presented in a manner that is best suited to the needs of their program, its business and operational environments.

As stated in DoD Directive 5000.1, E1.17, "PMs shall develop and implement performance-based logistics strategies that optimize total system availability while minimizing cost and logistics footprint. Sustainment strategies shall include the best use of public and private sector capabilities through government/industry partnering initiatives, in accordance with statutory requirements." Developing the Performance Based Logistics strategy, formalizing the warfighter performance agreement, and establishing the product support integrator are key components of the product support strategy and should be documented in the acquisition strategy.

Performance-Based Logistics Strategy. A Performance Based Logistics strategy focuses weapon system support on identified warfighter required performance outcomes, rather than on discrete transactional logistics functions. It should balance two major objectives throughout the life cycle of the weapon system: the requirement for logistics support should be minimized through technology insertion and refreshment, and the cost-effectiveness of logistics products and services should be continually improved. Careful balancing of investments in logistics and technology to leverage technological advances through the insertion of mature technology is critical. The program manager should insure that the Performance Based Logistics strategy addresses warfighter requirements during peacetime, contingency operations, and war.

The development of a Performance Based Logistics strategy is a lengthy, complex process, led by the program manager, involving a multitude of stakeholders. No two weapons system Performance Based Logistics strategies are exactly the same – each must be tailored to the unique requirements of the weapon system considering, at minimum, the factors and criteria listed below:

- Statutory requirements: Title 10 U.S.C. (Core, 50/50, public/private partnering, and others).
- Regulatory requirements: DoD Component policy (Contractors on the Battlefield, Service performance of organizational level support functions).
- Sources of support: Completion of the Depot Source of Repair (DSOR) process, market research, optimizing the best mix of public and private capabilities.
- Determining performance outcomes: Ensuring that warfighter performance requirements are commensurate with the available financial resources, ensuring flexibility in Performance Based Agreements to accommodate shifting financial priorities

5.3.1.1. Integrate Requirements and Support

An effective Performance Based Logistics implementation begins in the Joint Capabilities Identification System process by focusing capabilities needs on overall performance and linking supportability to performance. Understanding warfighter needs in terms of performance is an essential initial step in developing a meaningful support strategy. The program management team consults with the operational commands and organizations that support the warfighting combatant commanders. The operational commands are generally the weapon system customers. Their capability needs will be translated into performance and support metrics that will (a) be documented in Performance Based Agreements, and (b) serve as the primary measures of support provider performance. Supportability needs should, as appropriate, also be as a key performance parameter or other 'testable' metric.

Understanding warfighter requirements is not a one-time event. As scenarios change and the operational environment evolves, performance requirements may change. Thus, understanding the requirements is a continual management process for the program manager.

5.3.1.2. Form the Performance Based Logistics Team

The program manager should establish a team to develop and manage the implementation of a Performance Based Logistics weapon system strategy. The team may consist of government and private-sector functional experts; however, it is important that they are able to work across organizational boundaries. Establishing the team is a cultural change, as it will sometimes be difficult to find people who are comfortable sharing information and working outside of functional, stove piped organizations. Team-building within Performance Based Logistics is similar to traditional integrated logistics support management, except the focus on individual support elements is diminished and replaced by a system orientation focused on performance outcome.

The program manager invites DoD Component and Defense Logistics Agency logistics activities to participate in product support strategy development and integrated product teams (IPTs) to ensure that the product support concept is integrated with other logistics support and combat support functions and provide agile and robust combat capability. These participants help to ensure effective integration of system-oriented approaches with commodity-oriented approaches (common support approaches), optimize support to users, and maximize total logistics system value.

Integrating Across Traditional Stovepipe Organizational Boundaries. A team could include representatives from a component command headquarters and logistics representatives from supply, maintenance, and transportation staffs. It could also include representatives from operational commands, engineering, technical, procurement, comptroller, information technology organizations, and contract support. After the team is organized, the members establish their goals, develop plans of action and milestones, and obtain adequate resources.

Establishing the Public/Private Support Strategy IPT(s). These IPTs will ensure consideration, throughout support strategy design and development, of all factors and criteria necessary to achieve an optimum Performance Based Logistics strategy that utilizes the best capabilities of the public and private sectors in a cost effective manner.

5.3.1.3. Baseline the System

Defining and documenting the system baseline answers three key questions: What is the scope of your support requirement? Who are the key stakeholders? What are your cost and performance objectives? Use actual data when available for fielded systems.

To develop an effective support strategy, a program manager needs to identify the difference between existing and desired performance requirements. Accordingly, the program manager identifies and documents the current performance and cost baseline. The life cycle stage of a program determines the scope of a baselining effort. For new programs with no existing logistics structure, the baseline should include an examination of the cost to support the replaced system(s). If there is no replaced system, life cycle cost estimates should be used. For new systems, the business model for supporting the product demonstrates its risks and benefits as part of the systems engineering process. This "proof of concept" for the support solution is part of the system development and demonstration phase. Once identified, the baseline can be used to assess the necessary establishment of, or revisions to, the support concept to achieve the desired level of support.

5.3.1.4. Develop Performance Outcomes

At the top level, the performance outcomes and corresponding metrics should focus on the warfighter's needs: A system that is operationally available, reliable, and effective, with minimal logistics footprint and a reasonable cost.

The formal performance agreement with the warfighter states the objectives that form the basis of the Performance Based Logistics effort. For Performance Based Logistics, "performance" is defined in terms of military objectives, using the following criteria:

1. Operational Availability. The percent of time that a weapon system is available for a mission or ability to sustain operations tempo.
2. Operational Reliability. The measure of a weapon system in meeting mission success objectives (percent of objectives met, by weapon system). Depending on the weapon system, a mission objective would be a sortie, tour, launch, destination reached, capability, etc.
3. Cost per Unit Usage. The total operating costs divided by the appropriate unit of measurement for a given weapon system. Depending on weapon system, the measurement unit could be flight hour, steaming hour, launch, mile driven, etc.
4. Logistics Footprint. The government / contractor size or "presence" of logistics support required to deploy, sustain, and move a weapon system. Measurable elements include inventory / equipment, personnel, facilities, transportation assets, and real estate.
5. Logistics Response Time. This is the period of time from logistics demand signal sent to satisfaction of that logistics demand. "Logistics Demand" refers to systems, components, or resources, including labor, required for weapon system logistics support.

Performance Based Logistics metrics should support these desired outcomes. Performance measures will be tailored by the Military Departments to reflect specific

Service definitions and the unique circumstances of the Performance Based Logistics arrangements. See USD(ATL) Memorandum, August 2004, Performance Based Logistics: Purchasing Using Performance Based Criteria.

Linking these metrics to existing warfighter measures of performance and reporting systems is preferable. Many existing logistics and financial metrics can be related to top-level warfighter performance outcomes. It is important to select only those metrics that are within the control of each Performance Based Logistics provider.

5.3.1.5. Select the Product Support Integrator(s)

The program manager's responsibilities for oversight and management of the product support function are typically delegated to a 'product support manager' (an overarching term characterizing the various Service function titles, i.e. Assistant Program Manager for Logistics, System Support Manager, etc) who leads the development and implementation of the product support and Performance Based Logistics strategies, and ensures achievement of desired support outcomes during sustainment. The product support manager employs a Product Support Integrator (PSI), or a number of PSIs as appropriate, to achieve those outcomes. The PSI is an entity performing as a formally bound agent (e.g. contract, MOA, MOU) charged with integrating all sources of support, public and private, defined within the scope of the Performance Based Logistics agreements to achieve the documented outcomes. The product support manager, while remaining accountable for system performance, effectively delegates responsibility for delivering warfighter outcomes to the PSI. In this relationship, and consistent with "buying performance", the PSI has considerable flexibility and latitude in how the necessary support is provided, so long as the outcomes are accomplished.

Activities coordinated by the PSI can include, as appropriate, functions provided by organic organizations, private sector providers, or a partnership between organic and private sector providers. As with the Performance Based Logistics strategy and the warfighter agreement, the product support integration function is a key component of the product support strategy documented in the acquisition strategy. While product support execution is accomplished by numerous organizational entities, the PSI is the single point of accountability consistent with their level of functional responsibility for integrating all sources of support necessary to meet the agreed to support/performance metrics. Candidates for the integrator role include:

- The system's original equipment manufacturer or prime contractor.
- A DoD Component organization or command.
- A third-party logistics integrator from the private sector.

Further information can be found in the Product Support Guide.

5.3.1.6. Develop a Workload Allocation Strategy

DoD policy requires that "sustainment strategies shall include the best use of public and private sector capabilities through government/industry partnering initiatives, in accordance with statutory requirements." (DoDD 5000.1, E1.17) An effective support strategy considers 'best competencies' and partnering opportunities. To that end, a

workload allocation/sourcing strategy identifies what is best for each support function in terms of: capability, skills, infrastructure, opportunities for partnering, compliance with Title 10, public/private flexibility, and affordability.

5.3.1.7. Develop a Supply Chain Management Strategy

A supply chain management strategy is critical to the success of any Performance Based Logistics effort. Materiel support is a critical link in weapon systems supportability. All the skilled labor, advanced technology, and performance mean little without the 'right part, in the right place, at the right time.' The supply chain is also a primary target for utilizing industry flexibility, capability, and proprietary spares support.

5.3.1.8. Perform a Performance Based Logistics Business Case Analysis

A business case provides a best value analysis, considering not only cost, but other quantifiable and non-quantifiable factors, supporting an investment decision. To effectively provide this justification it is critical that the process, scope, and objectives of the business case developers be clearly understood and communicated. A business case should be developed in an unbiased manner without prejudice, and not be constructed to justify a pre-ordained decision. The analysis should stand on its own and be able to withstand rigorous analysis and review by independent audit agencies. It is expected that the business case will be used throughout the life cycle of the project. Specifically:

- This business case is used in the initial decision to invest in a project.
- It specifically guides the decision to select among alternative approaches.
- The business case also is used to validate any proposed scope, schedule, or budget changes during the course of the project. The business case should be a living document – as project or organization changes occur they should be reflected in updates to the business case.

Finally, the business case should be used to validate that planned benefits are realized at the completion of the project. This information should be used in further decisions to sustain or enhance the solution. This information should also be used to refine estimation of benefits and costs for future projects in the organization.

A Business Case Analysis is an expanded cost/benefit analysis with the intent of determining a best value solution for product support. Alternatives weigh total cost against total benefits to arrive at the optimum solution. The Business Case Analysis process goes beyond cost/benefit or traditional economic analyses by linking each alternative to how it fulfills strategic objectives of the program; how it complies with product support performance measures; and the resulting impact on stakeholders. A Business Case Analysis is a tailored process driven by the dynamics of the pending investment (i.e., Performance Based Logistics) decision. It independently, and without prejudice, identifies which alternative provides optimum mission performance given cost and other constraints, including qualitative or subjective factors. Development of the Performance Based Logistics Business Case Analysis should determine:

- The relative cost vs. benefits of different support strategies.

- The methods and rationale used to quantify benefits and costs.
- The impact and value of Performance/Cost/Schedule/Sustainment tradeoffs.
- Data required to support and justify the Performance Based Logistics strategy.
- Sensitivity of the data to change.
- Analysis and classification of risks
- A recommendation and summary plan of implementation for proceeding with the best value alternative.

The Business Case Analysis becomes an iterative process, conducted and updated as needed throughout the life cycle as program plans evolve and react to changes in the business and mission environment. For further discussion of Performance Based Logistics Business Case Analyses see the Product Support Guide, USD(ATL) Memorandum, January 2004, Performance Based Logistics Business Case Analysis and USD(ATL) Memorandum, March 2004, System Planning Guidance Performance Based Logistics BCA

5.3.1.9. Establish Performance Based Agreements

Warfighter performance based agreements provide the objectives that form the basis of the Performance Based Logistics effort. Generally, a focus on a few performance based outcome metrics – such as weapon system availability, mission reliability, logistics footprint, and overall system readiness levels – will lead to more effective solutions. However, in developing the actual Performance Based Logistics support arrangements, it may not be possible to directly state the warfighter performance objectives as support metrics, due to lack of support provider control of all support activities necessary to produce the warfighter performance (e.g. availability). Most DoD Component logistics policies and/or guidance mandate a preference for DoD Component-performed organizational level maintenance and retail supply functions.

A support provider in a Performance Based Logistics arrangement cannot be held accountable for functions they do not directly perform or manage. Accordingly, the program manager may select the next echelon of metrics for which the support provider can be held accountable, and which most directly contribute to the warfighter performance metrics. The use of properly incentivized ranges of performance to define metrics can provide flexibility and is recommended. Many existing logistics and financial metrics can be related to top-level warfighter performance outcomes. These include, but are not limited to, not mission capable supply (NMCS), ratio of supply chain costs to sales, maintenance repair turnaround time, depot cycle time, and negotiated time definite delivery. In structuring the metrics and evaluating performance, it is important to clearly delineate any factors that could affect performance but are outside the control of the Performance Based Logistics providers.

While objective metrics form the bulk of the evaluation of a Performance Based Logistics provider's performance, some elements of product support requirements might be more appropriately evaluated subjectively by the warfighter and the program manager team. This approach allows some flexibility for adjusting to potential support contingencies.

For example, there may be different customer priorities to be balanced with overall objective measures of performance. (See 5.3.2 and the Product Support Guide)

5.3.1.10. Award Contracts

The preferred Performance Based Logistics contracting approach is the use of long-term contracts with incentives tied to performance. Award term contracts should be used where possible to incentivize optimal industry support. Incentives should be tied to metrics tailored by the Military Departments to reflect their specific definitions and reporting processes. Award and incentive contracts shall include tailored cost reporting to enable appropriate contract management and to facilitate future cost estimating and price analysis. Performance Based Logistics contracts must include a definition of metrics and should be constructed to provide industry with a firm period of performance. Wherever possible, Performance Based Logistics contracts should be fixed price (e.g. fixed price per operating or system operating hour). Lack of data on systems performance or maintenance costs, or other pricing risk factors may necessitate cost type contracts for some early stage Performance Based Logistics. Full access to DoD demand data will be incorporated into all Performance Based Logistics contracts. Performance Based Logistics contracts should be competitively sourced wherever possible and should make maximum use of small and disadvantaged businesses as subcontractors, and may be incentivized to do so through Performance Based Logistics contractual incentives tied to small and disadvantaged business subcontracting goals.

Those purchasing Performance Based Logistics should follow Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) guidance, as appropriate, for the acquisition of logistics services and support, and should seek to utilize FAR Part 12 – "Acquisition of Commercial Items" to acquire Performance Based Logistics as a commercial item. See USD(ATL) Memorandum, August 2004, Performance Based Logistics: Purchasing Using Performance Based Criteria.

A Performance Based Logistics contract specifies performance requirements; clearly delineates roles and responsibilities on both sides; specifies metrics; includes incentives as appropriate; and specifies how performance will be assessed. Performance Based Logistics contracting strategies prefer utilizing an approach characterized by use of a Statements of Objectives versus early development of a detailed Performance Work Statement.

A documented performance-based agreement/contract between the program manager, product support integrator, and force provider that defines the system operational requirements (e.g. readiness, availability, response times, etc.), is essential. The product support manager, PSI, and product support provider(s) will define and include the required support metrics necessary to meet the system performance requirements (DoD Directive 5000.1, E1.29). (See 5.3.3)

5.3.1.11. Employ Financial Enablers

In executing performance agreements, the program manager should implement a financial process strategy that is an enabler. The program manager should estimate annual costs based on operational requirements and review funding streams for applicability. The force provider (customer) advocates for the required funding. Once the

funds have been appropriated, the customer should ensure that the funds are made available as needed to fund the support as defined in the Performance Based Agreement and (if present) subsequent implementing support contract. Although this process does not provide the program manager direct 'control' of the funds for support, it does put them in a clear management and oversight role of the funds used for sustainment.

5.3.1.12. Implement and Assess

The program manager's assessment role includes developing the performance assessment plan, monitoring performance, and revising the product support strategy and Performance Based Agreements as necessary. The program also acts as the agent for the warfighter, certifying PSI performance and approving incentive payments. The program manager should take a 'hands-on' approach and not assume that the contracts/agreements will be self-regulated.

Life cycle assessment identifies and properly addresses performance, readiness, ownership cost, and support issues, and includes post-deployment evaluation to support planning for ensuring sustainment and implementing technology insertion, to continually improve product affordability.

5.3.2. Performance Based Agreements

Performance Based Agreements are one of the key components of an effective product support strategy. (See DoD Directive 5000.1 and DoD Instruction 5000.2.) They establish the negotiated baseline of performance, and corresponding support necessary to achieve that performance, whether provided by commercial or organic support providers. The Program Manager, utilizing the desired performance of the warfighter, negotiates the required level of support to achieve the desired performance at a cost consistent with available support funding. Once the performance, support, and cost are accepted by the stakeholders, the program manager enters into performance-based agreements with users, which specify the level of operational support and performance required by the users. Likewise, program managers enter into performance-based agreements with organic sources and contracts with commercial sources, which focus on supporting the users in terms of cost, schedule, performance, sustainment, and disposal. To coordinate the work and business relationships necessary to satisfy the user agreement, program managers select a product support integrator from the government or private sector, who serves as a single point of accountability to integrate support from all sources to achieve the performance outcomes specified in the performance-based agreement. The agreements maintain flexibility, to facilitate execution year funding and/or priority revisions. Performance Based Agreements also reflect a range of support levels to facilitate revisions in support requirements without preparing new performance based agreements.

5.3.2.1. Performance Based Contracts

For support provided by commercial organizations, the contract is, in most cases, the performance-based agreement. Accordingly, the contract contains the agreed to performance and/or support metrics that have been identified as meeting the requirements of the warfighter. In most cases, the ultimate performance requirements (e.g., Availability) may be precluded as contract metrics because the contractor may not have

full control or authority over all of the support functions that produce system availability – some support functions may continue to be performed by organic organizations or other support providers. Accordingly, the contract metrics reflect the highest level of metric(s) that are the most critical in producing the desired performance outcome(s). In order to motivate the contractor to achieve the desired metrics, appropriate contract incentives include award fee, award term, and cost sharing, which promote and facilitate contractor performance.

5.3.2.2. Agreements with Organic Providers and Users

For support provided by organic organizations, a performance-based agreement, similar in structure to a Memorandum of Agreement, Memorandum of Understanding, or Service Level Agreement may be used in lieu of a contract to represent and document the terms of the performance based agreement for organic support. One important distinction, however, between Performance Based Agreements and other types of Agreements and Understandings is that Performance Based Agreements contain the agreed to performance and/or support metrics that have been identified as meeting the warfighter requirements, and to which the warfighter has agreed to commit funding. The intent of agreements with organic support providers is to formally document the agreed to level of support, and associated funding, required to meet performance requirements. Organic providers, like commercial providers, will have a set of performance metrics that will be monitored, assessed, incentivized, and focused on the target weapon system. The Performance Based Agreement metrics reflect the highest level of metric(s) that are the most critical in producing the desired performance outcome(s).

5.3.3. Source of Support

The program manager should use the most effective source of support that optimizes the balance of performance and life cycle cost, consistent with required military capability and statutory requirements. The source of support may be organic or commercial, but its primary focus should be to optimize customer support and achieve maximum weapon system availability at the lowest LCC. Consistent with DoD Instruction 5000.2, in advance of contracting for operational support services, the program manager shall work with the manpower community to determine the most efficient and cost effective mix of DoD manpower and contract support. Source of support decisions should foster competition throughout the life of the system.

5.3.3.1. Maintenance Source of Support

10 U.S.C. 2464 and DoD policy require organic core maintenance capabilities. Such capabilities provide effective and timely response to surge demands, ensure competitive capabilities, and sustain institutional expertise. Best value over the life cycle of the system and use of existing contractor capabilities, particularly while the system is in production, should be considered key determinants in the overall decision process. The program manager provides for long-term access to the data required for competitive sourcing of systems support and maintenance throughout its life cycle. For additional information and guidance, see DoD Directive 4151.18.

The program manager shall ensure that maintenance source of support selection complies with statutory requirements identified in DoD Instruction 5000.2, Core Logistics Analysis/Source of Repair Analysis.

Core Logistics Capability. 10 U.S.C. 2464 requires core logistics capability that is Government-owned and Government operated (including Government personnel and Government-owned and Government-operated equipment and facilities) to ensure a ready and controlled source of technical competence and resources necessary to ensure effective and timely response to mobilization, national defense contingency situations, or other emergency requirements. These capabilities must be established no later than 4 years after achieving IOC (10 U.S.C. 2464). These capabilities will include those necessary to maintain and repair weapon systems and other military equipment that are identified as necessary to enable the armed forces to fulfill the strategic and contingency plans prepared by the Chairman of the Joint Chiefs of Staff. Excluded are special access programs, nuclear aircraft carriers, and commercial items. Sufficient workload will be provided to maintain these core capabilities and ensure cost efficiency and technical competence in peacetime while preserving surge capacity and reconstitution capabilities necessary to fully support strategic and contingency plans. The program manager ensures that maintenance source of support decisions comply with this statutory requirement.

Depot Maintenance 50 Percent Limitation Requirement. 10 U.S.C. 2466 requires not more than 50 percent of the funds made available in a fiscal year to a military department or defense agency for depot-level maintenance and repair (see 10 U.S.C. 2460), workload be used to contract for performance by non-Federal Government personnel. As this is a military department and agency level requirement and not a weapon system specific requirement, the program manager should not undertake depot maintenance source of support decisions without consultation with accountable acquisition and logistics officials to ensure compliance with this statutory requirement.

Government and Industry Support Partnerships. Public-private partnerships can contribute to more effective DoD maintenance operations, the introduction of innovative processes or technology, and the economical sustainment of organic capabilities. Depot maintenance partnerships can be an effective tool to implement Performance-Based Logistics arrangements. Performance Based Logistics implementation strategies should consider partnering with public depot maintenance activities to satisfy the requirements of 10 U.S.C. 2464 and 10 U.S.C. 2466.

Depot maintenance operations in the Department of Defense can benefit from public-private partnerships that combine the best of commercial processes and practices with the Department's own extensive maintenance capabilities. It is in the mutual interests of both sectors to pursue the establishment and effective operation of partnerships across the widest possible segment of workload requirements.

Maintenance partnerships should be the preferred arrangements for maintaining and repairing DoD weapon systems, hardware, equipment, and software. For additional information and guidance, see DoD policy memorandum, January 30, 2002, Public-Private Partnerships for Depot Maintenance.

5.3.3.2. Supply Source of Support

DoD policy gives the program manager latitude in selecting a source of supply support, including support management functions, that maximizes service to the user, while minimizing cost. The program manager should select a source of supply support that gives the program manager and/or the support integrator sufficient control over financial and support functions to effectively make trade-off decisions that affect system readiness and cost. Supply requirements will be determined as a part of the maintenance planning process to ensure delivery of an integrated product.

Competitive Process. Supply support may be included as part of the overall system procurement or as a separate competition. The competitive selection process will result in a contract with a commercial source and/or an agreement with an organic source that prescribes a level of performance in terms of operational performance and cost. The program manager may use a competitive process to select the best value supply support provider, or supply support may be included in an overarching Performance Based Logistics support arrangement with a Product Support Integrator. While access to multiple sources of supply may be encouraged to reduce the risks associated with a single source, it is imperative that a single entity (e.g. the Product Support Integrator or a Prime Vendor arrangement) be established as a focal point of responsibility. Particular attention should be given to Prime Vendor contracts for specific commodities and Virtual Prime Vendor contracts for a wide range of parts support for specific subsystems. Additional guidance appears in DoD Directive 4140.1 and DoD 4140.1-R.

Organic Supply Source of Support. The program manager selects organic supply sources of support when they offer the best value (DoD Directive 5000.1 E1.17). When changing the support strategy for fielded equipment from organic support to contractor support or from contractor support to organic support, DoD-owned inventory that is unique to that system should be addressed in the source of support decision.

5.3.3.3. Transportation Source of Support

The program manager is encouraged to determine the best overall support strategy for the customer to include the use of all available transportation alternatives, and alternatives which may be provided by Original Equipment Manufacturers (OEMs) or commercial vendors. These alternatives may include the use of commercial transportation services and facilities to the maximum extent practicable; the use of organic transportation consistent with military needs; or the combination of both commercial and organic transportation to support customer requirements. In considering transportation options, program manager must also plan for transition of the supply and distribution chain from normal operations to expeditionary operations in austere locations that are not served, at least initially, by commercial transportation services and facilities. As in supply support, the program manager should strive to structure a support arrangement, such as Performance Based Logistics, that will consolidate the responsibility for transportation in a single entity, such as the Product Support Integrator.

Facilitating Vendor Shipments in the DoD Organic Distribution System. Many vendor contracts require vendors to distribute materiel using door-to-door commercial transportation. However, during certain circumstances such as crisis situations and contingency operations, door-to-door commercial delivery may not be possible. If this occurs, materiel enters the DoD organic distribution system for delivery to the ultimate

user. Such materiel is often insufficiently marked and labeled, and subsequently it becomes 'frustrated.' To reduce the amount of frustrated materiel, program managers are advised that when it is known prior to award that shipments under the contract will enter the DoD organic distribution system, the contract and/or delivery order should require the contractor to comply with the business rules in DoD policy memorandum, July 23, 2003, *Facilitating Vendor Shipments in the DoD Organic Transportation System*. All solicitations requiring that deliveries be made using door-to-door commercial transportation must include a provision that requires vendors to notify the contracting officer or the contracting officer's designee when they are unable to use door-to-door commercial transportation and to request alternate shipping instructions. The contracting officer or contracting officer's designee must expeditiously provide alternate shipping instructions and make the appropriate contract price adjustments. For additional information, visit the on-line Transportation Policy Library.

Arms, Ammunition, and Explosives. Program Managers are encouraged to refer to DoD 4500.9-R, Defense Transportation Regulation, Part 2, for transportation considerations regarding the movement of Arms, Ammunition, and Explosives.

5.3.3.4. Contractor Logistics Support/Contractors on the Battlefield (CLS/COTB) Integration, In-Theater

Civilian contractors can execute support missions in a variety of contingency operations. When support strategies employ contractors, program managers should, in accordance with Joint Publication 4-0 Chapter 5 and DoD Component implementing guidance, coordinate with affected Combatant Commanders. This coordination is carried out through the lead Service and ensures functions performed by contractors, together with functions performed by military personnel and Government civilians, are integrated in operations plans (OPLAN) and orders (OPORD).

Joint Publication 4-0 Chapter 5 also requires Combatant Commanders to:

- *Identify operational specific contractor policies and requirements, to include restrictions imposed by international agreements;*
- *Include contractor-related deployment, management, force protection, medical, and other support requirements, in the OPORD or a separate annex; and*
- *Provide this information to the DoD Components to incorporate into applicable contracts.*

The intent of the coordinated planning outlined above is to ensure the continuation of essential contractor services in the event the contractor provider is unable (or unwilling) to provide services during a contingency operation. Contingency plans are required for those tasks that have been identified as essential contractor services to provide reasonable assurance of continuation during crisis conditions in accordance with DoD Instruction 3020.37. In accordance with DoD Instruction 5000.2, program managers should also coordinate with the DoD Component manpower authority in advance of contracting for operational support services to ensure that tasks and duties that are designated as inherently governmental or exempt are not contracted.

5.4. Key Life-Cycle Logistics (LCL) Activities in the System Life Cycle

An acquisition program is structured in phases, which are separated by milestone decisions, in accordance with the Defense Acquisition Management Framework established in DoD Instruction 5000.2. In each phase of a program's life cycle, from concept to disposal, there are important Life-cycle logistics issues and actions to be addressed by the program manager.

This section provides an overview of key LCL activities and outputs in the context of the Defense Acquisition Management Framework, as depicted in Figure 5.4.1., to help program managers effectively implement LCL, Total Life Cycle Systems Management (TLCSM), and Performance Based Logistics. By placing the topics discussed in previous sections in the context of the Framework, this section provides a basic roadmap program managers can follow to achieve LCL goals. This section can also serve as a benchmark for assessment of program Performance Based Logistics implementation in the design and development of weapon systems and associated sustainment strategies.

This section is by no means a complete discussion of all the activities a program manager must carry out during each acquisition phase and in preparation for each milestone. The purpose of this section is to highlight important LCL related activities and issues a program manager should be aware of at appropriate points in the Acquisition Framework. Many of the issues discussed are applicable to multiple phases and the deliverables must be updated during subsequent phases, increments, or spirals. For a complete discussion of all the activities and requirements encompassed in the Defense Acquisition Management Framework see DoD Instruction 5000.2. A complete and detailed discussion of LCL throughout the life cycle can be found in the TLCSM Template published by the USD(AT&L) and in Chapter 3 of the Supportability Guide.

Figure 5.4.1. depicts the Defense Acquisition Management Framework and breaks out the LCL related design and systems engineering activities discussed in section 5.2. The colored boxes correspond to the colored boxes in Figure 5.2.2.1. Again, it is important to note that these processes are not carried out in a strictly linear progression, they are typically carried out in iterative, progressive loops in keeping with evolutionary acquisition and spiral development. The colored phase boxes (upper) are linked to the appropriate text below. The colored breakout boxes (lower) are linked to the appropriate text in section 5.2.

Evolutionary acquisition presents new challenges and benefits to the program manager in both acquisition and sustainment activities. An obvious challenge is the potential cost and configuration control problems that can arise with multiple configurations of end-items as well as the support system. This must be addressed early in development and evolution of the acquisition strategy. If planned correctly, configuration control efforts can provide the program manager the opportunity to observe and evolve the success of tentative support strategies.

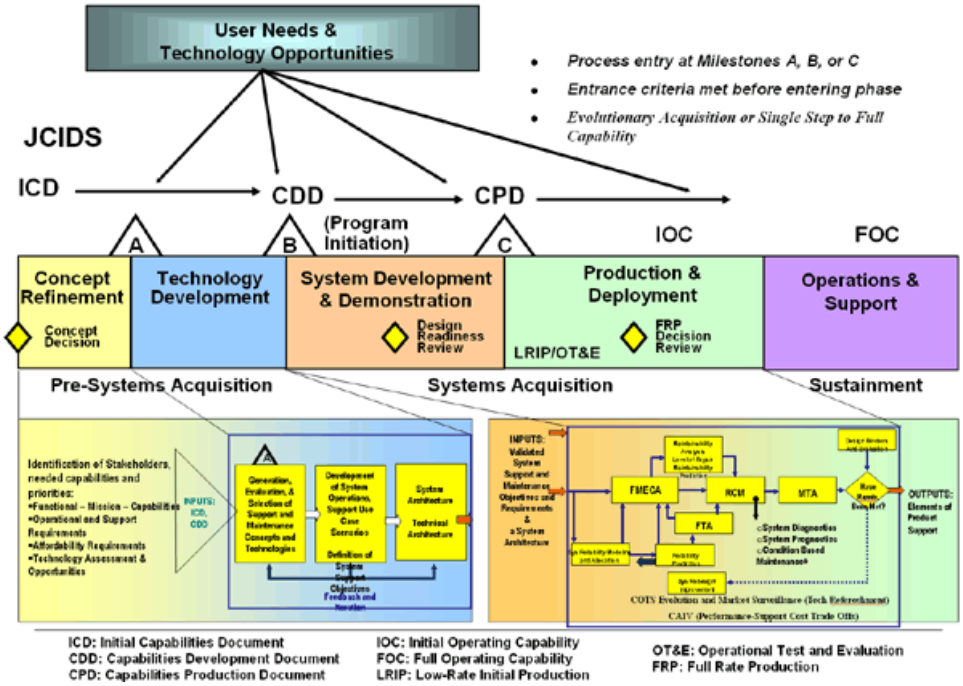

Figure5.4.1. Defense Acquisition Management Framework

5.4.1. Pre-Acquisition

Pre-acquisition presents the first substantial opportunity to influence weapon systems supportability and affordability by balancing threat scenarios, technology opportunities, and operational requirements. Emphasizing the critical performance-sustainment link, desired user capabilities should be defined in terms not only of objective metrics (e.g. speed, lethality) of performance to meet mission requirements affordably, but also of the full range of operational requirements (logistics footprint, supportability criteria) to sustain the mission over the long term. Assessment and demonstration of technology risk includes those related to supportability and to product support. Reliability, reduced logistics footprint, and reduced system life cycle cost are most effectively achieved through inclusion from the very beginning of a program – starting with the definition of needed capabilities.

LCL in the Joint Capabilities Integration and Development System (Joint Capabilities Integration and Development System) process. An effective and affordable LCL support program should be represented as a performance capability priority. As discussed in section 1.3, the Joint Capabilities Integration and Development System process documents operational phase technical and support-related performance capabilities where warfighters, or their operational user representatives, identify needed supportability and support-related performance capabilities parameters (RMS, cost per operating hour, diagnostic effectiveness, etc.). Planning, resourcing, and allocation of resources for logistics supportability should be mapped to these specific warfighter needs

for support-related system performance. Further, program management can more easily invest in Condition Based Maintenance Plus (CBM+) and related embedded instrumentation technology, when they are tied to Joint Capabilities Integration and Development System performance capability parameters. Affordable operational effectiveness is the overarching LCL goal that should be considered during the Joint Capabilities Integration and Development System process.

The Joint Capabilities Integration and Development System analysis process is composed of a structured, four-step methodology that defines capability gaps, capability needs, and approaches to provide those capabilities within a specified functional or operational area. Based on national defense policy and centered on a common joint warfighting construct, the analyses initiate the development of integrated, joint capabilities from a common understanding of existing joint force operations and doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) capabilities and deficiencies. The Joint Capabilities Integration and Development System analyses are led by the sponsor. The Joint Capabilities Integration and Development System process is initiated prior to concept refinement and remains linked into the Defense Acquisition Management Framework at each phase and milestone.

LCL-related Joint Capabilities Integration and Development System direction — for both the initial establishment of supportability and support-related performance criteria and for each evolutionary increment — includes the following:

- Cost (with threshold/objectives) is to be included in the Joint Capabilities Integration and Development System Capability Development Document as “life cycle” costs (CJCSM 3170.01, p. E-A-6, 15).
- Logistics supportability should be treated as an operational performance capability that’s inherent to systems design and development (CJCSI 3170.01, p. A-9, (b)).
- Functional needs analysis must include supportability as an inherent part of defining capability needs (CJCSI 3170.01, p. A-4, 2(a)).
- Within the "capabilities based" approach to setting formal warfighter requirements, "supportability" is a key attribute to be defined (CJCSI 3170.01, p. A-5, e(1)).
- Logistics supportability is an inherent element of both Operational Effectiveness and Operational Suitability (CJCSI 3170.01, p. GL-11, by definition).
- Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities (DOTMLPF) considerations include key logistics criteria that will help minimize logistics footprint and reduce cost (CJCSM 3170.01, p E-A-5, 13).
- The Joint Capabilities Integration and Development System process validates each increment’s support-related performance capability parameters, their threshold and objective values, and related metrics and measures of effectiveness.

Initial Capabilities Document. Joint Capabilities Integration and Development System analyses provide the necessary information for the development of the Initial Capabilities Document. In the Initial Capabilities Document, the user should document those lessons

learned and cost drivers of current systems, and/or constraints that impact the supportability-related design requirements of the planned system, along with those of the support system. The following LCL 'drivers' should be considered in the Initial Capabilities Document:

- System Maintenance/Support Profiles and Use Case Scenarios (Support Capability Packages)
- Reliability and Maintenance Rates
- Support Environment and Locations for Support
- Support and Maintenance Effectiveness
- Duration of Support

These details guide the acquisition community in refining the concept selected in the Initial Capabilities Document and identifying potential constraints on operating and support resource requirements.

5.4.1.1. Concept Refinement Leading to Milestone A

The Concept Refinement phase refines the selected concept through development of an approved Analysis of Alternatives, leading to development of a Technology Development Strategy. This phase begins with the Milestone Decision Authority approving the Analysis of Alternatives Plan and establishing a date for Milestone A review, all documented in an Acquisition Decision Memorandum.

Table 5.4.1.1.1. identifies documents and activities that should incorporate or address supportability/logistics considerations during the Concept Refinement phase. 'Entry Documents' should be completed when the phase is initiated. 'Exit Documents/Activities' are completed or updated during the phase, prior to exit. Links to relevant supportability/logistics discussions are provided in the right hand column.

Supportability/Logistics Considerations in Concept Refinement	
Entry Documents:	
Initial Capabilities Document	5.4.1.
Analysis of Alternatives Plan	5.4.1.1.1.
Exit Documents/Activities:	
Analysis of Alternatives	5.4.1.1.1.
Technology Development Strategy	5.4.1.1.2., Supportability Guide
Consideration of Technology Issues	5.4.1.1.2., Supportability Guide
Test and Evaluation Strategy	5.4.1.2.1., paragraph 5

Table 5.4.1.1.1. Supportability/Logistics Considerations in Concept Refinement

5.4.1.1.1. LCL Deliverables During Concept Refinement

Performance Parameters – LCL Focus. Identification of LCL performance and related support parameters for inclusion in the Capability Development Document and other

deliverables establishes their basis as design requirements for subsequent phases to affect availability, reliability, maintainability, interoperability, manpower, and deployment footprint – the overall capability of the system to perform and endure in the required mission operational environment. (DoD Instruction 5000.2)

An excellent example of a useful LCL performance parameter is Operational Availability (A_o). A_o is a calculation of various supportability functions at the systems level. The desired result of performing these calculations, coincident with system design, is to provide fielded systems with greater capability for the warfighter and enhanced support at the best possible value. A_o provides a method of predicting and assessing system performance and readiness during the acquisition process and then becomes the performance benchmark during initial operational capability (IOC), deployment, and operations/maintenance cycles.

Analysis of Alternatives. Analysis of alternatives is the evaluation of the operational effectiveness, operational suitability, and estimated cost of alternative systems to meet a mission capability. Operational effectiveness measures the overall ability of a system to accomplish a mission, including its supportability. Operational suitability is the degree to which a system can be placed and sustained satisfactorily in field use with consideration given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, habitability, manpower, logistics, supportability, natural environment effects and impacts, documentation, and training requirements. It is very important that the Analysis of Alternatives includes alternative operating and system support concepts, with specific consideration of performance-based options. The Analysis of Alternatives should consider the physical and operational maintenance environment of the proposed system. Data collected and analyzed during Analysis of Alternatives can be very useful for performing a Performance Based Logistics business cases analysis. (See 3.3.1 and 3.3.3)

It is important to note that LCL-related data in all program deliverables must be updated during subsequent phases, especially prior to milestone decisions.

5.4.1.1.2. Life-Cycle Logistics (LCL) Considerations During Concept Refinement

Important LCL related issues to be addressed during Concept Refinement, as well as in later phases, include (but are not limited to): technology maturity, modular open systems approach, and sustainability.

Maturity, use of Commercial Off-the-Shelf Items. Technology risk must receive intensive consideration as the system concept is developed (see section 4.4.1) Maximum use of mature technology provides the greatest opportunity to hold fast to program cost, schedule, and performance requirements and is consistent with an evolutionary acquisition approach.

Modular Open Systems Approach (MOSA). (See DoD Directive 5000.1.) Program managers apply MOSA as an integrated business and technical strategy upon defining user needs. Program managers assess the feasibility of using widely supported commercial interface standards in developing systems. MOSA should be an integral part of the overall acquisition strategy to enable rapid acquisition with demonstrated technology, evolutionary and conventional development, interoperability, Lifecycle

supportability, and incremental system upgradeability without major redesign during initial procurement and reprocurement of systems, subsystems, components, spares, and services, and during post-production support. It should enable continued access to cutting edge technologies and products and prevent being locked in to proprietary technology. Program managers should document their approach for using MOSA and include a summary of their approach as part of their overall acquisition strategy.

Sustainability. Sustainability is the ability to maintain the necessary level and duration of operational activity to achieve military objectives (section 5.2.2). Sustainability is a function of providing for and maintaining those levels of ready forces, materiel, and consumables necessary to support military effort.

RMS. Emphasis on RMS (section 4.4.8) and producibility during Concept Refinement and later phases is guided by a concise understanding of concept of operations, system missions, mission profiles, and capabilities. Such understanding is invaluable to understanding the rationale behind functional and performance priorities. In turn, this rationale paves the way for decisions about necessary trade-offs between system performance, availability, and system cost, with impact on the cost effectiveness of system operation, maintenance, and logistics support. The focus on RMS must be complemented by emphasis on system manufacturing and assembly, both critical factors related to the production and manufacturing, and to the sustainment cost of complex systems.

5.4.1.2. Technology Development leading to Milestone B

Upon approval of the Technology Development Strategy and selection of an initial concept, the project enters the Technology Development phase at Milestone A. The purpose of this phase is to reduce technology risk and determine the appropriate set of technologies to be integrated into a full system.

Table 5.4.1.2.1 identifies documents and activities that should incorporate or address supportability/logistics considerations during the Technology Development phase. ‘Entry Documents’ should be completed when the phase is initiated. ‘Exit Documents/Activities’ are completed or updated during the phase, prior to exit. Links to relevant supportability/logistics discussions are provided in the right hand column.

Supportability/Logistics Considerations in Technology Development	
Entry Documents:	**Relevant discussion:**
Analysis of Alternatives	5.4.1.1.1.
Technology Development Strategy	5.4.1.1.2., Supportability Guide (3.3, p. 21)
Market Analysis	Supportability Guide (3.3, p. 22)
Consideration of Technology Issues	5.4.1.1.2.,Suportability Guide (3.3, p. 23)
Test and Evaluation Strategy	5.4.1.2.1 para 5
Exit Documents/Activities:	**Relevant discussion:**

Analysis of Alternatives	5.4.1.1.1.
Technology Development Strategy	5.4.1.1.2.
Initial Capabilities Document and Capability Development Document	5.4.1 para 5, 5.4.2 para 2
Technology Readiness Assessment	5.4.1.1.2., Supportability Guide (3.3, p. 21)
Information Support Plan	5.1.3.2, 5.1.3.3, 5.1.3.4
Acquisition Strategy	5.4.1.2.1 para 1
Industrial Capabilities	5.2.2 para 12 & 14
Core Logistics Analysis/Source of Repair Analysis	5.3.3.1 para 3
Competition Analysis for Depot-Level Maintenance >$3M	5.3.3.1 para 3
Cooperative Opportunities	5.1.3.2.
Test and Evaluation Master Plan (TEMP)	5.4.1.2.1 para 5
Live-Fire Waiver and Alternative LFT&E Plan	5.4.1.2.1 para 5
Operational Test Agency Report of OT&E Results	5.4.1.2.1 para 5
Independent Cost Estimate and Manpower Estimate	5.1.3.5, 5.1.3.6
Affordability Assessment	5.1.3.5
DoD Component Cost Analysis	5.1.3.5, 5.1.3.6
Acquisition Program Baseline (APB)	5.1.3 para 5, 5.4.1.2.1 para 4

Table 5.4.1.2.1. Supportability/Logistics Considerations in Technology Development

5.4.1.2.1. LCL Deliverables During Technology Development

Acquisition Strategy. LCL and product support is an integral part of the weapon system support strategy that program managers develop as part of their acquisition strategy (see section 5.1.3). Product Support is defined as a package of logistics support functions necessary to maintain the readiness and operational capability of a system or subsystem. The package of logistics support functions includes functions such as materiel management, distribution, technical data management, maintenance, training, cataloging, configuration management, engineering support, repair parts management, failure reporting and analysis, and reliability growth. The Acquisition Strategy documents the Product Support Strategy.

Product Support Strategy. Program managers are responsible for laying out and executing a strategic blueprint for the logistics process so that every part of the package is integrated and contributes to the warfighter's mission capability. The product support strategy is reviewed and updated at least every five years, or when support metrics are not being met (USD(ATL) Memorandum, March 2003, TLCSM & PBL, p. 9). Program managers balance multiple objectives in designing the strategy to achieve operational effectiveness while maintaining affordability. The program manager, product support provider(s) will define and include the required support metrics necessary to meet the system performance requirements. Support providers may be public, private, or a mix to include public-private partnerships. Examples of public support providers include DoD Component maintenance depots, DoD Component and Defense Logistics Agency

inventory control points and distribution depots. The program manager, product support integrator, and the support provider(s) will enter into documented performance-based agreements that define and include the required support metrics necessary to meet the system performance requirements. Further discussion of the Product Support Strategy can be found in sections 5.1.3.

Statutory, Policy, and Guidance Factors. The product support strategy must ensure compliance with all statutory and regulatory requirements, and in particular the statutory limitations of Title 10 United States Code, Sections 2464, 2466, and 2469. Congress has enacted a number of statues that place controls on what actions the Department can take in using commercial sector maintenance capabilities. These legislative and statutory issues must be considered as an integral and evolving aspect of product support acquisition decisions.

Acquisition Program Baseline. As discussed in section 5.1.3, program managers must ensure that a description of the appropriate logistics metrics, criteria, and funding requirements are included in the APB (see section 2.1.1).

Test and Evaluation Master Plan. Proper testing of supportability is critical to achieve LCL goals and objectives, as demonstrated in section 5.2. Program managers must therefore ensure that a description of the appropriate logistics considerations and test points are included in the Test and Evaluation Master Plan (DoD Instruction 5000.2 and Guidebook section 9.6.2).

Work Breakdown Structure (WBS). The Work Breakdown Structure (WBS) is a system management tool very commonly used by program managers and industry. Created early in the life of a program, the Work Breakdown Structure (WBS) identifies deliverable work products (such as products, work packages, activities, tasks, etc.). These work products are then further sub-divided into successively smaller units until individual tasks can be assigned to people or organizations. This allows responsibility to be assigned for individual tasks and provides traceability from low-level tasks to high level work products. It is important for the Work Breakdown Structure (WBS) to consider and account for LCL and related Total Life Cycle Systems Management considerations. (See MIL-HDBK-881).

The Work Breakdown Structure (WBS) is often used early in the life of the program to generate initial cost estimates, program plans, and to support contracting and reporting. The Work Breakdown Structure (WBS) can also be used to help create a program schedule. The initial Work Breakdown Structure (WBS) may be modified by adding additional tasks or re-assigning personnel as more is learned about the system during the design process.

It is important to note that LCL related data in all program deliverables must be updated during subsequent phases, especially prior to milestone decisions.

5.4.1.2.2. Life-Cycle Logistics (LCL) Considerations During Technology Development

Commercial Integration (Items and Processes). Market analysis for system and product support capabilities (public and private) defines the extent and scope of

opportunities for achieving support objectives through design and viable product support strategies. Analysis should include:

- Elements of support currently provided (for a legacy system to be replaced).
- Current measures used to evaluate support effectiveness.
- Current efficacy of required support.
- All existing support data across the logistics support elements.
- Assessment of existing technologies and associated support that impact the new system under development.

Cost/Schedule/Performance/Supportability Trade-Offs. The best time to reduce LCC and program schedule is early in the acquisition process. Continuous cost/schedule/performance/ supportability trade-off analyses can accomplish cost and schedule reductions. Cost, schedule, performance, and supportability may be traded within the "trade space" between the objective and the threshold without obtaining Milestone Decision Authority approval. Trade-offs outside the trade space (i.e., program parameter changes) can require approval of both the Milestone Decision Authority and Validation Authority. Validated key performance parameter (KPP) threshold values cannot be reduced without Validation Authority approval (CJCSM 3170.01, pp. B-4 (3), F-4 9b). The program manager and the operational capabilities needs developer jointly coordinate all trade-off decisions.

5.4.2. Acquisition

The system formally enters the acquisition process at Milestone B, when Milestone Decision Authority approval permits the system to enter the System Development and Demonstration phase (section 5.4.2.1). A key Life-Cycle Logistics (LCL) emphasis during System Development and Demonstration is to ensure operational supportability with particular attention to minimizing the logistics footprint. Also during this phase, the support concept and strategy are refined and potential Performance Based Logistics Product Support Integrators and providers are identified. This is the most critical timeframe to optimize system sustainment through designed-in criteria.

Capability Development Document. The Capability Development Document is the sponsor's primary means of defining authoritative, measurable, and testable capabilities needed by the warfighters to support the System Development and Demonstration phase of an acquisition program. The Capability Development Document captures the information necessary to deliver an affordable and supportable capability using mature technology within a specific increment of an acquisition strategy. The following LCL 'drives' should be considered in the Capability Development Document:

- System Maintenance/Support Profiles and Use Case Scenarios (Support Capability Packages)
- Reliability and Maintenance Rates
- Support Environment and Locations for Support
- Support and Maintenance Effectiveness

- Duration of Support

5.4.2.1. System Development and Demonstration leading to Milestone C

The purposes of System Development and Demonstration are to: develop a system; reduce integration and manufacturing risk; ensure operational supportability with particular attention to reducing the logistics footprint; implement human systems integration; design for producibility; ensure affordability and protection of critical program information; and demonstrate system integration, interoperability, safety, and utility. In System Development and Demonstration, the program and the system architecture are defined based upon the selection and integration of the mature technology suite accomplished during Concept Refinement and Technology Development.

During System Development and Demonstration, system design requirements are allocated down to the major subsystem level. The support concept and strategy are refined, and potential Performance Based Logistics Product Support Integrator and providers are identified. Life-Cycle Logistics (LCL) documents and analyses are refined as a result of developmental and operational tests, and iterative systems engineering analyses. LCL is also an important component of the technical reviews, such as the Critical Design Review, conducted during System Development and Demonstration. The Systems Engineering Plan (SEP) should identify the process for development and update of the Failure Modes, Effects & Criticality Analysis (FMECA) matrix; Failure Reporting, Analysis & Corrective Action System (FRACAS); and Trend Analysis for maturation purposes of the weapon system and its support system.

Table 5.4.2.1.1. identifies documents and activities that should incorporate or address supportability/logistics considerations during System Development and Demonstration. 'Entry Documents' should be completed when the phase is initiated, beginning System Integration, and at the mid-phase Design Readiness Review initiating System Demonstration (see the Supportability Guide (3.4, p. 27) for further explanation). 'Exit Documents/Activities' are completed or updated during the phase, prior to exit. Links to relevant supportability/logistics discussions are provided in the right hand column.

Supportability/Logistics Considerations in System Development and Demonstration	
Entry Documents (System Integration):	**Relevant discussion:**
Initial Capabilities Document and Capability Development Document	5.4.1 para 5, 5.4.2 para 2
Acquisition Strategy	5.4.1.2.1 para 1
Technology Development Strategy	5.4.1.1.2, Supportability Guide (3.3, p. 21)
Acquisition Program Baseline	5.1.3 para 5, 5.4.1.2.1 para 4
Entry Documents (System Demonstration):	**Relevant discussion:**
Design Readiness Review	Supportability Guide (3.4, p. 27)
Developmental Test and Evaluation Report	5.4.1.2.1 para 5
Operational Test Plan	5.4.1.2.1 para 5

Exit Documents/Activities :	Relevant discussion:
Update documents from MS B as appropriate.	See table 5.4.1.2.1.
Capability Production Document	5.4.2.1 para 7

Table 5.4.2.1.1. Supportability/Logistics Considerations in Technology Development

System Design for Affordable Operational Effectiveness. As discussed in section 5.1.1, the Total Life Cycle Systems Management approach increases the significance of design for system reliability, maintainability, manufacturability, and supportability. The inherent objective of Total Life Cycle Systems Management is to enhance warfighter capability through improved SOE for new and fielded weapon systems. SOE is the composite of performance, availability, process efficiency, and life cycle cost (see section 5.1.3). The objectives of the SOE concept can best be achieved through influencing early design and architecture and through focusing on system design for affordable operational effectiveness. The SOE concept provides a framework within which trade studies can be conducted in a proactive manner.

LCL Systems Engineering Processes. Figures 5.2.2.1. and 5.4.1. show how key selected system reliability, maintainability, and supportability engineering processes (in the tan boxes), which are part of the overall systems engineering process, fit within the Defense Acquisition Management Framework. A Failure Modes and Effects Criticality Analysis helps identify the ways in which systems can fail, performance consequences, and the support remedies for system failures. A Fault Tree Analysis assesses the safety-critical functions within the system's architecture and design. A Maintainability Analysis and Prediction assesses the maintenance aspects of the system's architecture, including maintenance times and resources. A level of repair analysis optimally allocates maintenance functions for maximum affordability. Once the Failure Modes and Effects Criticality Analysis, a Fault Tree Analysis, and a Maintainability Analysis and Prediction are completed and system design has been established, Reliability-Centered Maintenance develops a focused, cost-effective system preventive maintenance program.

Performance Based Logistics Business Case Analysis. During this phase, the Performance Based Logistics Business Case Analysis is developed to determine the relative cost vs. benefits of different support strategies; the impact and value of performance/cost/schedule/sustainment trade-offs; and the data required to support and justify the Product Support Integrator strategy. See section 5.3.1.3for further discussion of a Product Support Integrator Business Case Analysis.

Product Support Integrator. A concluding step in refining a product support strategy, prior to the Milestone C decision, is establishing a product support integrator function. For further information on selecting the Product Support Integrator, see the Product Support Guide.

Capability Production Document. The Capability Production Document is the sponsor's primary means of providing authoritative, testable capabilities for the Production and Deployment phase of an acquisition program. A Capability Production Document is finalized after design readiness review and is validated and approved before

the Milestone C acquisition decision. The following LCL 'drives' should be considered in the Initial Capabilities Document:

- System Maintenance/Support Profiles and Use Case Scenarios (Support Capability Packages)
- Reliability and Maintenance Rates
- Support Environment and Locations for Support
- Support and Maintenance Effectiveness
- Duration of Support

5.4.2.2. Production and Deployment

The purpose of the Production and Deployment phase is to achieve an operational capability that satisfies mission needs. Milestone C authorizes entry into Low-Rate Initial Production (LRIP), at which time the system design should be sufficient to initiate production. The system level technical requirements have been demonstrated to be adequate for acceptable operational capability. At this point, the product support strategy is fully defined, a PSI (Product Support Integrator) has been selected, and Performance Based Logistics agreements that reflect performance, support, and funding expectations should be documented and signed. Funding should be identified and available for testing and implementation of the selected performance based logistics strategy with a selected Product Support Integrator.

Table 5.4.2.2.1. identifies documents and activities that should incorporate or address supportability/logistics considerations during Production and Deployment. 'Entry Documents' should be completed when the phase is initiated. 'Exit Documents/Activities' are completed or updated during the phase, prior to exit. Links to relevant supportability/logistics discussions are provided in the right hand column.

Supportability/Logistics Considerations in Production and Deployment	
Entry Documents:	**Relevant discussion:**
Capability Development Document and Capability Production Document	5.4.2 para 2, 5.4.2.1
Exit Documents/Activities :	**Relevant discussion:**
Update documents from MS C as appropriate.	See table 5.4.2.1.1.
LFT&E Report	5.4.1.2.1 para 5
DoD Component LFT&E Report	5.4.1.2.1 para 5
Information Supportability Certification	5.1.3.2, 5.1.3.3, 5.1.3.4
Post-Deployment Review	5.1.3.7, 5.4.3.2

Table 5.4.2.2.1. Supportability/Logistics Considerations in Technology Development

Pre-Initial Operational Capability Supportability Review and Analysis. This review should be performed at the DoD Component-level to:

- Confirm design maturity of the system.
- Determine status of correction of any deficiencies identified.
- Confirm configuration control.
- Certify product support integrator/providers plan to meet warfighter requirements.
- Verify product support integrator/providers agreements/contracts and funding are in place.

Establish Ongoing Support Strategy Review Process. Under Total Life Cycle Systems Management, the program manager is responsible for the product and related support activities throughout the life cycle. To accomplish this it is necessary for the program manager to establish an ongoing review process. Reviews should be conducted at defined intervals throughout the life cycle to identify needed revisions and corrections, and to allow for timely improvements in these strategies to meet performance requirements.

5.4.3. Sustainment: Operations and Support

While acquisition phase activities are critical to designing and implementing a successful and affordable sustainment strategy, the ultimate measure of success is application of that strategy after the system has been deployed for operational use. Total Life Cycle Systems Management, through single point accountability, and Performance Based Logistics, by designating performance outcomes vs. segmented functional support, enables that objective. Warfighters require operational readiness and operation effectiveness – systems accomplishing their missions in accordance with their design parameters in a mission environment. Systems, regardless of the application of design for supportability, will suffer varying stresses during actual operational deployment and use.

5.4.3.1. Continuing Post-IOC Product Support Strategy Assessments

The DoD Components conduct Post Deployment Reviews, periodic assessments of system support strategies vis-à-vis actual vs. expected levels of performance and support (USD(ATL) Memorandum, March 2003, TLCSM & PBL, p. 9). These reviews occur nominally every three to five years after IOC or when precipitated by changes in requirements/design or performance problems, and should at minimum include:

- Product Support Integrator/Provider performance.
- Product improvements incorporated.
- Configuration control.
- Modification of performance based logistics agreements as needed based on changing warfighter requirements or system design changes.

The program manager should perform reviews of PSI/PSP performance against the Performance Based Agreement on at least a quarterly basis and utilize that data to prepare for the DoD Component-level assessments.

5.4.3.2. Continuous Assessment and Product Improvements

Assessment and revision of agreements and support strategies should encompass all previous configuration/block increments, as well as elements of System Development and Demonstration phase activities. Life cycle assessments address not only 'adding on' new support as required, but also the total support strategy across the entire platform and range of deployed configurations.

Under TLCSM, the program manager assesses proposed system modifications in light of supportability and logistics support impact. Continued assessment of in-service system performance may identify system redesign needs to address inadequate characteristics, e.g., reliability, obsolescence, etc.

While some system deficiencies are best addressed through system design, many can be resolved by adjusting the product support strategy itself. Often, due to revisions in funding, mission requirements, or support organizations, logistics resources become out of balance or poorly-synchronized. Therefore, program manager efforts to increase weapon system availability while reducing life cycle costs and logistics footprint must include periodic assessments and, where necessary, improvements of the product support strategy (USD(ATL) Memorandum, March 2003, TLCSM & PBL, p. 9). Approaches useful to the program manager in making these improvements include:

- A Maintenance Plan Analysis: This analysis can help balance logistics support through thorough review of readiness degraders, maintenance data, maintenance program and implementation, and industrial coordination.
- Performance Based Agreements: Under a Performance Based Logistics strategy, properly documented and incentivized Performance Based Agreements with support providers encourage product support assessment and improvements. Performance-based agreements facilitate comparison of performance expectations against actual performance data.
- Changes to Product Support: Program managers can revise, correct, and improve product support strategies to meet performance requirements. Program managers can improve system supportability by balancing logistics resources and decreasing repair cycle times. Examples of product support improvements include performing an overhaul vs. repair, changing maintenance plans, improving off-aircraft diagnostic capabilities, transitioning to a commercial supply chain management system, etc.

The ability to continually compare performance against expectations takes actual equipment and support performance data to drive operational data analyses and a RCM decision analysis. Results are implemented through maintenance plan changes.

5.5. Life-Cycle Logistics (LCL) Tools and References

The following tools and references provide further information on LCL and its implementation throughout the program life cycle.

5.5.1. The Professional Logistics Workforce: A Key Enabler.

The professional logistics workforce is critical to the success of LCL efforts and the achievement of DoD's overall logistics goals. It is the program manager's primary resource for understanding and implementing LCL.

DoD is required to maintain "a fully proficient acquisition, technology, and logistics workforce that is flexible and highly skilled across a range of management, technical, and business disciplines" (DoD Directive 5000.1). This workforce provides "cradle-to-grave" support, not only in laboratories and program offices, but also in product centers, inventory control points, maintenance depots, and other Life-cycle logistics organizations. LCL requires the logistics workforce to be more diversified in their skill sets and proficient in executing a performance-based support philosophy. To that end, USD(AT&L) has worked with the DoD Components and the Defense Acquisition University to update the logistics training criteria for Life Cycle Logisticians and enhance the logistics workforce's ability to support Total Life Cycle Systems Management and Performance Based Logistics initiatives. Further information on education, training, and career development programs for the workforce can be found in the Acquisition Community Connection, Logistics Management Training Center.

5.5.2. The Acquisition Community Connection (ACC) and the Logistics Community of Practice (LOG CoP)

The Acquisition Community Connection, sponsored by the Defense Acquisition University (DAU), is a tool to facilitate collaboration, sharing, and the transfer of knowledge across the DoD AT&L workforce. ACC is a collection of communities of practice centered on different functional disciplines within the acquisition community. The Logistics Community of Practice (LOG CoP), is one of the communities currently residing within the ACC framework. LOG CoP provides a number of resources for implementing Lifecycle logistics. The community space also allows members to share (post to the website) their knowledge, lessons learned and business case related material so that the entire logistics community can access and benefit. The intention is to make LOG CoP the *"go to"* resource for the logistics community.

5.5.3. Total Life Cycle Systems Management (TLCSM) Template

The TLCSM template, developed by the USD(AT&L), provides a synopsis of the key activities and outputs to assist program managers in effectively implementing TLCSM and Performance Based Logistics within the defense acquisition management framework. The template is a useful benchmark for assessment of program implementation of Performance Based Logistics in the design and development of weapon systems and associated sustainment strategies.

5.5.4. Business Case Guidance

Business case development and analysis is a tailored process. The scope of a product support investment decision substantiated by the business case can range from a complete system-of-systems, to that of individual sub-system components. Likewise, each DoD Component has established ownership and structure of how business case development and analysis are conducted to support their investment decisions. For this reason, one specific approach, format, or template may not fit all situations. The LOG CoP contains

numerous references, guides, and templates to assist in business case development and analysis.

5.5.5. Performance Based Agreement Templates and Guidance

In addition to providing guidance and detailed explanations of Performance Based Logistics and related concepts, sample Performance Based Agreements, policy and guidance, contractual incentives and other resources are available under the Performance Based Logistics section of LOG CoP.

5.5.6. Performance Based Agreement Process for Organic Supply Support

The Performance Based Agreement process is the framework for creating and sustaining end-to-end user support and begins with collaborative, direct negotiations between DoD supply sources of support and their warfighter users (see section 5.3.2). The Performance Based Agreement represents the codification of the negotiated user requirements and performance expectations. The Performance Based Agreement development stages are: *Evaluating Current Conditions, Gain Commitment to Proceed, Define Scope and Objectives and Finalize Agreement, Execute Agreement/Assess Results, and Identify Improvements*. These 5 stages are intended to guide the user through the basic process steps required to develop and implement a Performance Based Agreement. The LOG Cop has a Performance Based Agreement Toolkit.

5.5.7. Performance Based Agreement Template for Organic Supply Support

An End to End Customer Support Performance Based Agreement template has been developed to provide DoD organizations a common framework, a 'checklist' to consider, when undertaking a performance based type agreement that may involve one or more supply chain support services. This template is guidance and not direction on how a Performance Based Agreement should be structured. As the Performance Based Agreement development and implementation process matures, "best practices" will evolve and define the Performance Based Agreement structure and content. Performance Based Agreement terms and definitions can be found in the appendix. Consider the following elements when developing a Performance Based Agreement: Objective and Scope; Content; Roles and Responsibilities; Performance Measures; Revisions and Flexibility; Accountability and Oversight; Contingency Agreements; Execution of Agreement.

5.5.8. Time Definite Delivery Tool

Time Definite Delivery (TDD) plays a significant role in end-to-end user support. Defined as the capability to deliver required materiel to the user within a given period of time with 85 percent reliability, TDD is an important metric to gauge user support. To aid the program manager in determining a TDD tailored to a particular user, a TDD tool was created to compute DoD requisition delivery performance for the total pipeline time (TPT) tailored by user for possible use in initial negotiations of performance agreements. The tool is available at the Office of The Assistant Deputy Under Secretary of Defense (Logistics & Materiel Readiness) Supply Chain Integration web site.

5.5.9. Designing and Assessing Supportability in DoD Weapon Systems

This guide provides a template for program managers when assigned or responsible activities to use in defining and assessing their program activities to meet QDR objectives and DoD policy requirements throughout the weapon system life cycle. Emphasis is placed on designing for increased reliability and reduced logistics footprint and on providing for effective product support through performance-based logistics (PBL) strategies. (The Supportability Guide)

5.5.10. Product Support: A Program Manager's Guide to Buying Performance

This guide presents a performance-based logistics (PBL) strategy for product support of weapon systems. The guide is a tool for program managers as they design product support strategies for new programs or major modifications, or as they reengineer product support strategies for legacy weapon systems.

5.5.11. White Paper: Performance Agreements

A discussion of the performance agreements within Performance Based Logistics can be found in this white paper entitled Performance Agreements as a Critical Component of Performance Based Logistics, which was developed by OADUSD (Logistics Plans and Programs).

5.5.12. Environment, Safety and Occupational Health (ESOH)

DoD ESOH Guidance for systems acquisition programs can be found in Chapter 4 Systems Engineering (4.4.11) and in the ESOH Special Interest Area on the Acquisition Community Connection.

5.5.13. Web References

This section contains a table designed to reference applicable Section 6 paragraphs to appropriate reference guide materials found on Web sites or attached as enclosures containing program examples, best practices illustrations, lessons learned and supporting guidance.

Section	Section Title	Link Name	Web Address
5.1	Lifecycle Logistics	DoD Directive 5000.1	http://dod5000.dau.mil/DOCS/DoD%20Dire signed%20(May%2012,%202003).doc
		Quadrennial Defense Review	http://www.defenselink.mil/pubs/qdr2001.pd
		Joint Vision 2020	http://www.dtic.mil/jointvision/
		Focused Logistics Campaign Plan	http://www.dtic.mil/jcs/j4/projects/foclog/foc
		DUSD(L&MR) Memo 6Nov01 Product Support Guide	http://www.acq.osd.mil/log/logistics_materie /product_support/new_prd_spt_gde/morales_
		DoD Instruction 5000.2	http://dod5000.dau.mil/DOCS/DoDI%20500 signed%20(May%2012,%202003).doc
		DoD 4140.1-R	http://www.dtic.mil/whs/directives/corres/htr
		USD(AT&L) Memo 7Mar03 TLCSM & Performance Based Logistics	http://acc.dau.mil/simplify/ev.php?URL_ID= RL_SECTION=201&reload=1062159864
		DoD 4160.21-M-1	http://www.dtic.mil/whs/directives/corres/htr
		Log Cop Training Center	http://acc.dau.mil/simplify/ev.php?URL_ID= RL_SECTION=201
5.2	LCL Systems Design	Supportability Guide	http://acc.dau.mil/
		DoD policy memorandum, September 4, 2002, Serialized Item Management	http://www.acq.osd.mil/log/logistics_materie ts/general_policy/SIMmemo.pdf
		DoD policy memorandum, July 29, 2003, Policy for Unique Identification (UID) of Tangible Items-New	http://www.acq.osd.mil/uid/uid_signed_polic

		Equipment, Major Modifications, and Reprocurement of Equipment and Spares	
		BEA-Log	www.bea-log.com
5.3	Performance Based Logistics (PBL)	DUSD(L&MR) Memorandum 6Mar03, Implementing the Future Logistics Enterprise End-to-End Customer Support	http://www.acq.osd.mil/log/logistics_materie endtoend_distribution/End%20to%20End.pd
		Product Support Guide	http://acc.dau.mil/simplify/ev.php?URL_ID= RL_SECTION=201&reload=1066831465
		10 U.S.C. 2464	http://www4.law.cornell.edu/uscode/10/2464
		DoD Directive 4151.18	http://www.dtic.mil/whs/directives/corres/htr
		10 U.S.C. 2466	http://www4.law.cornell.edu/uscode/10/2466
		DoD policy memorandum, January 30, 2002, Public-Private Partnerships for Depot Maintenance	http://www.acq.osd.mil/log/logistics_materie ts/depot_partnerships /public_private_partnerships_02.pdf
		DoD Directive 4140.1	http://www.dtic.mil/whs/directives/corres/htr
		DoD 4140.1-R	http://www.dtic.mil/whs/directives/corres/htr
		DoD Directive 4500.9	http://www.acq.osd.mil/log/logistics_materie ns_programs /defense_trans_library/5009/5009.html
		DoD policy memorandum, July 23, 2003, Facilitating Vendor Shipments in the DoD Organic Transportation System	http://www.acq.osd.mil/log/logistics_materie ns_programs/defense _trans_library/policy_facilitating_vendor_shi ution_system.pdf
		Defense TP Library	http://www.acq.osd.mil/log/tp/
		DoD 4500.9-R	www.transcom.mil/j5/pt/dtr.html
		Joint Pub 4-0 Chp 5	http://www.dtic.mil/doctrine/jel/new_pubs/jp
		DoD 4000.25-1-M Military Standard Requisitioning and Issue Procedures (MILSTRIP)	http://www.dtic.mil/whs/directives/corres/htr
		Subpart 251.1 Contractor Use of Government Supply	http://www.acq.osd.mil/dp/dars/dfars/html/r2

		Sources	
5.4	LCL Key Activities in the Program Life Cycle	CJCSI 3170.01	http://www.dtic.mil/cjcs_directives/cdata/unl
5.5	LCL Tools and References	ACC	http://acc.dau.mil
		Log COP	http://log.dau.mil
		TLCSM Template	http://acc.dau.mil/simplify/ev.php?URL_ID= RL_SECTION=201&reload=1062159864
		Customer Support Performance Based Agreement template	http://www.acq.osd.mil/log/logistics_materie toolkit/pba/pba_template_v1_may2003.pdf
		Time Definite Delivery Tool	http://www.acq.osd.mil/log/logistics_materie d.html
		Program Manager's Guide to Buying Performance	http://acc.dau.mil/simplify/ev.php?URL_ID= RL_SECTION=201&reload=1066394562
		Whitepaper: Performance Agreements	http://acc.dau.mil/simplify/ev.php?URL_ID= RL_SECTION=201&reload=1066394651
		ESOH Guidance	http://acc.dau.mil/simplify/ev.php?URL_ID= L_SECTION=201
		DoD Instruction 4500.9	http://www.dtic.mil/whs/directives/corres/htr

Table 5.5.13.1. Web references.

Chapter 6
Human Systems Integration (HSI)

6.0. Overview

DoD acquisition policy requires optimizing total system performance and minimizing the cost of ownership through a “total system approach” to acquisition management (see DoD Directive 5000.1).

6.0.1. Purpose

While Chapter 4 discusses systems engineering at large, this chapter specifically addresses the human systems elements of the systems engineering process. This chapter provides the Program Manager with the necessary background and understanding to design and develop systems that effectively and affordably integrate with human capabilities and limitations, it makes the program manager aware of the staff resources available to assist in this endeavor.

6.0.2. Contents

This chapter has six main sections. Section 6.1 briefly reviews the total systems approach directed by DoD Directive 5000.1. Section 6.2 describes each of the domains of Human Systems Integration: Manpower, Personnel, Training, Human Factors, Safety and Occupational Health, Personnel Survivability, and Habitability. Each of these sub-sections contains an overview of the domain, addresses domain requirements, and ends with a discussion of planning considerations, with one exception. Section 6.3 stands alone to provide extensive discussion and planning details for the Human Factors Engineering domain. Section 6.4then follows with the implementation of HSI, to include formulation of the HSI strategy and the sequencing of expected HSI activities along the timeline of the Defense Acquisition Framework. Section 6.5 describes the human considerations associated with resource estimating and planning; it is the HSI complement to Chapter 3. The last section, Section 6.6, provides two reference listings for additional information.

6.1. Total System Approach

The total system includes not only the prime mission equipment, but also the people who operate, maintain, and support the system; the training and training devices; and the operational and support infrastructure. Human Systems Integration (HSI) analysts assist program managers by focusing attention on the human part of the system and by integrating and inserting manpower, personnel, training, human factors, safety, occupational health, habitability, and personnel survivability considerations into the Defense acquisition process. Consistent with DoD Instruction 5000.2, when addressing HSI, the program manager must focus on each of the "domains" of HSI.

6.2. Human Systems Integration Domains

6.2.1. Manpower

6.2.1.1. Manpower Overview

Manpower factors are those job tasks, operation/maintenance rates, associated workload, and operational conditions (e.g., risk of hostile fire) that are used to determine the number and mix of military and DoD civilian manpower and contract support necessary to operate, maintain, support, and provide training for the system. Manpower officials contribute to the Defense acquisition process by ensuring that the program manager pursues engineering designs that optimize manpower and keep human resource costs at affordable levels (i.e., consistent with strategic manpower plans). Technology approaches and solutions used to reduce manpower requirements and control Lifecycle costs should be identified in the capabilities documents early in the process. For example, material-handling equipment can be used to reduce labor-intensive material-handling operations and embedded training can be used to reduce the number of instructors.

6.2.1.2. Manpower Parameters/Requirements

DoD Directive 5000.1 directs the DoD Components to plan programs based on realistic projections of the dollars and manpower likely to be available in future years. Manpower goals and parameters should be based on manpower studies and analysis. They should ensure that design options that reduce workload and ensure program affordability are pursued, and that lower-priority design features do not take precedence. Throughout the system life cycle, they should keep ownership costs and manpower at desired levels. And they should preserve future-year resources designated for other higher priority programs (i.e., not required later, additional funding)

When there are Congressional or Administrative caps placed on military end strength, the introduction of a new system or capability will require compensating reductions (trade-offs) elsewhere in the force structure or in the Individuals Account. Manpower officials should identify areas for offsets, or “bill-payers,” for the new system and establish constraints based on available resources. If the new system replaces a system in the inventory, manpower officials should determine whether the constraints placed on the predecessor system also apply to the new system. They should consider the priority of the new system and determine if either additional resources will be provided or more stringent constraints will apply. Manpower authorities should consider the availability of resources over the life of the program and weigh competing priorities when establishing manpower constraints for acquisition programs. Reviews should consider all military and civilian manpower and contract support needed to operate, maintain, support, and provide training for the system over the entire life of the program.

Manpower can be a major determinant of program cost and affordability. The Capability Development Document should identify any manpower constraints that, if exceeded, would require the Department to reconsider the utility of the program. The Capability Development Document should specify the expected location of the system on the battlefield and the expected operational conditions (e.g., a high [or low] likelihood of hostile fire or collateral damage). These specifications affect early cost, manpower mix, training, personnel, and survivability requirements.

The Capability Development Document should establish manpower parameters (objectives and thresholds) consistent with existing departmental constraints. If the

program is manpower intensive, it may be prudent to establish a manpower key performance parameter (KPP) early in the acquisition process. Setting a KPP will ensure the system fits within manpower parameters established by the Department, that agreed-upon resource thresholds are not exceeded, and that the system will not require additional resources from higher priority programs later in the acquisition process. A KPP should only be established if the adverse manpower effect of exceeding the KPP outweighs the overall benefits of the new capability. In all cases, manpower constraints and KPPs must be defendable and commensurate with the priority and utility of the new capability.

The CDD Capability Development Document should also address specific, scenario-based, factors that affect manpower, such as surge requirements, environmental conditions (e.g., arctic or desert conditions), and expected duration of the conflict. These factors are capability-related and directly affect the ability of the commander to sustain operations in a protracted conflict.

6.2.1.3. Manpower Planning

Manpower analysts determine the number of people required, authorized, and available to operate, maintain, support, and provide training for the system. Manpower requirements are based on the range of operations during peacetime, low intensity conflict, and wartime. They should consider continuous, sustained operations and required surge capability. The resulting Manpower Estimate accounts for all military (Active Reserve, and Guard), DoD civilian (U.S. and foreign national), and contract support manpower.

DoD Instruction 5000.2 requires the program manager to work with the manpower community to determine the most efficient and cost-effective mix of DoD manpower and contract support, and identify any issues (e.g., resource shortfalls) that could impact the program manager's ability to execute the program. Generally, the decision to use DoD civilians and contract labor in theater during a conflict where there is a high likelihood of hostile fire or collateral damage is made on an exception basis. In all cases, risk reduction shall take precedence over cost savings. Additionally, the program manager shall consult with the manpower community in advance of contracting for operational support services to ensure that sufficient workload is retained in-house to adequately provide for career progression, sea-to-shore and overseas rotation, and combat augmentation. The program manager should also ensure that inherently governmental and exempted commercial functions are not contracted. These determinations shall be based on the Manpower Mix Criteria.

Consistent with sections E1.4 and E1.29 of DoD Directive 5000.1, the program manager must evaluate the manpower required and/or available to support a new system and consider manpower constraints when establishing contract specifications to ensure that the human resource demands of the system do not exceed the projected supply. The assessment must determine whether the new system will require a higher, lower, or equal number of personnel than the predecessor system, and whether the distribution of ranks/grade will change. Critical manpower constraints must be identified in the Capability Development Document to ensure that manpower requirements remain within DoD Component end-strength constraints. If sufficient end-strength is not available, a request for an increase in authorizations should be submitted and approved as part of the trade-off process.

When assessing manpower, the system designers should look at labor-intensive (high-driver) tasks. These tasks might result from hardware or software interface design problems. These high-driver tasks can sometimes be eliminated during engineering design by increasing equipment or software performance. Based on a top-down functional analysis, an assessment should be conducted to determine which functions should be automated, eliminated, consolidated, or simplified to keep the manpower numbers within constraints.

Manpower requirements should be based on task analyses that are conducted during the functional allocation process and consider all factors including fatigue; cognitive, physical, sensory overload; environmental conditions (e.g., heat/cold), and reduced visibility. Additionally, manpower must be considered in conjunction with personnel capabilities, training, and human factors engineering trade-offs.

Tasks and workload for individual systems, systems-of-systems, and families-of-systems should be reviewed together to identify commonalities, merge operations, and avoid duplication. The cumulative effects of system-of-system, family-of-systems and related system integration should be considered when developing manpower estimates.

When reviewing support activities, the program manager should work with manpower and functional representatives to identify process improvements, design options, or other initiatives to reduce manpower requirements, improve the efficiency or effectiveness of support services, or enhance the cross-functional integration of support activities.

The support strategy should document the approach used to provide for the most efficient and cost-effective mix of manpower and contract support and identify any cost, schedule, or performance issues, uncompleted studies that could impact the program manager's ability to execute the program.

6.2.2. Personnel

6.2.2.1. Personnel Overview

Personnel factors are those human aptitudes (i.e., cognitive, physical, and sensory capabilities), knowledge, skills, abilities, and experience levels that are needed to properly perform job tasks. Personnel factors are used to develop the military occupational specialties (or equivalent DoD Component personnel system classifications) and civilian job series of system operators, maintainers, trainers, and support personnel. Personnel officials contribute to the Defense acquisition process by ensuring that the program manager pursues engineering designs that minimize personnel requirements, and keep the human aptitudes necessary for operation and maintenance of the equipment at levels consistent with what will be available in the user population at the time the system is fielded.

6.2.2.2. Personnel Parameters/Requirements

DoD Instruction 5000.2 requires the program manager to work with the personnel community to define the performance characteristics of the user population, or "target audience," early in the acquisition process. The program manager should work with the personnel community to establish a Target Audience Description (TAD) that identifies

the cognitive, physical, and sensory abilities-i.e., capabilities and limitations, of the operators, maintainers, and support personnel that are expected to be in place at the time the system is fielded. When establishing the TAD, HSI analysts should verify whether there are any recruitment or retention trends that could significantly alter the characteristics of the user population over the life of the system. Additionally, HSI analysts should consult with the personnel community and verify whether there are new personnel policies that could significantly alter the scope of the user population (e.g., policy changes governing women in combat significantly changed the anthropometric requirements for occupational specialties).

Per DoD Instruction 5000.2, to the extent possible, systems shall not be designed to require cognitive, physical, or sensory skills beyond those found in the specified user population. During functional analysis and allocation, tasks should be allocated to the human component consistent with the human attributes-i.e., capabilities and limitations, of the user population to ensure compatibility, interoperability, and integration of all functional and physical interfaces. Personnel requirements should be established consistent with the knowledge, skills, and abilities (KSAs) of the user population that is expected to be in place at the time the system is fielded and over the life of the program. Personnel requirements are usually stated as a percentage of the population. For example, the Capability Development Document might require "physically accommodating the central 90% of the target audience." Setting specific, quantifiable, personnel requirements in the Capability Development Document assists establishment of test criterion in the TEMP.

6.2.2.3. Personnel Planning

Personnel capabilities are normally reflected as knowledge, skills, abilities (KSAs), and other characteristics. The availability of personnel and their KSAs should be identified early in the acquisition process. The DoD Components have a limited inventory of personnel available, each with a finite set of cognitive and psychomotor abilities. This could affect specific system thresholds.

The program manager should use the target audience description (TAD) as a baseline for personnel requirements assessment. The TAD should include information such as inventory; force structure; standards of grade authorizations; personnel classification (e.g., MOS/NEC) description; biographical information; anthropometric data; physical qualifications; aptitude descriptions as measured by the Armed Forces Vocational Aptitude Battery (ASVAB)); task performance information; skill grade authorization; physical profile (PULHES); security clearance; and reading grade level.

The program manager should assess and compare the cognitive and physical demands of the projected system against the projected personnel supply. The program manager should also determine the physical limitations of the target audience (e.g., color vision, acuity, and hearing). The program manager should identify and shortfalls highlighted by these studies.

The program manager should determine if the new system contains any aptitude-sensitive critical tasks. If so, the program manager should determine if it is likely that personnel in the target audience can perform the critical tasks of the job.

The program manager should consider personnel factors such as availability, recruitment, skill identifiers, promotion, and assignment. He/She should consider the impact on recruiting, retention, promotions, and career progression when establishing program costs, and should assess these factors during trade-off analyses.

The program manager should use a truly representative sample of the target population during T&E to get an accurate measure of system performance. A representative sample during T&E will help identify aptitude constraints that affect system use.

Individual system and platform personnel requirements should be developed in close collaboration with related systems throughout the Department and in various phases of the acquisition process to identify commonalities, merge requirements, and avoid duplication. The program manager should consider the cumulative effects of system-of-systems, family-of-systems, and related systems integration in the development of personnel requirements

Consistent with DoD Instruction 5000.2, Enclosure 7, the program manager must summarize major personnel initiatives that are necessary to achieve readiness or rotation objectives or to reduce manpower or training costs, when developing the acquisition strategy. The acquisition and support strategy must address modifications to the knowledge, skills, and abilities of military occupational specialties for system operators, maintainers, or support personnel if the modifications have cost or schedule issues that could adversely impact program execution. The program manager should also address actions to combine, modify, or establish new military occupational specialties or additional skill indicators, or issues relating to hard-to-fill occupations if they impact the program manager's ability to execute the program.

6.2.3. Training

6.2.3.1. Training Overview

Training is the learning process by which personnel individually or collectively acquire or enhance predetermined job-relevant knowledge, skills, and abilities by developing their cognitive, physical, sensory, and team dynamic abilities. The "training/instructional system" integrates training concepts and strategies and elements of logistic support to satisfy personnel performance levels required to operate, maintain, and support the systems. It includes the "tools" used to provide learning experiences such as computer-based interactive courseware, simulators, and actual equipment (including embedded training capabilities on actual equipment), job performance aids, and Interactive Electronic Technical Manuals.

6.2.3.2. Training Parameters/Requirements

When developing the training/instructional system, the program manager should employ transformational training concepts, strategies, and tools such as computer based and interactive courseware, simulators, and embedded training consistent with the strategy, goals and objectives of the Training Transformation Strategic Plan (March 1, 2002) and the Training Transformation Implementation Plan and Appendix 1 (June 2004).

The Departments vision for Training Transformation is to provide dynamic, capabilities-based training in support of national security requirements across the full spectrum of Service, joint, interagency, intergovernmental, and multinational operations. This new approach emphasizes the mission requirements of the combatant commanders (COCOM). The COCOM is the customer. The intent is to design systems and structure acquisition programs focused on the training needs of the COCOM. The desired outcome is to fully support COCOM requirements, missions, and capabilities, while preserving the ability of the DoD Components to train for their core competencies. The Under Secretary of Defense for Personnel and Readiness, as a member of the Defense Acquisition Board, assesses the ability of the acquisition program to support the Military Departments, COCOMs, and DoD Components.

"Training," in this context, includes training, education, and job-performance aiding. Joint training must be able to support a broad range of roles and responsibilities in military, multinational, interagency, and intergovernmental contexts, and the Department of Defense must provide such training to be truly flexible and operationally effective. Training readiness will be assessed and reported, not only in the traditional joint context, but also in view of this broader range of "joint" operations. Joint training and education will be recast as components of lifelong learning and made available to the Total Force-active, reserve, and DoD civilians. The Department will expand efforts to develop officers well versed in joint operational art. The interfaces between training systems and the acquisition process will be strengthened. The Under Secretary of Defense for Personnel and Readiness, as a member of the Defense Acquisition Board, assesses an acquisition program's ability to support the Combatant Commander's and DoD Components' capabilities to provide HSI as an integral part of an acquisition program.

The program manager should summarize major elements of the training plan in the Support Strategy. This should include logistics support planning for training, training equipment and training device acquisitions and installations.

***A Special Note on Embedded Training*.** Both the sponsor and the program manager should give careful consideration and priority to the use of embedded training as defined in DoD Directive 1322.18: “Capabilities built into, strapped onto, or plugged into operational materiel systems to train, sustain, and enhance individual and crew skill proficiencies necessary to operate and maintain the equipment.” The sponsor’s decisions to use embedded training should be made very early in the capabilities determination process. Analysis should be conducted to compare the embedded training with more traditional training media (e.g., simulator based training, traditional classroom instruction, and/or maneuver training) for consideration of a system’s Total Operating Cost. The analysis should compare the costs and the impact of embedded training (e.g., training operators and maintenance personnel on site compared to off station travel to a temporary duty location for training). It should also compare the learning time and level of effectiveness (e.g., higher “kill” rates and improved maintenance times) achieved by embedded training. When making decisions about whether to rely exclusively on embedded training, analysis must be conducted to determine the timely availability of new equipment to all categories of trainees (e.g., Reserve and Active Component units or individual members). For instance, a National Guard tank battalion that stores and maintains its tanks at a central maintenance/training facility may find it more cost

effective to rely on mobile simulator assets to train combat tasks rather than transporting its troops to the training facility during drill weekends. A job aid for embedded training costing and effectiveness analyses is: "A Guide for Early Embedded Training Decisions," U.S. Army Research Institute for the Behavioral and Social Sciences Research Product 96-06.

6.2.3.3. Training Planning

This section will prepare the Program Manager to understand training capabilities as an integral part of the Joint Capabilities Integration and Development System and, with assistance of the training community, translate those capabilities into system design features.

First, the Joint Capabilities Integration and Development System process should address joint training parameters for military (Active, Reserve, and Guard) and civilian personnel who will operate, maintain, and support the system. Training programs should employ a cost-effective solution, consisting of a blend of capabilities that use existing training programs and introduces new performance-based training innovations. This may include requirements for school and unit training, as well as new equipment training, or sustainment training. This also may include requirements for instructor and key personnel training and new equipment training teams.

Training should be considered early in the capabilities development process beginning with the analyses that supports development of the Initial Capabilities Document and continues with development of the Capability Development Document.

The Capability Development Document should discuss the specific system training requirements:

- Allow for interactions between platforms or units (e.g., through advanced simulation and virtual exercises) and provide training realism to include threats (e.g., virtual and surrogate), a realistic electronic warfare environment, communications, and weapons.
- Embedded training capabilities that do not degrade system performance below threshold values nor degrade the maintainability or component life of the system.
- That Initial Operational Capability is attained and that training capabilities are embedded and met by Initial Operational Capability.
- An embedded performance measurement capability to support immediate feedback to the operators/maintainers and possibly to serve as a readiness measure for the unit commander.
- Training logistics necessary to support the training concept(e.g., requirements for new or upgrades to existing training facilities).

The training community should be specific in translating capabilities into system requirements. They should also set training resource constraints. Examples are:

- The training community should consider whether the system be designed with a mode of operation that allows operators to train interactively on a continuous basis, even when deployed in remote locations.
- The training community should consider whether the system be capable of exhibiting fault conditions for a specified set of failures to allow rehearsal of repair procedures for isolating faults or require that the system be capable of interconnecting with other (specific) embedded trainers in both static and employed conditions.
- The training community should consider whether embedded training capabilities allow enhancements to live maneuver such that a realistic spectrum of threats is encountered (e.g., synthetic radar warnings generated during flight).
- The training community should consider whether the integrated training system be fully tested, validated, verified, and ready for training at the training base as criteria for declaring Initial Operational Capability.

From the earliest stages of development and as the system matures, the program manager should emphasize training requirements that enhance the user's capabilities, improve readiness, and reduce individual and collective training costs over the life of the system. This may include requirements for expert systems, intelligent tutors, embedded diagnostics, virtual environments, and embedded training capabilities. Examples of training that enhances user's capabilities follow:

- Interactive electronic technical manuals provide a training forum that can significantly reduce schoolhouse training and may require lower skill levels for maintenance personnel while actually improving their capability to maintain an operational system;
- Requirements for an embedded just-in-time mission rehearsal capability supported by the latest intelligence information and an integrated global training system/network that allows team training and participation in large scale mission rehearsal exercises can be used to improve readiness.

In all cases, the paramount goal of the training/instructional system should be to develop and sustain a ready, well-trained individual/unit, while giving strong consideration to options that can reduce Life-cycle costs and provide positive contributions to the joint context of a system, where appropriate.

Training devices and simulators are systems that, in some cases, may qualify for their own set of HSI requirements. For instance, the training community may require the following attributes of a training simulator:

- Accommodate "the central 90 percent of the male and female population on critical body dimensions;"
- Not increase manpower requirements and should consider reductions in manpower requirements;
- Consider reduced skill sets to maintain because of embedded instrumentation;
- Be High Level Architecture compliant;

- Be Sharable Content Object Reference Model compliant;
- Be Test and Training Enabling Architecture compliant;
- Use reusable simulation objects.

6.2.4. Human Factors

6.2.4.1. . Human Factors Overview

Human factors are the end-user cognitive, physical, sensory, and team dynamic abilities required to perform system operational, maintenance, and support job tasks. Human factors engineers contribute to the Defense acquisition process by ensuring that the program manager provides for the effective utilization of personnel by designing systems that capitalize on and do not exceed the abilities (cognitive, physical, sensory, and team dynamic) of the user population. The human factors engineering community integrates the human characteristics of the user population into the system definition, design, development, and evaluation processes to optimize human-machine performance for both operation and maintenance of the system.

Human factors engineering is primarily concerned with designing human-machine interfaces consistent with the physical, cognitive, and sensory abilities of the user population. Human-machine interfaces include:

- Functional interfaces (functions and tasks, and allocation of functions to human performance or automation);
- Informational interfaces (information and characteristics of information that provide the human with the knowledge, understanding and awareness of what is happening in the tactical environment and in the system);
- Environmental interfaces (the natural and artificial environments, environmental controls, and facility design);
- Cooperational interfaces (provisions for team performance, cooperation, collaboration, and communication among team members and with other personnel);
- Organizational interfaces (job design, management structure, command authority, policies and regulations that impact behavior);
- Operational interfaces (aspects of a system that support successful operation of the system such as procedures, documentation, workloads, job aids);
- Cognitive interfaces (decision rules, decision support systems, provision for maintaining situation awareness, mental models of the tactical environment, provisions for knowledge generation, cognitive skills and attitudes, memory aids); and,
- Physical interfaces (hardware and software elements designed to enable and facilitate effective and safe human performance such as controls, displays, workstations, worksites, accesses, labels and markings, structures, steps and ladders, handholds, maintenance provisions, etc,).

6.2.4.2. Human Factors Parameters/Requirements

Human factors requirements, objectives, and thresholds should provide for the effective utilization of personnel through the accommodation of the cognitive, physical, and sensory characteristics that directly enhance or constrain system performance.

Cognitive requirements address the human's capability to evaluate and process information. Requirements are typically stated in terms of response times and are typically established to avoid excessive cognitive workload. Operations that entail a high number of complex tasks in a short time period can result in cognitive overload and safety hazards. The Capability Development Document should specify whether there are human-in-the-loop requirements. This could include requirements for "human in control," "manual override," or "completely autonomous operations."

Physical requirements are typically stated as anthropometric (measurements of the human body), strength, and weight factors. Physical requirements are often tied to human performance, safety, and occupational health concerns. To ensure the average user can operate, maintain, and support the system, requirements should be stated in terms of the user population. For instance, when the user requires a weapon that is "one-man portable," weight thresholds and objectives should be based on strength limitations of the user population and other related factors (e.g., the weight of other gear and equipment and the operational environment). For example, it may be appropriate to require that "the system be capable of being physically maintained by the 5th through 95th percentile soldiers wearing standard battle dress, or arctic and MOPP IV protective garments inside the cab," or that "the crew station physically accommodate a female/male population, defined by the 5th -95th anthropometric female/male soldier, for accomplishment of the full range of mission functions."

Sensory requirements are typically stated as visual, olfactory (smell), or hearing factors. The Capability Development Document should identify operational considerations that affect sensory processes. For example, systems may need to operate in noisy environments where weapons are being fired or on an overcast moonless night with no auxiliary illumination.

6.2.4.3. Human Systems Planning

Paragraph 6.3 contains an extensive discussion of human factors planning.

6.2.5. Safety and Occupational Health

6.2.5.1. Safety and Occupational Health Overview

Safety factors consist of those system design characteristics that serve to minimize the potential for mishaps causing death or injury to operators and maintainers or threaten the survival and/or operation of the system. Prevalent issues include factors that threaten the safe operation and/or survival of the platform; walking and working surfaces including work at heights; pressure extremes; and control of hazardous energy releases such as mechanical, electrical, fluids under pressure, ionizing or non-ionizing radiation (often referred to as "lock-out/tag-out"), fire, and explosions. Occupational health factors are those system design features that serve to minimize the risk of injury, acute or chronic

illness, or disability; and/or reduce job performance of personnel who operate, maintain, or support the system. Prevalent issues include noise, chemical safety, atmospheric hazards (including those associated with confined space entry and oxygen deficiency), vibration, ionizing and non-ionizing radiation, and human factors issues that can create chronic disease and discomfort such as repetitive motion diseases. Many occupational health problems, particularly noise and chemical management, overlap with environmental impacts. Human factors stresses that create risk of chronic disease and discomfort overlap with occupational health considerations.

6.2.5.2. Safety and Occupational Health Hazard Parameters/Requirements

Safety and health hazard parameters should address all activities inherent to the life cycle of the system, including test activity, operations, support, maintenance, and final demilitarization and disposal. Safety and health hazard requirements should be stated in measurable terms, whenever possible. For example, it may be appropriate to establish thresholds for the maximum level of acoustic noise, vibration, acceleration shock, blast, temperature or humidity, or impact forces etc., or "safeguards against uncontrolled variability beyond specified safe limits," where the Capability Development Document specifies the "safe limits." Safety and health hazard requirements often stem from human factor issues and are typically based on lessons learned from comparable or predecessor systems. For example, both physical dimensions and weight are critical safety requirements for the accommodation of pilots in ejection seat designs. Safety and health hazard thresholds are often justified in terms of human performance requirements, because, for example, extreme temperature and humidity can degrade job performance and lead to frequent or critical errors. Another methodology for specifying safety and health requirements is to specify the allowable level of residual risk as defined in MIL-STD-882D, for example, "There shall be no high or serious residual risks present in the system."

6.2.5.3. Safety and Occupational Health Planning

6.2.5.3.1. Programmatic Environment, Safety, and Occupational Health (ESOH) Evaluation (PESHE)

The HSI Strategy and the PESHE should jointly define how the program intends to avoid duplication of effort and to ensure the effective and efficient flow of information between the HSI and ESOH personnel working the integration of human safety and health considerations into the systems engineering process.

6.2.5.3.2. Health Hazard Analysis (HHA)

During early stages of the acquisition process, sufficient information may not always be available to develop a complete HHA. As additional information becomes available, the initial analyses are refined and updated to identify health hazards, assess the risks, and determine how to mitigate the risks, formally accept the residual risks, and monitor the effectiveness of the mitigation measures. The health hazard risk information is documented in the PESHE. Health hazard assessments should include cost avoidance

figures to support trade-off analysis. There are nine health hazard issues typically addressed in a health hazard analysis (HHA):

- Acoustical Energy. The potential energy that transmits through the air and interacts with the body to cause hearing loss or damage to internal organs.
- Biological Substances. The exposure to microorganisms, their toxins, and enzymes.
- Chemical Substances. The hazards from excessive airborne concentrations of toxic materials contracted through inhalation, ingestion, and skin or eye contract.
- Oxygen Deficiency. The displacement of atmospheric oxygen from enclosed spaces or at high altitudes.
- Radiation Energy. Ionizing: The radiation causing ionization when interfacing with living or inanimate mater. Non-ionizing: The emissions from the electromagnetic spectrum with insufficient energy to produce ionizing of molecules.
- Shock. The mechanical impulse or impact on an individual from the acceleration or deceleration of a medium.
- Temperature Extremes and Humidity. The human health effects associated with high or low temperatures, sometimes exacerbated by the use of a materiel system.
- Trauma. Physical: The impact to the eyes or body surface by a sharp or blunt object. Musculoskeletal: The effects to the system while lifting heavy objects.
- Vibration. The contact of a mechanically oscillating surface with the human body.

6.2.6. Personnel Survivability

6.2.6.1. Personnel Survivability Overview

Personnel survivability factors consist of those system design features that reduce the risk of fratricide, detection, and the probability of being attacked; and that enable the crew to withstand man-made hostile environments without aborting the mission or suffering acute chronic illness, disability, or death.

6.2.6.2. Survivability Parameters/Requirements

The Capability Development Document should include applicable crew survivability parameters. This may include requirements to eliminate significant risks of fratricide or detectability, or to be survivable in a nuclear, biological, and chemical (NBC) battlefield. NBC survivability, by definition, includes the instantaneous, cumulative, and residual effects of NBC weapons upon the system, including its personnel. It may be appropriate to require that the system "permit performance of mission-essential operations, communications, maintenance, re-supply and decontamination tasks by suitably clothed, trained, and acclimatized personnel for the survival periods and NBC environments required by the system."

The consideration of survivability should also include system requirements to ensure the integrity of the crew compartment and rapid egress when the system is damaged or destroyed. It may be appropriate to require that the system provide for adequate emergency systems for contingency management, escape, survival, and rescue.

6.2.6.3. Personnel Survivability Planning

The Joint Capabilities Integration and Development System capability documents define the program's combat performance and survivability needs. Consistent with those needs, the program manager should establish a Personnel Survivability program. This program overseen by the program manage, and seeks to minimize, the probability of encountering combat threats, the severity of potential wounds and injury incurred by personnel operating or maintaining the system, and the risk of potential fratricidal incidents. To maximize effectiveness, the program manager should assess Personnel Survivability in close coordination with systems engineering and test and evaluation activities.

Personnel survivability assessments assume the warfighter is integral to the system during combat. Damage to the equipment by enemy action, fratricide, or an improperly functioning component of the system can endanger the warfighter. The Personnel Survivability program should assess these events and their consequences. Once these initial determinations are made, the design of the equipment should be evaluated to determine if there are potential secondary effects on the personnel. Each management decision to accept a potential risk should be formally documented by the appropriate management level as defined in DoD Instruction 5000.2.

During early stages of the acquisition process, sufficient information may not always be available to develop a complete list of Personnel Survivability issues. An initial report is prepared listing those identified issues and any findings and conclusions. Classified data and findings are to be appropriately handled according to each DoD Component's guidelines. Personnel Survivability issues typically are divided into the following components:

- *Reduce Fratricide*. Fratricide is the unforeseen and unintentional death or injury of "friendly" personnel resulting from friendly forces employment of weapons and munitions. To avoid these types of survivability issues, personnel systems and weapon systems should include anti-fratricide systems, such as Identification of Friend or Foe (IFF) and Situational Awareness (SA) systems.
- *Reduce Detectability*. Reduce detectability considers a number of issues to minimize signatures and reduce the ranges of detection of friendly personnel and equipment by confounding visual, acoustic, electromagnetic, infrared/thermal, and radar signatures and methods that may be utilized by enemy equipment and personnel. Methods of reducing detectability could include camouflage, low-observable technology, smoke, countermeasures, signature distortion, training, and/or doctrine.
- *Reduce Probability of Attack*. Analysts should seek to reduce the probability of attack by avoiding appearing as a high value-target and by actively preventing or deterring attack by warning sensors and use of active countermeasures.

- *Minimize Damage if Attacked.* Analysts should seek to minimize damage if attacked by: 1) designing the system to protect the operators and crewmembers from enemy attacks; 2 improve tactics in the field so survivability is increased; 3) design the system to protect the crew from on-board hazards in the event of an attack (e.g., fuel, munitions, etc.); and 4) design the system to minimize the risk to supporting personnel if the system is attacked. Subject matter experts in areas such as nuclear, biological and chemical warfare, ballistics, electronic warfare, directed energy, laser hardening, medical treatment, physiology, human factors, and Information Operations can add additional issues.
- *Minimize Injury*. Analysts should seek to minimize: 1) combat, enemy weapon-caused injuries; 2) the combat-damaged system's potential sources and types of injury to both its crew and supported troops as it is used and maintained in the field; 3) the system's ability to prevent further injury to the fighter after being attacked; and 4) the system's ability to support treatment and evacuation of injured personnel. Combat-caused injuries or other possible injuries are addressed in this portion of personnel survivability, along with the different perspectives on potential mechanisms for reducing damage. Evacuation capability and personal equipment needs (e.g. uniform straps to pull a crew member through a small evacuation port are addressed here.
- *Minimize Physical and Mental Fatigue*. Analysts should seek to minimize injuries that can be directly traced to physical or mental fatigue. These types of injuries can be traced to complex or repetitive tasks, physically taxing operations, sleep deprivation, or high stress environments.
- *Survive Extreme Environments*. This component is to address issues that will arise once the warfighter evacuates or is forced from a combat-affected system such as an aircraft or watercraft and must immediately survive extreme conditions encountered in the sea or air until rescued or an improved situation on land is reached. Dependent upon requirements, this may also include some extreme environmental conditions found on land, but generally this component is for sea and air where the need is immediate for special consideration to maintain an individual's life. Survival issues for downed pilots behind enemy lines should be considered here.

The program manager should summarize plans for personnel survivability in the support strategy and address personnel survivability risks and plans for risk mitigation. If the system or program has been designated by Director, Operational Test & Evaluation (DOT&E), for live fire test and evaluation (LFT&E) oversight, the program manager should integrate T&E to address crew survivability issues into the LFT&E program to support the Secretary of Defense LFT&E Report to Congress (10 U.S.C. 2366). The program manager should address special equipment or gear needed to sustain crew operations in the operational environment.

6.2.7. Habitability

6.2.7.1. Habitability Overview

Habitability factors are those living and working conditions that are necessary to sustain the morale, safety, health, and comfort of the user population. They directly contribute to personnel effectiveness and mission accomplishment, and often preclude recruitment and retention problems. Examples include: lighting, space, ventilation, and sanitation; noise and temperature control (i.e., heating and air conditioning); religious, medical, and food services availability; and berthing, bathing, and personal hygiene

Habitability consists of those characteristics of systems, facilities (temporary and permanent), and services necessary to satisfy personnel needs. Habitability factors are those living and working conditions that result in levels of personnel morale, safety, health, and comfort adequate to sustain maximum personnel effectiveness, support mission performance, and avoid personnel retention problems.

6.2.7.2. Habitability Parameters/Requirements

Habitability is one of several important factors included in the overall consideration of unit mission readiness. Per DoD Instruction 5000.2, the program manager shall work with habitability representatives to establish requirements for the physical environment (e.g., adequate light, space, ventilation, and sanitation, and temperature and noise control) and, if appropriate, requirements for personal services (e.g., religious, medical, and mess) and living conditions (e.g., berthing and personal hygiene) if the habitability factors have a direct impact on meeting or sustaining performance requirements, sustaining mission effectiveness, or that have such an adverse impact on quality of life or morale that recruitment or retention rates could be degraded. Examples include requirements for heating and air-conditioning, noise filters, lavatories, showers, dry-cleaning and laundry.

While a system, facility, and/or service should not be designed solely around optimum habitability factors, habitability factors cannot be systematically traded-off in support of other readiness elements without eventually degrading mission performance.

6.2.7.3. Habitability Planning

The program manager should address habitability planning in the support strategy and identify habitability issues that could impact personnel morale, safety health, or comfort or degrade personnel performance, unit readiness, or result in recruitment or retention problems.

6.3. Human Factors Engineering (HFE)

6.3.1. Mandatory Guidance

As required by DoD Instruction 5000.2, the program manager shall employ human factors engineering to design systems that require minimal manpower; provide effective training; can be operated and maintained by users; and are suitable (habitable and safe with minimal environmental and occupational health hazards) and survivable (for both the crew and equipment).

6.3.2. Application of HFE

HFE plays an important role in each phase of the acquisition cycle, to include system definition, design, development, evaluation, and system reliability and maintainability in the field. To realize the potential of HFE contributions, HFE must be incorporated into the design process at the earliest stages of the acquisition process (i.e., during the Concept Refinement and Technology Development phases). The right decisions about the human-machine interfaces early in the design process will optimize human performance. HFE participation continues to each succeeding acquisition phase. The HFE practitioners provide expertise that includes design criteria, analysis and modeling tools, and measurement methods that will help the program office design systems that are operationally efficient and cost-effective. In any system acquisition process, it is important to recognize the differences between the competencies (skills and knowledge) required for the various warfighters. Application of HFE processes will lead to an understanding of the competencies needed for the job, and help identify if requirements for knowledge, skills, and abilities (KSAs) exceed what the user can provide and whether the deficiency will lead to a training or operational problem. HFE tools and techniques can be used to identify the KSAs of the target audience and account for different classes and levels of users and the need for various types of information products. While it is critical to understand the information processing and net-centric requirements of the system, it is equally important to understand the factors affecting format and display of the data presented to the user to avoid cognitive overload.

6.3.3. General Guidelines

HFE should be applied during development and acquisition of military systems, equipment, and facilities to integrate personnel effectively into the design of the system. An HFE effort should be provided to: (a) develop or improve all human interfaces of the system; (b) achieve required effectiveness of human performance during system operation, maintenance, support, control, and transport; and (c) make economical demands upon personnel resources, skills, training, and costs. The HFE effort should include, but not necessarily be limited to, active participation in the following three major interrelated areas of system development.

6.3.3.1. Analysis

Starting with a mission analysis developed from a baseline scenario, the functions that must be performed by the system in achieving its mission objectives should be identified and described. These functions should be analyzed to determine their best allocation to personnel, equipment, software, or combinations thereof. Allocated functions should be further dissected to define the specific tasks that must be performed to accomplish the functions. Each task should be analyzed to determine the human performance parameters; the system, equipment, and software capabilities; and the tactical/environmental conditions under which the tasks will be conducted. Task parameters should be quantified where possible, and should be expressed in a form that permits effectiveness studies of the human-system interfaces in relation to the total system operation. HFE high-risk areas should be identified as part of the analysis. Task analysis must include maintenance and sustainment functions performed by crew and support facilities. Analyses should be updated as required to remain current with the design effort.

6.3.3.2. Design and Development

HFE should be applied to the design and development of the system equipment, software, procedures, work environments, and facilities associated with the system functions requiring personnel interaction. This HFE effort should convert the mission, system, and task analysis data into a detailed design and development plans to create a human-system interface that will operate within human performance capabilities, meet system functional requirements, and accomplish mission objectives.

6.3.3.3. . Test and Evaluation (T&E)

HFE should be incorporated into the system T&E program and integrated into engineering design and development tests, contractor demonstrations, flight tests, acceptance tests, other development tests and operational testing. Compliance with HFE requirements should be tested as early as possible. T&E should include evaluation of maintenance and sustainment activities and evaluation of the dimensions and configuration of the environment relative to criteria for HFE. HFE findings from design reviews, modeling, simulations, demonstrations, and other early engineering tests should be used in planning and conducting later tests. Test planning should be directed toward verifying that the system can be operated, maintained, supported, and controlled by user personnel in its intended operational environment with the intended training. HFE test planning should also consider data needed or provided by operational T&E. (See 9.4.5 and 9.8.1.11.)

6.3.3.4. Support Strategy and Acquisition Strategy

The program manager should summarize the steps planned to be taken (e.g., contract deliverables) to ensure human factors engineering/cognitive engineering is employed during systems engineering over the life of the program to provide for effective human-machine interfaces and meet HSI requirements.

6.4. HSI Integration

The key to a successful HSI strategy is integration. To optimize total system performance and determine the most effective, efficient, and affordable design entails trade studies both within the HSI elements (manpower, personnel, training, safety and occupational health, human factors, survivability, and habitability) and between the HSI elements and the system platform (hardware and software). The program manager should integrate the system requirements for the eight HSI elements with each other, and also with the system platform. The results of these integration efforts should be reflected in updates to the requirements, objectives, and thresholds in the Capability Development Document.

In today's Joint environment, the integration across systems of systems is necessary to achieve a fully networked Joint war fighting capability. The Warfighter requires a fully networked environment and must be able to operate efficiently and effectively across the continuum of systems from initial recognition of the opportunity to engage through to mission completion. To accomplish this, HSI should be considered through system of system analysis, modeling and testing to identify opportunities for integration, synchronization, collaboration, and coordination of capabilities to meet requirements.

This may require a fully integrated investment strategy with joint sponsorship from initial concept through a series of spiral or incremental developments.

Values for objectives and thresholds, and definitions for parameters contained in the capabilities documents, Manpower Estimate, TEMP, and APB, should be consistent. This ensures consistency and thorough integration of program interests throughout the acquisition process.

6.4.1. Integrated Product and Process Development and Integrated Product Teams

DoD acquisition policy stresses the importance of integrated product and process development (IPPD). IPPD is a management technique that integrates all acquisition activities starting with capabilities definition through systems engineering, production, fielding/deployment and operational support in order to optimize the design, manufacturing, business, and supportability processes. At the core of the IPPD are Integrated Product Teams (IPTs). HSI should be a key consideration during the formation of IPTs. (See related discussions of IPPD and IPTs) For instance, human factors engineers should be included as members of systems engineering and design teams and other IPTs that deal with human-oriented acquisition issues or topics. The training community should be included in IPTs to ensure that the operators, maintainers and support personnel are properly trained and can maintain their operational effectiveness (i.e., maintain proficiency in tasks critical to mission success) and to ensure that system users and organization/unit leaders are prepared to employ the system advantageously. The HSI community assists with IPPD as part of the Integrated Product Teams (IPTs) by ensuring that:

- HSI parameters/requirements in the Initial Capabilities Document, Capability Development Document, and Capability Production Document are based upon and consistent with the user representative's strategic goals and strategies and are addressed throughout the acquisition process starting with technology development and continuing throughout engineering design, trade-off analysis, testing, fielding/deployment, and operational support;
- Safety and efficiency issues, identified in legacy systems and by review of design capability risks, are used to establish a preliminary hazard list (PHL) for risk management and that the issues are effectively evaluated and managed throughout the systems Life-cycle at a management level consistent with the hazard;
- The factors, tools, methodologies, risk assessment/mitigations, and set of assumptions used by the acquisition community to assess manpower, personnel, and training (MPT) requirements, measure human-in-the-loop system performance, and evaluate safety, occupational health hazards, survivability, and habitability are consistent with what the functional communities/user representatives use to evaluate performance and establish performance based metrics;
- The factors used by the acquisition community to develop cost estimates are consistent with the 1) manpower and personnel requirements reported in the Manpower Estimate; 2) training requirements reported in the DoD Component

training plans; and 3) assessments of safety and health hazards documented in the PESHE; and,

- The Manpower Estimates and training strategies reported during the acquisition milestone reviews are reflected in the manning documents, training plans, personnel rosters, and budget submissions when the systems are fielded.

6.4.2. HSI Strategy, Risk, and Risk Mitigation

An HSI strategy should be initiated early in the acquisition process, when the need for a new capability or improvements to an existing capability is first established. To satisfy DoD Instruction 5000.2, the program manager should have a plan for HSI in place prior to entering System Development and Demonstration. The program manager should describe the technical and management approach for meeting HSI parameters in the capabilities documents, and identify and provide ways to manage any HSI-related cost, schedule, or performance issues that could adversely affect program execution.

When a defense system has complex human-systems interfaces; significant manpower or training costs; personnel concerns; or safety, health hazard, habitability, or survivability issues; the program manager should use the HSI plan to identify solutions. HSI risks and risk mitigation should be addressed in the acquisition strategy and the program manager's risk management program.

The HSI plan should address potential readiness or performance risks. For example, skill degradation can impact combat capability and readiness. The HSI plan should call for studies to identify operations that pose the highest risk of skill decay. When analysis indicates that the combat capability of the system is tied to the operator's ability to perform discrete tasks that are easily degraded (such as those contained in a set of procedures), solutions such as embedded training should be considered to address the problem. Information overload and requirements for the warfighter to dynamically integrate data from multiple sources can result in degradation of situational awareness and overall readiness. Careful consideration of common user interfaces, composable information sources, and system workload management will mitigate this risk. An on-board "performance measurements capability" can also be developed to support immediate feedback to the operators/maintainers and possibly serve as a readiness measure to the unit commander. The lack of available ranges and other training facilities, when deployed, are issues that should be addressed. The increased use of mission rehearsal, as part of mission planning, and the preparation process and alternatives supporting mission rehearsal should be addressed in the HSI plan. Team skills training and joint battle space integration training should also be considered in the HSI plan and tied to readiness.

The program manager's Programmatic Environment, Safety, and Occupational Health (ESOH) Evaluation (PESHE) describes the strategy for integrating ESOH considerations into the systems engineering process and defines how PESHE is linked to the effort to integrate HSI considerations into systems engineering. The PESHE also describes how ESOH risks are managed and how ESOH and HSI efforts are integrated. It summarizes ESOH risk information (hazard identification, risk assessment, mitigation decisions, residual risk acceptance, and evaluation of mitigation effectiveness). The HSI Strategy

should address the linkage between HSI and ESOH and how the program has been structured to avoid duplication of effort.

DoD Directive 5000.1 prescribes supportability comparable to cost, performance, and schedule in program decision-making. Program managers should establish a logistics support concept (e.g., two level, three level), training plans, and manpower and personnel concepts, that when taken together, provide for cost-effective, total, Life-cycle support. MIL-HDBK-29612-1A, -2A, -3A, & -4A may be used as a guide for Instructional Systems Development/Systems Approach to Training (ISD/SAT) and education process for the development of instructional materials. Manpower, personnel, training analyses should be tied to supportability analyses and should be addressed in the HSI plan.

Program risks related to cost, schedule, performance, supportability, and/or technology can negatively impact program affordability and supportability. The program manager should prepare a "fall-back" position to mitigate any such negative effect on HSI objectives. For example, if the proposed system design relies heavily on new technology or software to reduce operational or support manning requirements, the program manager should be prepared with design alternatives to mitigate the impact of technology or software that is not available when expected.

6.4.3. HSI in the Capabilities Documents

The Initial Capabilities Document may seek to establish a new capability, improve an existing capability, or exploit an opportunity to reduce costs or enhance performance. The Initial Capabilities Document should describe the key boundary conditions and operational environments that impact how the system is employed to satisfy the mission need. Key boundary conditions include critical manpower, personnel, training, safety, occupational health, human factors, habitability, and personnel survivability factors that have a major impact on system performance and Lifecycle costs. The DOTMLPF considerations and implications section of the Initial Capabilities Document should discuss all relevant domains of HSI. HSI capabilities in the Capability Development Document should be specified in measurable, testable, performance-based language that is specific to the system and mission performance. A discussion of the analyses and/or results conducted to determine the HSI capabilities is not appropriate for the Initial Capabilities Document or Capability Development Document. This information should be contained in other programmatic documentation (e.g., HSI plan, Training Systems plan, or Manpower Estimate).

6.4.4. Refining Required Capabilities

As plans for the system mature, the capabilities documents should become more specific and reflect the integration of program objectives. The program manager should work with HSI analysts and user representatives to translate HSI thresholds and objectives in the capabilities documents into quantifiable and measurable system requirements. The program manager should refine and integrate operational and design requirements so they result in the proper balance between performance and cost, and keep programs affordable. Additionally, system requirements should serve as the basis for developing engineering specifications, and should be reflected in the statement of work (SOW), contracts, Test and Evaluation Master Plan (TEMP), and other program documentation.

Over the course of the acquisition process, as trade-offs are made and plans for the system design mature, the capabilities documents should be updated to reflect a more refined and integrated set of parameters.

6.4.5. HSI throughout the System Life Cycle

6.4.5.1. Research and Development (R&D), Studies, and Analyses in Support of HSI

Continuous application of human-centered research data, methods, and tools will ensure maximum operational and training effectiveness of the system. Continual analysis of system functionality provides data to help determine the best allocation of tasks to personnel, hardware, or software. Results guide human workload predictions, man-machine interface requirements, and procedural, software, and hardware innovations needed to ensure that the human element can fulfill and enhance total system performance. Each military department conducts HFE research. The products of this research form the basis for creating and maintaining HFE military standards, design criteria, methodologies, tools, and data bases used when applying HFE to defense systems acquisition. Within each military department, HFE practitioners support ongoing concepts and studies that identify potential HFE impacts on operational effectiveness and resource needs of alternative solutions. Examples of these activities include field assessments, human performance modeling, simulations, and technology demonstrations.

6.4.5.2. Technology Development and System Development and Demonstration

The purpose of the TD and SDD phases is to develop a system or an increment of capability; reduce integration and manufacturing risk (technology risk reduction occurs during Technology Development); ensure operational supportability with particular attention to reducing the logistic footprint; implement HSI; design for produceability; ensure affordability and protection of critical program information (CPI) by implementing appropriate techniques such as anti-tamper; and demonstrate system integration, interoperability, safety and utility.

6.4.5.2.1. Systems Engineering

Once parameters are established in the Initial Capabilities Document and Capability Development Document, it is the program manager's responsibility to ensure that they are addressed during the systems engineering process and properly considered during cost/performance trade-off analyses. Consistent with section E1.29 of DoD Directive 5000.1, the program manager shall apply HSI to optimize total system performance operational effectiveness, suitability, survivability, safety, and affordability. Program manager s shall consider supportability, life cycle costs, performance, and schedule comparable in making program decisions. As required by DoD Instruction 5000.2, the program manager shall take steps (e.g., contract deliverables and Government/contractor IPT teams) to ensure human factors engineering/cognitive engineering is employed during systems engineering from the initial concept phase through the life of the program to provide for effective human-machine interfaces, meet HSI requirements, and (as

appropriate) support a system-of-system acquisition approach. The program manager shall also ensure that HSI requirements are included in performance specifications and test criteria. MPT functional representatives, as user representatives, participate in the systems engineering process to help produce the proper balance between system performance and cost and to ensure that requirements remain at affordable levels. Manpower, personnel, training, and supportability analyses should be conducted as an integral part of the systems engineering process beginning with concept refinement and continuing throughout program development.

6.4.5.2.1.1. System Design

Human factors engineers play a major role in the design process. Front-end analysis methods, such as those described in MIL-HDBK-46855A, should be pursued to maximize the effectiveness of the new system. Initial emphasis should be placed on "lessons learned" from predecessor or comparable systems to help identify and eliminate characteristics in the new system that require excessive cognitive, physical, or sensory skills or high aptitudes; involve complex fault location or workload intensive tasks; necessitate excessive training; require proficiency training; or result in frequent or critical errors or safety/health hazards. Placing an emphasis on the "human-in-the-loop" ensures that systems are designed to operate consistent with human performance capabilities and limitations, meet system functional requirements, and fulfill mission goals with the least possible demands on manpower, personnel, and training. Moreover, human factors engineers minimize added costs that result when systems have to be modified after they are fielded in order to correct performance and safety issues.

6.4.5.2.1.2. Logical Analysis and Allocations

During systems engineering, logical analysis should be performed iteratively to define successively lower functional and performance requirements, to identify functional interfaces, and to allocate functions to components of the system (e.g., hardware, software, and human). Tasks should be allocated to the human component consistent with human attributes (i.e., capabilities and limitations) of the user population as established in the Target Audience Description (TAD). Requirements analysis should be conducted iteratively in conjunction with logical analysis to develop and refine system level performance requirements, identify external interfaces, and provide traceability among user requirements and design requirements. Human-machine interfaces should be identified as an outgrowth of the functional allocation process. Another product of the systems engineering process is a list of job tasks with performance/confidence levels. This information is used to further refine manpower, personnel and training requirements.

6.4.5.2.2. Specifications and Standards

It is primarily the responsibility of the program manager, with the assistance of the IPTs, to establish performance specifications, design criteria standards, interface standards, and data specifications in the solicitation and resulting contract. Strong consideration should be given to establishing standards when uniform configuration is necessary for ease of operation, safety, or training purposes. For instance, a control panel or avionics suite may need to be standardized to enhance the ability of the user to access information and to

respond quickly in an emergency situation. Standard features preclude the need to teach multiple (or conflicting) responses to similar tasks. Standardization is particularly important when a standard performance is required for safety reasons. For instance, rapid ejection from the cockpit should require standard procedures and tasks. If there are unique health hazard or survivability requirements, such as vibration or shock tolerances, extended temperature range, or noise levels, standardization may be the most efficient way to ensure that the system meets those special requirements. Preference should be given to specifications and standards developed under the Defense Standardization Program. Regulatory occupational exposure standards create performance thresholds. However, use of guidance exposure criteria and ergonomic/HSI guidelines should be considered to ensure personnel protection, promote efficiency, and anticipate more stringent standards that are likely to be required during the Lifecycle of the system.

Performance standards for operators, maintainers, both individual and team, are derived from the performance requirements of the total system. For example, human performance requirements (e.g., completion times or success rates) presumes that in order for the total system to achieve specified performance levels, the human will have to complete tasks or achieve performance objectives within specified confidence levels (usually expressed in terms of per cent of actions completed within a specified time-frame and/or error limit). The training/instructional system should be developed to ensure that operators can meet or exceed the personnel performance levels required to operate/maintain the systems. Additionally, manpower should be determined based on these same performance requirements. Operational tests should also be based on the same criteria.

6.4.5.2.3. Solicitations and Source Selection

HSI considerations must be clearly defined and given proper weight in solicitations and proposal evaluation guidelines provided to the government evaluation team. The record of contractors in safety and implementation of human engineering can be an element of bid selection and contract performance criteria.

6.4.5.3. Production and Deployment

The objective of this phase of the acquisition process is to achieve an operational capability that satisfies mission needs. Operational test and evaluation shall determine the effectiveness and suitability of the system.

6.4.5.4. Operations and Support (O&S)

The objective of this phase is the execution of a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its Lifecycle. As required by DoD Directive 5000.1, planning for O&S shall begin as early as possible in the acquisition process. Efforts during the O&S phase should be directed towards ensuring that the program meets and has the resources to sustain the threshold values of all support performance requirements. Once the system is fielded or deployed, a follow-on operational testing program, to assess performance, quality, compatibility, and interoperability, and identify deficiencies, should be conducted, as appropriate. Post fielding verification of the manpower, and information resulting from training exercises, readiness reports, and audits can also be used to assess the operational

capability of the system. During fielding, deployment, and throughout operational support, the need for modifications to the system should be assessed.

6.5. Affordability

Consistent with DoD Directive 5000.1, all participants in the acquisition system shall recognize the reality of fiscal constraints. The user shall address affordability when establishing capability needs and at each milestone decision point. As required by DoD Instruction 5000.2, the affordability of the system is determined during the requirements process and is included in each Capability Development Document using Life-cycle cost or, if available, total ownership cost. Transition into the System Development and Demonstration phase requires full funding (i.e., inclusion of the dollars and manpower needed for all current and future efforts to carry out the acquisition strategy in the budget and out-year program) which shall be programmed when a system concept and design have been selected. In the case of a replacement system, when the Milestone B is projected to occur in the first two years of the Future Years Defense Program under review, the program shall be fully funded in that Planning, Programming, and Budget Execution process cycle. In no case shall full funding be provided later than Milestone B, unless a program first enters the acquisition process at Milestone C.

6.5.1. Lifecycle Cost Objectives

As required by DoD Directive 5000.1, the estimation of ownership costs shall begin as early as possible in the acquisition process. Life-cycle cost objectives are usually established prior to program initiation. These objectives embody the planned affordability for the program. At each subsequent milestone review, the Milestone Decision Authority assesses Life-cycle cost objectives and progress towards achieving them.

The O&S portion of the Life-cycle costs should be consistent with manpower, personnel, and training constraints established in the Capability Development Document.

6.5.2. Manpower Estimates

Manpower Estimates shall address manpower affordability in terms of military end strength (including force structure and student end strength) and civilian work years beginning at Milestone B. Consistent with DoD Directive 5000.1, DoD Components shall plan programs based on realistic projections of the dollars and manpower likely to be available in future years. When major manpower increases are required to support the program, or major manpower shortfalls exist, they shall be identified as risks in the Manpower Estimate, and addressed in the risk assessment section of the Acquisition Strategy. Program risks that result from manpower shortfalls should be addressed in terms of their impact on readiness, operational availability, or reduced combat capability.

6.5.3. Cost as an Independent Variable

DoD Directive 5000.1 requires the program manager to view cost as an independent variable. During trade-off analysis, program managers should consider whether it is more cost effective for the Department to spend additional money during the engineering and design process to achieve a system with reduced support costs than it is to design a more

resource intensive system at reduced acquisition costs. Such comparisons should consider all aspects of Lifecycle costs, including mishaps resulting in lost work time.

6.6. Additional References

6.6.1. DoD Publications

The following DoD Directives and Instructions provide manpower, personnel, and training policy and direction:

- DoD Directive 1100.4, "Guidance for Manpower Programs"
- DoD Directive 1100.9, "Military-Civilian Staffing of Management Positions in Support Activities"
- DoD Directive 1100.18, "Wartime Manpower Mobilization Planning"
- DoD Directive 1322.18, "Military Training"
- DoD Directive 1430.13, "Training Simulators and Devices"
- DoD Instruction 1322.20, "Development and Management of Interactive Courseware for Military Training"
- Training Transformation Implementation Plan June 2004

6.6.2. Discretionary Practices

The following military standards (MIL-STD), DoD Handbooks (DOD-HDBK), and Military handbooks (MIL-HDBK) may be used to support HSI analysis:

- MIL-STD-882D, *Standard Practice for System Safety*
- MIL-STD-1472, *DoD Design Criteria Standard: Human Engineering*
- MIL-STD-1474, *Noise Limits for Military Materiel*
- MIL-STD-1477, *Symbols for Army Air Defense System Displays*
- MIL-STD-1787, *Aircraft Display Symbology*
- MIL-STD-1801, *Human Engineering Requirements for User/Computer Interface*
- DOD-HDBK-743, *Anthropometry of U. S. Military Personnel*
- DOD-HDBK-761, *Human Engineering Guidelines for Management Information Systems*
- MIL-HDBK-759, *Human Engineering Design Guidelines*
- MIL-HDBK-29612-1A, *Guidance for Acquisition of Training Data Products and Services*
- MIL-HDBK-29612-2A, *Instructional Systems Development/Systems Approach to Training and Education*
- MIL-HDBK-29612-3A, *Development of Interactive Multimedia Instruction*

- MIL-HDBK-29612-4A, *Glossary of Training Terms*
- MIL-HDBK-29612-5, *Advanced Distributed Learning (ADL) Products and Systems*
- MIL-HDBK-1473, *Color and Marking of Army Materie*l
- MIL-HDBK-1908, *Definitions of Human Factors Terms*
- MIL-HDBK-46855A, *Human Engineering Program Process and Procedures*
- MILPRF 29612, *Performance Specification, Training Data Products "A Guide for Early Embedded Training Decisions," U.S. Army Research Institute for the Behavioral and Social Sciences Research Product 96-06.*

Chapter 7

Acquiring Information Technology and National Security Systems

7.0 Chapter Overview

7.0.1. Purpose

The goal of this chapter is to help program managers and Sponsors/Domain Owners implement DoD policies intended to achieve"fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battle space." This chapter explains how the Department of Defense is using a network-centric strategy to transform DoD warfighting, business, and intelligence capabilities. The chapter provides descriptions and explanations of many of the associated topics and concepts. This chapter also discusses many of the activities that enable the development of net-centric systems. However, not all activities are the direct responsibility of the Program Manager. Many activities reflect Department-level effort that occurs prior to or outside of the acquisition process. The detailed discussions of such a broad set of activities are presented here to help the Program Manager understand the context of the capabilities described in the Joint Capabilities Integration and Development System documents and required of the system under development.

7.0.2. Contents

This chapter contains 10 sections that present the Program Manager with a comprehensive review of topics, concepts, and activities associated with the acquisition of Information Technology and National Security Systems.

Section 7.1, “Introduction,” explains net-centricity in the context of the discussions and requirements outlined in the various other sections of this chapter.

Section 7.2, “Global Information Grid (GIG),” explains several important concepts that provide a foundation for acquiring net-centric Information Technology and National Security Systems. The overarching concept is that of the GIG as the integrated enterprise information technology architecture used to describe and document current and desired relationships among warfighting operations, business and management processes, and information technology. The integrated architecture products and artifacts:

Describe existing and desired capabilities;

Provide a basis for interoperability and supportability reviews and certifications;

Provide a component of the Net-Ready Key Performance Parameter;

Provide required components of the Capability Development Document and Capability Production Document;

Develop and describe Key Interface Profiles; and

Document consistency with the GIG architecture and policies.Section 7.2 continues with an explanation of compliance with the GIG architecture, and outlines eight requirements for compliance. It discusses a tool called the Net-Centric Operations

and Warfare Reference Model (NCOW RM). (The NCOW RM helps program managers and Sponsors/Domain Owners describe their transition from the current environment to the future net-centric environment. This will be a key tool during program oversight reviews.) The section defines what compliance with the NCOW RM means, and provides a method of assessing compliance with the model.

Finally, section 7.2 also introduces the DoD Net-Centric Data Strategy, the DoD Information Assurance Strategic Plan, and the GIG Enterprise Services Strategy, and relates each of these strategies to the NCOW RM.

The remaining sections elaborate on specific areas on which the Sponsors/Domain Owners and Program Managers should focus as they work to deliver and improve the reach, richness, agility, and assurance of net-centric capabilities:

Section 7.3, "Interoperability and Supportability of Information Technology and National Security Systems," explains interoperability and supportability, outlines the use of the Net-Ready Key Performance Parameter in these processes, and describes the process of building an Information Support Plan.

Section 7.4, "Net-Centric Data Strategy," provides guidance on implementing the Net-Centric Data Strategy and outlines important data tasks as they relate to the acquisition process.

Section 7.5, "Information Assurance," explains the requirements for Information Assurance and provides links to resources to assist in developing an Information Assurance strategy.

Section 7.6, "Electromagnetic Spectrum," offers help understanding the process of Spectrum Supportability.

Section 7.7, "Business Modernization Management Program," provides important information for the Department's business domains about the Business Modernization Management Program. The Business Modernization Management Program is developing an essential subset of the GIG architecture called the Business Enterprise Architecture. Section 7.7 also provides links to related websites and resources.

Section 7.8, "Clinger-Cohen Act," helps program managers and Sponsors/Domain Owners understand how to implement the Clinger-Cohen Act and associated statutory and regulatory requirements.

Section 7.9, "Post Deployment Reviews," discusses how the Department of Defense uses the Post Implementation Review to support Clinger-Cohen Act compliance. And finally,

Section 7.10, "Commercial, Off-The-Shelf (COTS) Solutions," provides insight into Department guidance regarding acquisition of commercial-off-the-shelf (COTS) software products.

In summary, this chapter should help Program Managers and Sponsors/Domain Owners understand and apply the tools of the GIG architecture so that they can more effectively:

Describe and measure the degree to which their programs are interoperable and supportable with the GIG;

Ensure their programs employ and institutionalize approaches that make data visible, accessible, understandable, trusted, interoperable and responsive;

Achieve the Department's objectives for Information Assurance;

Ensure their programs will have assured, interoperable access to electromagnetic spectrum; and

Achieve these goals within the constraints of the law and where possible, through the use of commercially available solutions.

7.1 Introduction

The DoD Transformation Planning Guidance defines the desired outcome of transformation as "fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battle space." The goal of this chapter is to help Program Managers and Sponsors/Domain Owners implement the DoD policies that are intended to achieve this outcome. This introduction briefly explains net-centricity in context of the requirements outlined in the various other sections of this chapter.

Net-centricity is "the realization of a robust, globally networked environment (interconnecting infrastructure, systems, processes, and people) within which data is shared seamlessly and in a timely manner among users, applications, and platforms. By securely interconnecting people and systems, independent of time or location, net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Users are empowered to better protect assets; more effectively exploit information; more efficiently use resources; and unify our forces by supporting extended, collaborative communities to focus on the mission."

The Department's approach for transforming to net-centric operations and warfare aims to achieve four key attributes: reach, richness, agility, and assurance. This approach uses the Global Information Grid as "the organizing and transforming construct for managing information technology throughout the Department." It envisions moving to trusted network-centric operations through the acquisition of systems and families-of-systems that are secure, reliable, interoperable, and able to communicate across a universal Information Technology infrastructure, to include National Security Systems. This Information Technology infrastructure includes data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities.

The rest of this chapter describes the concepts, topics, and activities to achieve this transformation.

7.2 Global Information Grid (GIG)

7.2.1 Introduction

The Global Information Grid (GIG) is the organizing and transforming construct for managing information technology (IT) throughout the Department. GIG policy, governance procedures, and supporting architectures are the basis for developing and

evolving IT capabilities, IT capital planning and funding strategies, and management of legacy (existing) IT services and systems in the DoD. In discussing the GIG and how a particular program interacts with, supports, or relies upon the GIG, it is useful to think of the GIG from three perspectives-its vision, its implementation, and its architecture.

7.2.1.1 The Global Information Grid (GIG) Vision

The GIG vision is to empower users through easy access to information anytime and anyplace, under any conditions, with attendant security. Program managers and Sponsors/Domain Owners should use this vision to help guide their acquisition programs. This vision requires a comprehensive information capability that is global, robust, survivable, maintainable, interoperable, secure, reliable, and user-driven. The goal is to increase the net-centricity of warfighter, business, intelligence, DoD enterprise management, and enterprise information environment management operations by enabling increased reach among the GIG users, increased richness in the information and expertise that can be applied to supporting operational decisions, increased agility in rapidly adapting information and information technology to meet changing operational needs, and increased assurance that the right information and resources to do the task will be there when and where it is required.

7.2.1.2. The Implementation Component of the Global Information Grid (GIG)

The implementation component of the GIG is the existing, globally interconnected, end-to-end set of capabilities, processes, and personnel for collecting, processing, storing, disseminating, and managing information. The GIG includes all Information Technology (IT) and National Security Systems (NSS) throughout the DoD, and their interfaces to allied and coalition forces, industry, and other Federal agencies. All DoD information systems that currently exist or that have been approved for implementation comprise the GIG. Every DoD acquisition program having an IT component is a participant in the GIG. Each new IT-related acquisition program replaces, evolves, or adds new capabilities to the GIG. Components, Combat Developers, Sponsors, Domain Owners, DoD Agencies, and program managers should consider the existing and planned capabilities of the GIG that might be relevant as they develop their integrated architectures, Joint Capabilities Integration and Development System documentation (see CJCSI 3170.1), and related program requirements.

7.2.1.3. The DoD Enterprise Architecture

The DoD Chief Information Officer (CIO) plays the central role in the description, development, acquisition, and management of the Department's Information Technology (IT) capabilities. As the Secretary of Defense's principal staff assistant for IT and information resources management, the CIO develops, maintains, and uses the Department's enterprise IT architecture--the Global Information Grid (GIG) Architecture and the Net-Centric Operations and Warfare (NCOW) Reference Model to guide and oversee the evolution of the Department's IT-related investments to meet operational needs.

The GIG Architecture is the Department's *IT architecture*. It describes the implementation component of the GIG, with integrated operational, systems, and technical views. The GIG Architecture fulfills, in part, the requirement to develop a Department-wide enterprise architecture. As defined by the Office of Management and Budget, *enterprise architecture* is the explicit description and documentation of the current and desired relationships among business and management processes and IT. The Enterprise Architecture describes the "current architecture" and "target architecture," and provides a strategy that will enable an agency to transition from its current state to its target environment. All DoD architectures, including warfighter, intelligence, business process, and enterprise management architectures, are part of the GIG Architecture. Versions 1 and 2 of the GIG Architecture are the current and target DoD IT architectures, respectively and describe the enterprise view of the GIG.

The NCOW Reference Model provides the means and mechanisms for the Department and its combat developers, sponsors, domain owners, and program managers to describe their transition from the current environment (described in GIG Architecture Version 1) to the future environment (described in GIG Architecture Version 2).

7.2.1.4. Net-Centric Operations and Warfare Reference Model (NCOW RM)

The NCOW RM (see the DoD Global Information Grid Architectures website) represents the strategies for transforming the enterprise information environment of the Department. It is an architecture-based description of activities, services, technologies, and concepts that enable a net-centric enterprise information environment for warfighting, business, and management operations throughout the Department of Defense. Included in this description are the activities and services required to establish, use, operate, and manage this net-centric enterprise information environment. Major activity blocks include the generic user-interface (A1), the intelligent-assistant capabilities (A2), the net-centric service (core, Community of Interest, and enterprise control) capabilities (A3), the dynamically allocated communications, computing, and storage media resources (A4), and the enterprise information environment management components (A5). Also included is a description of a selected set of key standards and/or emerging technologies that will be needed as the NCOW capabilities of the Global Information Grid (GIG) are realized.

Transforming to a net-centric environment requires achieving four key attributes: reach, richness, agility, and assurance. The initial elements for achieving these attributes include the Net-Centric Enterprise Services Strategy, the DoD Net-Centric Data Strategy, and the DoD Information Assurance (IA) Strategy to share information and capabilities. The NCOW RM incorporates (or will incorporate) these strategies as well as any net-centric results produced by the Department's Horizontal Fusion pilot portfolio.

The NCOW RM provides the means and mechanisms for acquisition program managers to describe their transition from the current environment (described in GIG Architecture Version 1) to the future environment (described in GIG Architecture Version 2). In addition, the NCOW RM will be a key tool during program oversight reviews for examining integrated architectures to determine the degree of net-centricity a program possesses and the degree to which a program can evolve to increased net-centricity.

Compliance with the NCOW RM is one of the four elements that comprise the Net-Ready Key Performance Parameter.

7.2.2. Mandatory Policies

DoD Instruction 5000.2, Operation of the Defense Acquisition System, May 12, 2003**:**

Requires the DoD Chief Information Officer (CIO) to "lead the development and facilitate the implementation of the Global Information Grid Integrated Architecture, which shall underpin all mission area and capability architectures." (See Section 3.2.1.2).

Requires DoD acquisition programs to demonstrate consistency with GIG policies and architectures, to include relevant standards, at Milestones A, B and Full Rate Production Decision Review (FRPDR) (or their equivalent). (See Enclosure 4, Table E4.T1, Clinger-Cohen Act (CCA) Compliance Table).

A number of **other DoD directives and instructions** provide policies relating to the GIG. These include:

CJCS Instruction 6212.01, Interoperability and Supportability of Information Technology (IT) and National Security Systems, November 20, 2003**:**

> *It is DOD policy that all IT and NSS and major modifications to existing IT and NSS will be compliant with the Clinger-Cohen Act, DOD interoperability regulations and policies, and the most current version of the DOD Information Technology Standards Registry (DISR). Establishing interoperability and supportability in a DOD system is a continuous process that must be managed throughout the lifecycle of the system. The NR-KPP is comprised of the following elements: compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM), applicable Global Information Grid (GIG) Key Interface Profiles (KIP), DOD information assurance requirements, and supporting integrated architecture products required to assess information exchange and use for a given capability. (See paragraph 5.a.)*

DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), May 5, 2004**:**

> *IT and NSS, of the DoD Global Information Grid (GIG), shall provide for easy access to information, anytime and anyplace, with attendant information assurance. The GIG architecture shall be used as the organizing construct for achieving net-centric operations and warfare. (See paragraph 4.2.)*

DoD Directive 5000.1, The Defense Acquisition System, May 12, 2003, Enclosure 1, Additional Policy**:**

> *E1.9: Information Assurance. Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that*

depend on external information sources or provide information to other DoD systems.

E1.10: Information Superiority. Acquisition managers shall provide U.S. Forces with systems and families of systems that are secure, reliable, interoperable, compatible with the electromagnetic spectrum environment, and able to communicate across a universal information technology infrastructure, including NSS, consisting of data, information, processes, organizational interactions, skills, analytical expertise, other systems, networks, and information exchange capabilities.

E1.13: Interoperability. Systems, units, and forces shall be able to provide and accept data, information, materiel, and services to and from other systems, units, and forces and shall effectively interoperate with other U.S. Forces and coalition partners. Joint concepts and integrated architectures shall be used to characterize these interrelationships.

Directive 8000.1, Management of DoD Information Resources and Information Technology, February 27, 2002, Incorporating Change 1, March 20, 2002

DoD Directive 8100.1, Global Information Grid Overarching Policy, September 19, 2002 (Certified current as of November 21, 2003):

Addresses GIG Architecture compliance and includes the following requirements:

Section 4.3. [requires GIG assets to] be interoperable, in accordance with approved requirements documents, and compliant with the operational, system, and technical views … of the GIG architecture.

Section 4.4. [requires development of] an integrated DoD Architecture with operational, system, and technical views, [to be] maintained, and applied to determine interoperability and capability requirements, promote standards, accommodate the accessibility and usability requirements of reference (k), and implement security requirements across the DoD enterprise to provide the basis for efficient and effective acquisition and operation of IT capabilities.

Section 4.6. [The GIG Architecture] shall be the sound and integrated information technology architecture required by [the Clinger-Cohen Act of 1996].

7.2.3. Integration into the Acquisition Life Cycle

The following sections outline steps that the DoD Components, Combat Developers, Sponsors, Domain Owners, DoD Agencies, program managers, and/or other assigned managers should take to facilitate Global Information Grid (GIG) compliance and net-centricity when acquiring information technology-enabled capabilities that will interoperate within the GIG.

7.2.3.1. Before Milestone A

Ensure that appropriate steps are taken to prepare or update an operational view (High-level Operational Concept Description, OV-1) of the integrated architecture for key mission areas and business processes using the DoD Architecture Framework and the guidance in CJCS Instruction 6212.01, Enclosure E, paragraph 3. The Initial Capabilities Document should reflect this architecture work, as prescribed by CJCS Instruction 3170.01 and in the format prescribed by CJCS Manual 3170.01. It also supports analysis of alternatives, business process reengineering efforts, development of the acquisition strategy and acquisition Information Assurance (IA) strategy, and provides key artifacts that support development of the information support plan. Ensure that integrated architectures adhere to the three DoD net-centric strategies (Net-Centric Enterprise Services, Data, and Information Assurance Strategies) that have been incorporated into Net-Centric Operations and Warfare Reference Model.

For systems in the scope of the Business Management Modernization Program, architecture efforts should also align closely with the Business Enterprise Architecture.

Develop an Initial Capabilities Document to describe capability gaps identified through analysis of joint concepts and integrated architectures. Use the criteria in CJCS Instruction 6212.01, Enclosure E, Table E-1, "ICD Interoperability Standards Assessment Criteria," to ensure the Initial Capabilities Document and supporting OV-1 address required interoperability standards.

7.2.3.2. Before Milestone B

Build or update the integrated architecture and supporting views (Operational View, Systems View, and Technical Standards View).

Develop a Capability Development Document, as prescribed by CJCSI 3170.01 and in the format prescribed by CJCSM 3170.01, and a Net-Ready Key Performance Parameter (NR-KPP) that address the interoperability and Information Assurance requirements described in CJCS Instruction 6212.01, Enclosure F, "Net-Ready Key Performance Parameter."

Address issues associated with the updated integrated architecture, the Capability Development Document, and the Net-Centric Operations and Warfare Reference Model.

Use the required integrated architecture products to support development of the Information Support Plan. See CJCS Instruction 6212.01, Table A-2, "Joint Capabilities Integration and Development System Documents/NR-KPP Products Matrix."

Begin development of the Information Support Plan for Stage 1 Review. (See section 7.3.6 for details.)

Use the criteria in CJCS Instruction 6212.01, Enclosure E, Table E-2, "Net-Centric Assessment Criteria," to guide the acquisition of net-centric capabilities.

7.2.3.3. Before Milestone C

Update the integrated architecture and supporting views (Operational View, Systems View, and Technical Standards View) and ensure changes are reflected in the

Capability Production Document, as prescribed by CJCS Instruction 3170.01 in the format prescribed by CJCS Manual 3170.01, and in the Net-Ready Key Performance Parameter (NR-KPP).

If the program is entering the acquisition process at Milestone C, develop a NR-KPP using guidance in CJCS Instruction 6212.01, Enclosure G, "Net-Ready Key Performance Parameter."

Address any remaining issues associated with mapping to the Net-Centric Operations and Warfare Reference Model, especially those related to Service-Level Agreements. A Service-Level Agreement defines the technical support, business parameters, and/or critical interface specifications that a service provider will provide to its clients. The agreement typically spells out measures for performance parameters and protocols used in interfacing, and consequences for failure.

Ensure the program delivers capabilities responsive to the Capability Production Document and meets interoperability and Information Assurance requirements reflected in the updated NR-KPP.

Use the criteria in CJCS Instruction 6212.01, Enclosure G, Table G-3, "Net Centric Assessment Criteria" to ensure services and data products delivered by the acquisition align with the Department's objectives for net-centricity.

Prepare and submit the Information Support Plan for final Stage 2 Review. (See section 7.3.6 for details.)

Address all information exchange requirements as part of the Information Support Plan Interoperability Requirements Certification and the Information Technology and National Security Systems Interoperability Certification processes.

7.2.3.4. After Milestone C and the Full-Rate Production Decision Review,

Continue Lifecycle compliance with the Information Support Plan Interoperability Requirements Certification and the Information Technology and National Security System Interoperability Certification.

Continue Lifecycle compliance with Information Assurance Certification and Accreditation.

7.2.4. Global Information Grid (GIG) Architecture-Related Guidance

The following paragraphs describe the major sources of guidance and tools related to the GIG Architecture and supporting DoD strategies for implementing the architecture in Information Technology and National Security Systems programs. Program managers and Sponsors/Domain Owners should use the guidance, tools, and strategies outlined below throughout a program's Lifecycle to meet a variety of statutory and regulatory requirements.

7.2.4.1. DoD Architecture Framework (DoDAF)

The DoDAF provides the rules, guidance, and product descriptions for developing and presenting architecture descriptions to ensure a common denominator for understanding, comparing, and integrating architectures. An integrated architecture consists of multiple views or perspectives (Operational View (OV), Systems View (SV), Technical Standards View (TV) and All View (AV)) that facilitate integration and promote interoperability across capabilities and among related integrated architectures.

The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions.

The SV is a description, including graphics, of systems and interconnections providing for, or supporting, DoD functions.

The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

The AV products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture.

Typically the Combat Developer (or Domain Owner/Sponsor) will be responsible for the architecture description prior to Milestone B with the program manager taking on the responsibility subsequent to the approval at Milestone B.

(See https://pais.osd.mil/enterprisearchitectures)

7.2.4.2. DoD Information Technology (IT) Standards Registry (DISR)

A new capability, called the DoD IT Standards Registry (DISR), is an online repository for a minimal set of primarily commercial IT standards formerly captured in the Joint Technical Architecture (JTA), Version 6.0. These standards are used as the “building codes” for all systems being procured in the Department of Defense. Use of these building codes facilitates interoperability among systems and integration of new systems into the Global Information Grid (GIG). In addition, the DISR provides the capability to build profiles of standards that programs will use to deliver net-centric capabilities.

When building systems, requests for proposals and contract statements of work should be reviewed as part of approved acquisition processes to ensure IT standards established in Initial Capabilities Documents, Capability Development Documents, and Capability Production Documents are translated into clear contractual requirements. In addition, requests for proposals and contract statements of work should contain additional requirements for contractors to identify instances where cost, schedule, or performance impacts may preclude the use of IT standards mandated in DISR.

Key net-centric elements that program architectures should focus on include:

Internet Protocol – Ensure data packets are routed across network, not switched via dedicated circuits. Focus on establishing IP as the convergence layer.

Secure and Available Communications – Encrypted initially for core network; goal is edge-to-edge encryption and hardened against denial of service. Focus is on Black

(encrypted) Transport Layer to be established through the Transformational Communications Architecture implementation.

Assured Sharing – trusted accessibility to net resources (data, services, applications, people, devices, collaborative environment, etc). Focus on assured access for authorized users and denied access for unauthorized users.

Quality of Service – Data timeliness, accuracy, completeness, integrity, availability, and ease of use. This is envisioned as being measured through the Net-Ready Key Performance Parameter. Focus on Service Level Agreements and service protocols with quality and performance metrics.

7.2.4.3. Core Architecture Data Model (CADM)

Provides a common approach for organizing and portraying the structure of architecture information, and is designed to capture common data requirements. The CADM facilitates the exchange, integration, and comparison of architecture information throughout the Department of Defense, improving joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance interoperability.

7.2.4.4. Global Information Grid (GIG) Capstone Requirements Document

This is required for legacy Capstone Requirements Documents and Capstone Requirements Document updates directed by the Joint Requirements Oversight Council.

7.2.4.5. DoD Net-Centric Data Strategy

The Data Strategy provides the basis for implementing and sharing data in a net-centric environment. It describes the requirements for inputting and sharing data, metadata, and forming dynamic communities to share data. Program managers and Sponsors/Domain Owners should comply with the explicit requirements and the intent of this strategy, which is to share data as widely and as rapidly as possible, consistent with security requirements. Additional requirements and details on implementing the DoD Data Strategy are found in section 7.4. Specific architecture attributes associated with this strategy that should be demonstrated by the program manager include:

Data Centric – Data separate from applications; applications talk to each other by posting data. Focus on metadata registered in DoD Metadata Repository.

Only Handle Information Once – Data is posted by authoritative sources and made visible, available, and usable (including the ability to re-purpose) to accelerate decision-making. Focus on re-use of existing data repositories.

Smart Pull (vice Smart Push) – Applications encourage discovery; users can pull data directly from the net or use value added discovery services. Focus on data sharing, with data stored in accessible shared space and advertised (tagged) for discovery.

Post in Parallel – Process owners make their data available on the net as soon as it is created. Focus on data being tagged and posted before processing.

Application (Community of Interest (COI) Service) Diversity – Users can pull multiple applications (COI Services) to access same data or choose same applications (Core and COI Services) for collaboration. Focus on applications (COI service) posting and tagging for discovery.

7.2.4.6. DoD Information Assurance (IA) Strategy

The Net-Centric Information Assurance (IA) Strategy describes the DoD strategy for integration of information assurance into the global, net-centric information environment. The end-to-end IA component of the GIG is comprised of a set of informational documents and DoD Architecture Framework (DoDAF) products (tools) that define information assurance constructs as conceptualized and specified for integration of IA into the net-centric information environment in support of a secure, globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, defense policymakers, and support personnel. The intent of the Net-Centric IA Strategy is to reflect an approach to IA concepts and definitions from a "services" point-of-view instead of a "system" point-of-view, without specifying requirements related to specific implementations or architectures.

7.2.4.7. Global Information Grid (GIG) Enterprise Services (GIG ES) Capability Development Document

The GIG ES Capability Development Document is currently focused on nine core enterprise services to be provided by the Net Centric Enterprise Services (NCES) Program. These services are the foundation for the initial net-centric capabilities to be provided by the Defense Information Systems Agency. The Capability Development Document describes the overall set of services in detail.

The NCES program will develop the core enterprise services incrementally. The NCES Program Plan describes the increments and their anticipated schedule. Each program that is dependent upon the core services being developed by the NCES program should address the impact of the incremental NCES schedule on their program. The Net-Centric Operations and Warfare Reference Model (NCOW RM) provides a basis for discussing issues associated with these core services. Table 7.2.4.7.1. shows the relationship of the nine Core Services articulated in the GIG ES Capability Development Document to the services articulated in the NCOW RM.

GIG ES Capability Development Document/NCES	NCOW RM Activity
Application	A316 (Provide Applications Services)
Collaboration	A312 (Provide Collaboration Services)
Discovery	A311 (Perform Discovery Services)
Enterprise Services Management/NetOps	A33 (Environment Control Services) and A5 (Manage Net-Centric Environment)
Information Assurance/ Security	A33 (Environment Control Services) and A5 (Manage Net-Centric Environment)
Mediation	A314 (Perform Information Mediation Services)
Messaging	A313 (Provide Messaging Services)
Storage	A315 (Perform Information Storage Services)
User Assistance	A2 (Perform User Agent Services)

Table7.2.4.7.1. Mapping of Global Information Grid Enterprise Services/Net Centric Enterprise Services Core Services to Net-Centric Operations and Warfare Reference Model Services

7.2.5. Compliance with the Global Information Grid (GIG)

Compliance with the GIG means an information technology-based initiative or an acquisition program, throughout its lifecycle:

1. Meets the DoD Architecture Framework (DoDAF) requirements in producing architectural products. This requirement is met by producing a complete integrated architecture using the specified products described in the DoDAF and having it assessed for accuracy, consistency, and sufficiency with respect to its intended use (e.g., capability definition, process re-engineering, investment decisions, and integration engineering).
2. Meets the Core Architecture Data Model (CADM) requirements for using/reusing architecture data. This requirement is met through reuse of CADM data in a program's integrated architecture and through contributing new reusable architecture data (if any) to the CADM.
3. Meets the DoD Information Technology Standards Registry (DISR) requirements in selecting technologies and standards. This requirement is met by defining and implementing capabilities, based on technologies and standards contained within

the JTA/DISR. Meeting this requirement should be validated at every milestone. When building systems, requests for proposals and contract statements of work should be reviewed as part of approved acquisition processes to ensure IT standards established in Initial Capabilities Documents, Capability Development Documents, and Capability Production Documents are translated into clear contractual requirements. In addition, requests for proposals and contract statements of work should contain additional requirements for contractors to identify instances where cost, schedule, or performance impacts may preclude the use of IT standards mandated in DISR.

4. Meets the DoD Net-Centric Data Strategy requirements and intent. Make explicit the data that is produced and used by the program's implemented operations. Provide the associated metadata, and define and document the program's data models. This requirement is met by:

    a. Describing the metadata that has been registered in the DoD Data Metadata Registry for each data asset used and for each data asset produced (i.e., data for which the program is the Source Data Authority).

    b. Providing the documented data models associated with the program.

5. Explicitly addresses net-centricity and determine the program's net-centric correspondence to key net-centric criteria (e.g., concepts, processes, services, technologies, standards, and taxonomy). (For further information see the Net-Centric Operations and Warfare Reference Model (NCOW RM) Compliance Assessment Methodology (Draft) - found on the GIG Architecture website). An important aspect of this is the program's mapping of its operational, systems, and technical view content to the NCOW RM key net-centric criteria. This correspondence shall describe-in terms of the programs content---operational, systems, and technical view-what the program provides, what the program dependencies are, and what the program gaps are. The correspondence shall also provide additional information related to the NCOW RM and its emerging technologies and standards, and a transition roadmap (when gaps are identified). Additionally, the program shall provide an explicit evaluation of risk with respect to achieving net-centricity at each program milestone.

6. Meets the broad requirements set forth in the GIG Capstone Requirements Document. This requirement is met by describing the program elements that address each requirement and by expressing an overall degree of conformance to the GIG Capstone Requirements Document. Where conformance cannot be achieved, appropriate rationale and associated risks (near, mid, and/or long term) should be presented.

7.2.6. Compliance with the Net-Centric Operations and Warfare Reference Model (NCOW RM)

The NCOW RM is focused on achieving net-centricity. Compliance with the NCOW RM translates to articulating how each program approaches and implements net-centric features. Compliance does not require separate documentation; rather, it requires that program managers and Sponsors/Domain Owners address, within existing architecture,

analysis, and program architecture documentation, the issues identified by using the model, and further, that they make explicit the path to net-centricity the program is taking.

To this end, the material below will help program managers and Sponsors/Domain Owners in this articulation. It describes the features of net-centricity, key strategies in attaining net-centricity, and how to use the NCOW RM as a common basis for discussing program architectures and corresponding implementations with respect to these DoD net-centric strategies.

7.2.6.1. Features of Net-Centricity

Transforming to a net-centric environment requires satisfying four key features: *reach*, *richness*, *agility*, and *assurance*.

- **Reach** can be operationally defined in terms of space-time where "distance is not a factor," but recognizing that the integration of spatially disconnected capabilities costs time (i.e., there is a minimum delivery time). Time is the dominant limitation in success!
- **Richness** can be operationally defined in terms of the total set of expertise, information, and/or capabilities that can be brought to bear, within a unit of time, to effect a decision or an action subsequent to a decision. Richness contributes to driving the margin of uncertainty in a decision or action downward.
- **Agility** can be operationally defined in terms of the number of effective adaptations that can be accomplished per unit of time. Thus, highly agile capabilities are those that can anticipate or react and successfully adapt to changes in the environment faster than less agile capabilities.
- **Assurance** can be operationally defined in terms of achieving expected levels of operational and systems performance within a specified context, including an adversarial force in a specified timeframe. Adversarial force (i.e., counters to assurance) is measured in terms of work-factors (time to accomplish a condition or effect) and probabilities (likelihood of occurrence). Note that this is a broad definition of assurance that includes the general concept of information assurance. Assurance should:

  Provide the capability to deter an adversarial force.

  Prevent adversarial force from succeeding within a specified time and/or detect an adversarial force when it is being applied in time to provide mitigating responses to counter such a force application.

  Provide the capability to recover in a timely fashion from an adversarial force, given that the application of such a force has succeeded to some degree.

Assurance can be directly related to the time-value of mission operations. That is, the time-value related to mission might be assessed by the following types of questions:

Can the mission succeed within the resources/unit time expected?

Can mission performers respond to operational and systems failures, and still succeed within some time boundary?

Can operational or system resources be reconstituted, upon catastrophic failure, in time to still enable mission success?

7.2.6.2. Key Strategies for Achieving Net-Centricity

The initial means for attaining these net-centric features include implementing the Net-Centric Enterprise Services (NCES), Net-Centric Data, and Information Assurance (IA) Strategies to share information rapidly and widely.

The NCES Strategy focuses on achieving a set of Net-Centric Enterprise Core Services (NCE--being developed by Defense Information Systems Agency) that can be dynamically shared and used by everyone in conjunction with selectable sets of Community of Interest (COI) services to rapidly assemble information capabilities and integrate processes as needed. Core services may be developed within a program, when it is determined that the core services of the NCES Program cannot meet program needs and then made available to the Enterprise for reuse. COI services, as identified by a program, are expected to be developed and registered by every program that contributes to the evolution of the Global Information Grid (GIG). Environment Control services, as expressed in the Net-Centric Operations and Warfare Reference Model are expected to be provided through DoD GIG End-to-End IA Initiative and through other programs contributing to the GIG. Reuse of registered services is strongly encouraged. This service-oriented approach enables flexibility in reuse of service modules and a more loosely coupled infrastructure that can be adapted more readily to changing operational needs.

The Net-Centric Data Strategy focuses on more rapid, widespread, and agile data sharing through the establishment of dynamic COIs, and includes concepts such as Only Handle Information Once; Task, Post, Process, and Use; and the use of descriptive metadata tagging.

The IA Strategy (See DoD IA Strategy and section 7.4 of this chapter) focuses on assuring information processing, transport, storage, and the dynamic sharing of information within and across DoD boundaries. Tagging is also central to the IA strategy.

7.2.6.3. How to Use the Net-Centric Operations and Warfare Reference Model (NCOW RM)

These strategies have been captured in the Guidebook Chapter and program managers and sponsors/ domain owners can use the NCOW RM to help describe how they are implementing these strategies in their programs.

NCOW RM objectives include:

- Providing a model that guides the development of net-centric architectures throughout the Department.

- Supporting the identification, description, and evolution of enterprise information technology capabilities required for operating in the net-centric environment.
- Providing a model that can be used to support oversight and governance of Global Information Grid (GIG) net-centric transformation.

Conformance to the NCOW RM means that a program:

- Uses NCOW RM definitions and vocabulary
- Incorporates NCOW RM capabilities and services (or demonstrates equivalence) in its materiel solution, including those represented by the:
    - Net-Centric Enterprise Services Strategy
    - Net-Centric Data Strategy
    - Net-Centric Information Assurance Strategy
- Incorporates NCOW RM Information Technology and National Security Systems standards in the Technical View products developed for its materiel solution.

7.2.6.4. A Step-By-Step Approach

Compliance does not require separate documentation; rather, it requires that the Combat Developers, DoD Agencies, or program managers address, within existing architecture, analysis, and program documentation products, the issues identified by using the model and further they make explicit the path to net-centricity the program is taking. Using the model consists of the following steps:

1. Establishing the categorical positioning of the program with respect to the overall DoD enterprise. This is accomplished by articulating the domain decomposition in which the program exists by describing its domain and "portfolios of capabilities"
    - For example, the Warfighter Domain may consist of Joint Command and Control (C2), Force Application, Force Protection, Focused Logistics, or Battlespace Awareness Sub-Domains.
    - If the program is associated with a platform (e.g., Joint Strike Fighter), it may belong primarily in the Force Application Sub-Domain, but have "portfolios of capabilities" in the Joint C2, Battlespace Awareness, and Force Protection Sub-Domains.
    - More specifically, the Joint Strike Fighter may have communication (e.g. TADIL, IP, etc) links that cover several Sub-Domains, it may have integrated test capabilities that support the Focused Logistics Sub-Domain, and it may have integrated avionics, navigation, targeting, and fire control that support the platform itself and its weapons, within Force Application Sub-Domain.

It is the program's set of operational functions, activities, applications, services, and interface descriptions that are categorized into these portfolios that is of interest. These portfolios will be referenced in establishing the set of program-provided "Community of

Interest (COI) Service" with respect to the Net-Centric Operations and Warfare Reference Model (NCOW RM).

2. Determining the program architecture's degree of NCOW RM correspondence by activity mapping. This requires orientation of the program's architecture to the NCOW RM activity decomposition. (Note - Additional guidance and specific examples of mapping to cover services/systems or technical views will be provided in the next release of the DoD Acquisition Guidebook.)

   - The landmark for activity mapping orientation is the NCOW RM COI Services and more specifically, the categorical portfolios established in step one, (e.g., Domain--Warfighter, Business, Intelligence, Enterprise Management, and/or Enterprise Information Management) are placed within the A321 or A322 blocks of COI Services. Examples (for illustration only) might include:

     1. A321 - Warfighter: Joint Future Combat System: (JTF) Engagement Execution Control.

     2. A321 - Warfighter: Army Future Combat System: (Unit of Action) Tactical Execution Control.

     3. A321 - Business: BEA: Provide Educational Benefits: Application for Benefits.

     4. A321 - Business: BEA: Provide Educational Benefits: Determine Eligibility.

     5. A322 - Modeling & Simulation: Warfighter Joint: Theater Engagement Modeling.

     6. A322 - Training: Enterprise Information Environment Management: NetOps: Global (Tier 1) Joint: Assess Threats: CND Watch Officer.

   - Mapping Correspondence to NCOW RM. By placing the program's operational activity model (i.e., its portfolio of COI Services) into the NCOW RM 's COI Services, a PM can map the program's "similarity" and/or identify the specific use of NCOW RM Activities (e.g., Core Services and Environmental Control Services).

     1. COI Services export to the User Interaction Activity a set of Capability Interfaces (i.e., the program's user interactions). These are specializations of the generic capabilities identified in the NCOW RM User Interaction Activity. A program may have both specialized and generic interfaces, but is not expected to have just the NCOW RM generic interfaces.

     2. If the program utilizes the concept of a User Assistant, it will map to it. If not, it will indicate that it is currently not applicable (i.e. a potential future gap).

     3. If the program is dependent upon Net-Centric Enterprise Services (NCES) for its Core Services, it should indicate that fact and detail any

issues associated with incremental deployment of the DoD's NCES program. If it is providing its own set of core services, it should describe the correspondence of their core service set to the NCOW RM Core Services.

4. The program must map its policies and controls to the Environment Control Services. That is, all program policies associated with implementing and integrating Enterprise Information Environment control must be made explicit. Enforcement issues (e.g., where and/or how a policy is to be enforced) should be raised, especially if enforcement is dependent upon other Global Information Grid (GIG) participants. These policies might be needed within the program to ensure a specific quality of service, a specified condition of maintaining confidentiality while sharing information, or the least privilege aspects of a given role being instantiated through the program. The controls might identify specific parameters and mechanisms that the program will need to enable and enforce such policies. For example, the adaptive encryption controls within a software-based radio may provide for the needed confidentiality in using shared space.

5. The program must identify the computing, communications, and storage resources it will use, especially those to provide a wider sharing of information. Policies associated with use dynamics and resource allocation must be made explicit. The physical resources (e.g., computing, communications, and storage) the program is providing must be identified with explicit sharing policies.

6. The program must address its approach to managing its information environment and how that approach integrates with the overall approach for managing the GIG (e.g., NetOps). The Manage Enterprise Information Environment Activity represents a set of services associated with Enterprise Information Environment (EIE) Management and Operations. Each program must articulate its local, regional, and global EIE management aspects, identifying what it provides and what it is dependent upon.

7. Finally, the program mapping must show (a) what activities the program depends upon from the GIG (e.g., GIG Enterprise Services); (b) what activities the program provides to the GIG (e.g., new control policies, new control mechanisms, new services); and (c) activity gap--where the source of fulfilling the program requirement cannot be readily identified (e.g., Identity Management), or a required component will not be readily available when needed (e.g., tactical-level core services).

- A capabilities roadmap should be derived from this mapping. This roadmap should be part of the Capability Development Document.
- Service-Level Agreements should be established and incorporated into the Capability Production Document.

1. A service-level agreement should be made with each provider of a supporting capability to assure accountability for each external dependency. The Capability Production Document should address these agreements.

2. A service-level agreement should be made with each program consumer of a supported capability to assure accountability for each dependency upon the program. The Capability Production Document should address these agreements.

- The Program Manager should address the risk of not achieving the net-centric strategies represented in the Reference Model and gap mitigation in the Analysis of Alternatives, and in the Initial Capabilities Document, Capability Development Document, and Capability Production Document.

3. Identifying information producer and consumer relationships that the program serves (e.g., those that are currently known and those for which data may be re-purposed). Specifically identify all producer/consumer relationships that originate external to the GIG (e.g., allies, coalition partners, commercial business, and other Federal Government). These relationships are part of the integrated architecture and should be addressed in the Capability Development Document.

4. Identifying the requirement for close-coupled relationships and those relationships that can be more loosely coupled. Address in the Capability Development Document.

5. Identifying the metadata for all data assets created in the program's implemented operations and aligning those assets with similar data assets within the program's domain(s). These data assets must be registered in the DoD Metadata Repository in accordance with the DoD Data Strategy.

6. Identifying the data assets to be used or consumed in the program's implemented operations and ensuring that such assets have been identified with metadata and that this metadata is registered in the DoD Metadata Repository in accordance with the DoD Data Strategy.

7. Identifying all policy needs of the program that must be incorporated or accommodated by the Environment Control Services (e.g., authentication, authorization, fault-tolerance, continuity of operations, qualities of service). These are both policy-enabling activities and policy enforcing activities. Policy, and its associated parameters, should be made explicit and not left implicit. Identify the differences between enterprise-level policies and program-level policies. This should be addressed in the Capability Development Document and in the integrated architecture.

8. Identifying the emerging technologies and standards that will (might) be used in the program's implementation. This should be addressed in the Capability Development Document and in the integrated architecture. In this identification, both the utility expected and the risks to be mitigated should be addressed. Planned upgrades and migration strategies should be addressed in the Capability Development Document.

7.2.7. Net-Centric Operations and Warfare Reference Model (NCOW RM) Compliance Assessment Methodology

Compliance evaluation, or assessment, will be performed by inspection and analysis of a program's documentation against specific criteria related to the NCOW RM. These criteria are grouped into net-centric concepts, processes, services, standards, and taxonomy and are described below:

Concept: Analysis and review of the program's Overview and Summary Information (AV-1), High Level Operational Concept Graphic (OV-1), and other products (e.g. - DoD Architecture Framework (DoDAF) diagrams or reports, the Analysis of Alternatives, the Capability Development Document, etc.) to determine if the program conforms to NCOW RM concepts as expressed in the three key DoD net-centric strategies: Data, Information Assurance, and Global Information Grid (GIG) Enterprise Services.

- **Processes:** Analysis and review of the program's Operational Node Connectivity Description (OV-2), Activity Model (OV-5), Operational Event/Trace Description (OV-6C), Operational Information Exchange Matrix (OV-3), and other products (e.g. - DoDAF diagrams or reports, the Analysis of Alternatives, the Capability Development Document, etc.) to determine the degree of the program's correspondence to NCOW RM operational activities and process threads.
- **Services:** Analysis and review of the System Interface Description (SV-1), System Communications Description (SV-2), Operational Activity to Services/System Function Traceability Matrix (SV-5 (SER)), and other products (e.g. - DoDAF diagrams or reports, the Analysis of Alternatives, the Capability Development Document, etc.) to determine if the program conforms to NCOW RM Core Services (such as Discovery, Mediation, etc), Community of Interest Services, and Enterprise Control Services.

Standards: Analysis and review of the Technical Architecture Profile (TV-1) and possibly the Systems Evolution Description (SV-8), if required, and other products (e.g. - DoDAF diagrams or reports, the Analysis of Alternatives, the Capability Development Document, etc.) to determine if the program uses appropriate current standards from the DoD Information Technology Standards Resposity (DISR) and emerging technologies identified in the NCOW RM Target Technical View to accomplish net-centric concepts, processes, and services. Issues of interoperability and information assurance will be addressed in this assessment area.

- **Taxonomy:** Analysis and review of the Integrated Dictionary (AV-2) to ensure common language and definitions are used and are consistent with the NCOW RM (AV-2).

7.2.8. Architecture Product Requirements

The following policy-based Architecture Product Requirements table (Table 7.2.8.1.) aligns architecture products required for Joint Capabilities Integration and Development System products (Initial Capabilities Documents, Capability Development Documents, etc.) and shows the DoD policy source for each requirement. These requirements

continue throughout the Joint Capabilities Integration and Development System and Defense Acquisition processes.

POLICY	AV-1	AV-2	OV-1	OV-2	OV-3	OV-4	OV-5	OV-6c	SV-1	SV-2	SV-4	SV-5	SV-6	SV-10c	TV-1
DODD 5000.1															
No Product Requirements															
DODI 5000.2															
No Product Requirements															
DODD 4630.5															
No Product Requirements															
DODI 4630.8															
ISP	X	1	X	X		X	X	X	X		X	X	X		X
ISP NR-KPP	X			X		X	X	X			X	X	X		X
CJCSI 3170.01															
No Product Requirements															
CJCSM 3170.01															
ICD			X												
CDD	X			X		X	X	X			X	X	X		2
CPD	X			X		X	X	X			X	X	X		3
CRD			4		4		4								
CJCSI 6212.01															
ICD			X												
CDD NR-KPP	X			X		X	X	X			X	X	X		X
CPD NR-KPP	X			X		X	X	X			X	X	X		X
CRD (I-KPP)			4		4										
CRD (NR-KPP)			4				4								
DODAF															
Integrated Architecture	X	X		X	X		X		X						X

Table7.2.8.1. Policy-Based Architecture Product Requirements

Legend:

X - Required Architecture Product

1 - Acronym List

2 - Draft Information Technology (IT) Standards Profile generated by DoD IT Standards Registry (DISR)

3 - Final IT Standards Profile generated by DoD IT Standards Registry (DISR)

4 - Required for legacy Capstone Requirements Documents and Capstone Requirements Document updates directed by the Joint Requirements Oversight Council.

Policy-based Products:

- DoD Directive 5000.1, DoD Instruction 5000.2, DoD Directive 4630.5, and CJCSI 3170.01 do not show requirements for architecture products.
- DoD Instruction 4630.8
- ISP - Information Support Plan (Replaces C4I Support Plan - C4ISP)
- NR-KPP - Net-Ready Key Performance Parameter
- ISP NR-KPP - NR-KPP for an ISP
- ICD - Initial Capabilities Document
- Capability Development Document - Capability Development Document
- CPD - Capability Production Document
- CRD - Capstone Requirements Document
- Capability Development Document NR-KPP - NR-KPP for a Capability Development Document
- CPD NR-KPP - NR-KPP for a CPD
- CRD (I-KPP) - CRD based on an Interoperability KPP
- CRD (NR-KPP) - CRD based on a NR-KPP
- Policy References do not show requirements for OV-6b, OV-6a, OV-7, SV-3, SV-7, SV-8, SV-9, SV-10a, SV-10b, SV-11, or TV-2.

7.2.9. DoD Chief Information Officer (CIO) Use of the Global Information Grid (GIG) Architecture

The DoD CIO uses the GIG Architecture in all three of the major decision processes of the Department (see Chapter 1).

The DoD CIO uses the GIG architecture throughout the processes included in operating the Joint Capabilities Integration and Development System to:

- Advise the Joint Requirements Oversight Council.

- Provide the basis for the development and refinement of joint integrated architectures by the Joint Staff and other DoD Components in support of the Joint Capabilities Integration and Development System.
- Develop assessments and provide recommendations to the JROC; the GIG Architecture, including its concepts, products, data, conclusions, and implications provides a key source for these assessments.

The DoD CIO uses the GIG architecture throughout the Planning, Programming, Budgeting, and Execution process to:

- Review and provide recommendations for development of the Strategic Planning Guidance and the Joint Programming Guidance.
- Provide recommendations to the Senior Level Review Group relating to Information Technology, National Security Systems, interoperability, and information assurance.
- Review and evaluate Program Change Proposals and Budget Change Proposals relating to Information Technology, National Security Systems, interoperability, and information assurance.
- Provide recommendations for Program Objective Memorandum planning and programming advice.

Finally, the DoD CIO uses the GIG Architecture throughout the Defense Acquisition Process to:

- Provide the basis for clear and comprehensive guidance in Information Technology Acquisition Decision Memoranda.
- Form and support his decisions and recommendations as a member of the Defense Acquisition Board, the lead for the Information Technology Acquisition Board, and the Milestone Decision Authority for Acquisition Category IA programs.
- Identify and specify Information Technology and National Security Systems implications associated with systems acquisition.
- Assess interoperability and supportability during the Overarching Integrated Product Team process.
- Review Information Support Plans and evaluate the interoperability, interoperability key performance parameters, and information assurance aspects of those plans.

7.2.10. Net-Centric Attributes

Combat Developers, DoD Agencies, and program managers may use the Net-Centric Checklist available from ASD(NII) as an additional net-centric assessment aid.

Table 7.2.10.1. outlines the major characteristics of net-centricity. Combat Developers, DoD Agencies, and program managers should ensure acquisition programs adhere to the policies, standards, and design tenets outlined below. For a more detailed discussion, see

CJCS Instruction 6212.01, Enclosure E, Table E-2, “Net Centric Assessment Criteria and the NCOW RM”.

Title	Description	Metric	Source
Internet Protocol (IP)	Data packets routed across network, not switched via dedicated circuits	**IP as the Convergence Layer** Net-Centric Operations and Warfare Reference Model (NCOW RM), Technical View compliant with JTA v6.	NCOW RM, GIG Arch v2, IPv6 Memos (9 Jun 03 and 29 Sep 03), DISR
Secure and available communications	Encrypted initially for core network; goal is edge-to-edge encryption and hardened against denial of service	**Black Transport Layer** Transformational Communications Architecture (TCA) compliance; Technical View compliant with DISR	TCA; IA Component of Assured GIG Architecture; DISR
Only handle information once (OHIO)	Data posted by authoritative sources and visible, available, usable to accelerate decision making	**Reuse of existing data repositories**	Community of interest policy (TBD)
Post in parallel	Business process owners make their data available on the net as soon as it is created	**Data tagged and posted before processing** NCOW RM, Technical View compliant with DISR	NCOW RM, DoD Net-Centric Data Strategy (9 May 03) DISR
Smart pull (vice smart push)	Applications encourage discovery; users can pull data directly from the net or use value-added discovery services	**Data stored in public space and advertised (tagged) for discovery** NCOW RM, Technical View compliant with DISR	NCOW RM; DoD Net-Centric Data Strategy (9 May 03); DISR
Data centric	Data separate from applications; apps talk to each other by posting data	**Metadata registered in DoD Metadata Registry** NCOW RM, Technical View compliant with DISR	NCOW RM; DoD Net-Centric Data Strategy (9 May 03); DISR
Application diversity	Users can pull multiple apps to access same data or choose same app (e.g., for collaboration)	**Apps posted to net and tagged for discovery** NCOW RM, Technical View compliant with DISR	NCOW RM; JTA Memo DISR
Assured Sharing	Trusted accessibility to net resources (data, services, apps,	**Access assured for authorized users; denied for unauthorized users**	Security/IA policy (TBD);

	people, collaborative environment, etc.)		IA Component of Assured GIG Architecture; DISR
Quality of service	Data timeliness, accuracy, completeness, integrity, and ease of use	Net-ready key performance parameter	Service level agreements (TBD); DISR

Table7.2.10.1. Net-Centric Characteristics

7.3 Interoperability and Supportability of Information Technology and National Security Systems

7.3.1 Interoperability and Supportability

Interoperability is the ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information Technology (IT) and National Security Systems interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations and missions over the life cycle, and it should be balanced with information assurance.

Supportability for Information Technology systems and National Security Systems is the ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain the design, development, testing, training, or operations of the IT or NSS to achieve its required operational and functional capability(ies).

7.3.2. Mandatory Policies

DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

> 4.1. *IT and NSS employed by U.S. Forces shall, where required (based on capability context), interoperate with existing and planned, systems and equipment, of joint, combined and coalition forces and with other U.S. Government Departments and Agencies, as appropriate.*
>
> 4.3. *IT and NSS interoperability and supportability needs, for a given capability, shall be identified through:*
>
> - The Defense Acquisition System (as defined in the DoD 5000 series issuances);
> - the Joint Capabilities Integration and Development System process;
> - and the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) change recommendation process (see CJCSI 3180.01, Joint Requirements Oversight Council (JROC) Programmatic Processes For Joint Experimentation And Joint Resource Change Recommendations*).*
>
> *4.5. IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system's life, or upon changes affecting interoperability or supportability, to assess, evaluate, and certify its overall interoperability and supportability within a given capability. Joint interoperability certification testing shall be as comprehensive as possible, while still being cost effective, and shall be completed prior to fielding of a new IT and NSS capability or upgrade to existing IT and NSS.*

4.8. Interoperability and supportability needs shall be balanced with requirements for Information Assurance (IA)

DoD Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

E3.1.5.A Net-Ready Key Performance Parameter (NR-KPP), consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. A NR-KPP shall be defined for all IT and NSS defense acquisition and procurement programs and shall be specified to a level of detail that allows verification of interoperability throughout a system's life. The defined NR-KPP shall be developed in such a way that it can be reliably measured, tested and evaluated.

E3.1.6.IT and NSS interoperability and supportability needs shall be managed, evaluated, and reported over the life of the system using an Information Support Plan (ISP). For all DoD Acquisition Category (Acquisition Category) programs and non-Acquisition Category acquisitions and procurements, an Information Support Plan (ISP) shall be produced and used to analyze interoperability and supportability requirements specified in the NR-KPP.

Note: Paragraph 7.3.6.7 of this guide provides detailed guidance on ISPs.

6.2.3.6.1.All IT and NSS, regardless of Acquisition Category, must be tested for interoperability before fielding and the test results evaluated and systems certified by the DISA (JITC). IT and NSS interoperability test and evaluation shall be conducted throughout a system's life, and should be achieved as early as is practical to support scheduled acquisition or procurement decisions. Interoperability testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early-user test) whenever possible to conserve resources.

6.2.3.6.2.IT and NSS interoperability testing can occur in multiple stages. Evolutionary acquisitions or procurements, and normal Lifecycle modifications, result in a progressively more complete capability. Therefore, there may be instances when it is important to characterize a system's interoperability before all critical interface requirements have been tested and certified. However, all critical interfaces, identified in the NR-KPP, which have been tested, must be successfully certified for interoperability prior to fielding. When appropriate (e.g., between successful completion of operational testing and the fielding decision), the DISA (JITC) shall issue interim interoperability certification letters specifying which of the system's interoperability needs have been successfully met and which have not. The DISA (JITC) shall issue an overall system certification once the system successfully meets all requirements of the NR-KPP validated by the Chairman of the Joint

Chiefs of Staff. The DISA (JITC) shall provide interoperability certification letters to the USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, the DPA&E, the DOT&E the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, as well as to the OTA and program manager, as applicable.

6.2.3.7.Interoperability Reviews. IT and NSS shall be subject to interoperability reviews over the life of a system to determine if interoperability objectives are being met. The Interoperability Senior Review Panel (ISRP) comprised of senior officers from the following DoD Organizations: the USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, the DOT&E, the DPA&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM; reviews and assesses interoperability to identify IT and NSS interoperability deficiencies. Multiple sources may be used to identify IT and NSS interoperability deficiencies including Joint Capabilities Integration and Development System documents; ISPs; TEMPs and operational test plans; and observation of tests and exercises by the DOT&E and the OTAs, the USJFCOM interoperability priority list, the Joint Warfighting Capability Assessments, program management offices, the MCEB, the MIB, DISA, DoD Component interoperability testing organizations, and the Joint C4ISR Battle Center. Identified IT and NSS interoperability deficiencies may pertain to both the technical exchange of information and the end-to-end operational effectiveness of that exchange required for mission accomplishment.

Note: The Interoperability Senior Review Panel maintains an Interoperability Watch List (IWL). DoD Instruction 4630.8, paragraph 6.2.3.8.1, discusses procedures for placing programs with significant interoperability deficiencies on the IWL. Program managers should be aware of the process and the criteria for nominating programs to the IWL.

DoD Directive 5000.1, The Defense Acquisition System, Enclosure 1

Paragraph E1.10.: Establishes the requirement to acquire systems and families of systems that are interoperable.

Paragraph E1.11.: States the requirement that test and evaluation shall assess interoperability.

Paragraph E1.16.: Cites interoperability as a primary reason for acquisition managers to consider and use performance-based strategies for acquiring and sustaining products and services.

DoD Instruction 5000.2, Operation of the Defense Acquisition System, Enclosure 5

Paragraph E5.1.4.9 states that "All DoD MDAPs, programs on the OSD T&E Oversight list, post-acquisition (legacy) systems, and all programs and systems that must interoperate, are subject to interoperability evaluations throughout their life cycles to validate their ability to support mission accomplishment. For IT systems, including NSS, with interoperability requirements, the Joint Interoperability Test Command (JITC) shall provide system interoperability test certification memoranda

to the Director, Joint Staff J-6, throughout the system life cycle and regardless of Acquisition Category."

Paragraph E5.1.5 states that "During Developmental Test and Evaluation (DT&E) the materiel developer shall:

E5.1.5.4. Assess technical progress and maturity against critical technical parameters, to include interoperability, documented in the TEMP.

E5.1.5.8. In the case of IT systems, including NSS, support the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and Joint Interoperability Certification (JIC) process."

CJCS Instruction 6212.01, Interoperability And Supportability Of Information Technology And National Security Systems provides implementing instructions and checklists to the DoD Directive 4630.5 and DoD Instruction 4630.8.

7.3.3. Interoperability and Supportability Integration into the Acquisition Life Cycle

Figure 7.3.3.1. is a chart from CJCS Instruction 6212.01 that depicts the relationship between key interoperability and supportability activities and the Joint Capabilities Integration and Development System and Defense Acquisition processes:

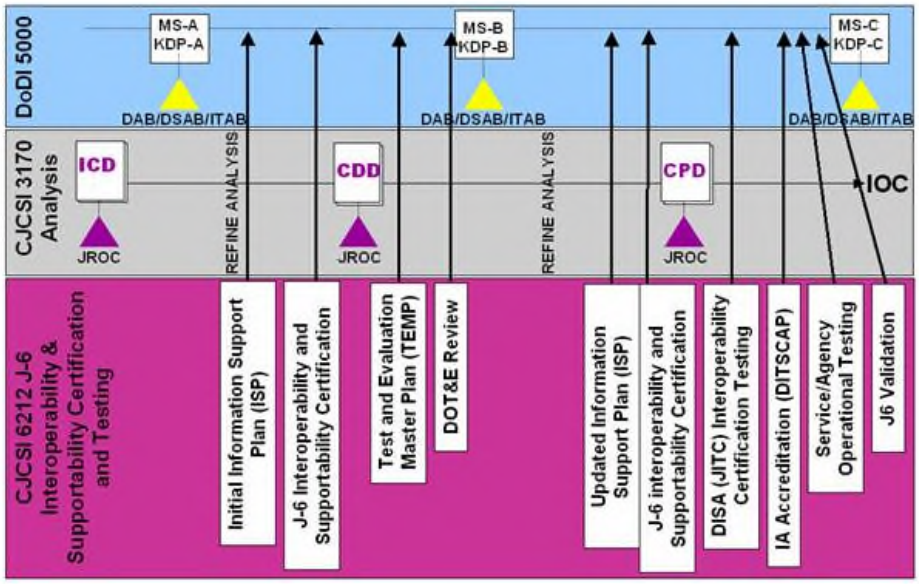

Figure7.3.3.1. J-6 Interoperability and Supportability Certification, Testing and Validation Process for ACAT Programs

7.3.4. Net-Ready Key Performance Parameter (NR-KPP)

The NR-KPP has been developed to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP, and incorporates net-centric concepts for achieving Information Technology (IT) and National Security Systems (NSS) interoperability and supportability. The NR-KPP assists Program Managers, the test community, and Milestone Decision Authorities in assessing and evaluating IT and NSS interoperability.

The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. Program managers will use the NR-KPP documented in Capability Development Documents and Capability Production Documents to analyze, identify, and describe IT and NSS interoperability needs in the Information Support Plan and in the test strategies in the Test and Evaluation Master Plan. The following elements comprise the NR-KPP:

- Compliance with the Net-Centric Operations and Warfare Reference Model.
- Compliance with applicable Global Information Grid Key Interface Profiles.
- Compliance with DoD Information Assurance requirements.
- Supporting integrated architecture products.

7.3.4.1. Compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM)

The NCOW RM, Figure7.3.4.1.1., describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (i.e., core services, Community of Interest services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the Global Information Grid are realized.

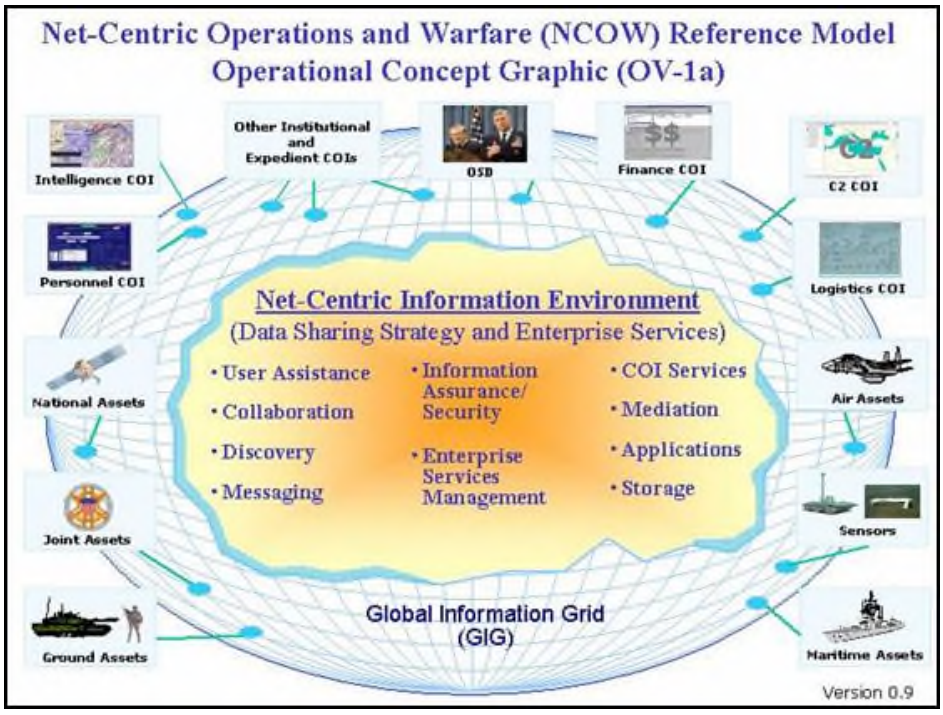

Figure7.3.4.1.1. Depiction of the Net-Centric Operations and Warfare Reference Model (NCOW RM)

Program manager compliance with the NCOW RM is demonstrated through inspection and analysis of a capability's:

Use of NCOW RM definitions and vocabulary;

Incorporation of NCOW RM Operational View capabilities and services in the materiel solution;

Incorporation of NCOW RM Technical View Information Technology and National Security Systems standards in the Technical View products developed for the materiel solution.

See section 7.2.6 for a description of how program managers show compliance with the NCOW RM. In addition, CJCS Instruction 3170.01 and CJCS Instruction 6212.01 for detailed discussions of the inspection and analysis processes.

7.3.4.2. Compliance with Applicable Global Information Grid (GIG) Key Interface Profiles (KIPs)

- ☑ Refined Operational View
- ☑ Refined System View
- ☑ Interface Control Specifications -- Interface Control Document (ICD)
- ☑ Technical View & SV-TV Bridge
- ☑ Configuration Management Plan
- ☑ Procedures for standards conformance and interoperability testing utilizing reference implementations
- ☑ Engineering Management Plan

	Communications KIPs
1.	Logical Networks to DISN Transport Backbone
2.	Space to Terrestrial Interface
3.	JTF to Coalition
4.	JTF Component to JTF Headquarters
5.	Teleport (i.e., deployed interface to DISN)
6.	Joint Interconnection Service
7.	DISN Service Delivery Node
8.	Secure Enclave Service Delivery Node (e.g., SCI/Collateral KIP)
	Connection KIPs
9.	Application Server to Database Server
10.	Client to Server
11.	Applications to COE/CCP (NCES/GES)
	Network Operations KIPs
12.	End System to PKI
13.	Management Systems to (integrated) Management Systems
14.	Management Systems to Managed Systems
15.	IDM to Distribution Infrastructure
16.	Information Servers to IDM Infrastructure
	Applications
17.	Application Server to Shared Data - IIOP (SADE)

Figure7.3.4.2.1. GIG Key Interface Profiles (KIPs)

GIG KIPs, Figure 30, provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces. A KIP is the set of documentation produced as a result of interface analysis which: designates an interface as key; analyzes it to understand its architectural, interoperability, test and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis. The profile consists of refined operational and systems view products, Interface Control Document/Specifications, Systems Engineering Plan, Configuration Management Plan, Technical Standards View (TV-1) with SV-TV Bridge, and procedures for standards conformance and interoperability testing. Relevant GIG KIPs, for a given capability, are documented in the Capability Development Document and Capability Production Document. Compliance with identified GIG KIPs are analyzed during the development of the Information Support Plan and Test and Evaluation Master Plan, and assessed during Defense Information Systems Agency (Joint Interoperability Test Command) joint interoperability certification testing. An interface is designated as a key interface when one or more the following criteria are met:

The interface spans organizational boundaries.

The interface is mission critical.

The interface is difficult or complex to manage.

There are capability, interoperability, or efficiency issues associated with the interface.

The interface impacts multiple acquisition programs.

Program manager compliance with applicable GIG KIPs is demonstrated through inspection of Joint Capabilities Integration and Development System documentation and test plans, and during Joint Interoperability Test Command interoperability certification testing (see CJCS Instruction 3170.01 and CJCS Instruction 6212.01 for detailed discussions of the process).

7.3.4.3. Compliance with DoD Information Assurance (IA) Requirements

Requirements for DoD information assurance certification and accreditation are specified in DoD Directive 8500.1, DoD Instruction 8500.2, DoD Directive 8580.1, and DoD Instruction 5200.40. Satisfaction of these requirements results in IA compliance verification of the capability with previously agreed to security requirements. See section 7.5 for details.

7.3.4.4. Supporting Integrated Architecture Products

Framework Product	Framework Product Name	General Description
AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
OV-2	Operational Node Connectivity Description	Operational nodes, operational activities performed at each node, connectivity and information exchange needlines between nodes
OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
OV-5	Operational Activity Model	Operational Activities, relationships among activities, inputs and outputs. Overlays can show cost, performing nodes, or other pertinent information.
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity sequence and timing - traces actions in a scenario or sequence of events and specifies timing of events
SV-4	Systems Functionality Description	Functions performed by systems and the information flow among system functions
SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to operational capabilities or of system functions back to operational activities
SV-6	Systems Data Exchange Matrix	Provides details of systems data being exchanged between systems
TV-1	Technical Standards Profile	Extraction of standards that apply to the given architecture

Table7.3.4.4.1. Architecture Products Required to Assess Information Exchange and Use

In accordance with the DoD 4630 Series, integrated architecture products defined in DoD Architecture Framework Version 1.0 (and described in Table 7 and Figure 31) shall be used to assess information exchange and use for a given capability. The functional

proponent, domain owner, PSA, and Program Manager use the supporting integrated architecture products in developing the Net-Ready Key Performance Parameter and preparing the Information Support Plan.

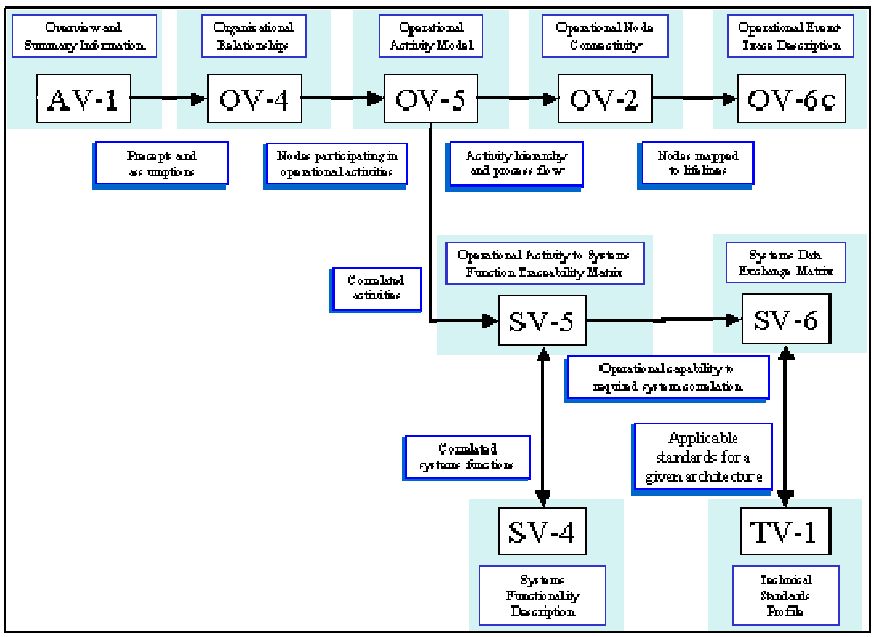

Figure7.3.4.4.1. Supporting Integrated Architecture Products

7.3.4.5. Compliance with Integrated Architecture Products

Program manager compliance with required supporting integrated architecture products is demonstrated through inspection and analysis of developed architecture products to determine conformance with DoD Architecture Framework specifications, and that all required products have been produced. Detailed procedures are contained in CJCS Instruction 3170.01 and CJCS Instruction 6212.01.

7.3.5. Net-Ready Key Performance Parameter (NR-KPP) Compliance Checklist

The following checklist summarizes the requirements for demonstrating compliance with the NR-KPP and should be useful in preparing for milestone approvals:

7.3.5.1. Required Documentation

Does the capability have the following required documentation?

AV-1, OV-2, OV-4, OV-5, OV-6c, SV-4, SV-5, SV-6

DISR Standards Compliance with draft TV-1

LISI Interconnectivity Profile

NR-KPP Compliance Statement

NCOW-RM Compliance

IA Compliance Statement

KIP Declaration List

7.3.5.2. Supporting Integrated Architecture Products

Have all architecture products been developed in accordance with the DoD Architecture Framework?

Does the AV-1 describe a net centric environment?

Has the TV-1 been prepared using applicable information technology standards profiles contained in the DISR?

Have all the interfaces listed in the OV-2 and SV-6 been appropriately labeled with the GIG core enterprise services needed to meet the requirements of the applicable capability integrated architecture?

Have all the applicable OV-5 activities identified in the specific capability integrated architecture been appropriately described at each critical or enterprise level interface in terms of policy enforcement controls and data enterprise sharing activities in the NCOW-RM, Node Tree OV-5?

Have specific capability integrated architecture OV-6c time event parameters been correlated with GIG architecture OV-6c?

Have verifiable performance measures and associated metrics been developed using the integrated architectures, in particular, the SV-6?

7.3.5.3. Key Interface Profiles

Have applicable Key Interface Profiles definitions been included as part of the KIP compliance declaration?

Are the information technology standards for each applicable KIP technical view included in the draft TV-1 for the specific Joint integrated architecture?

Are the appropriate KIP test procedures addressed as part of the requirement for interoperability system testing and certification?

7.3.5.4. Net-Centric Operations and Warfare Reference Model

Have the activities listed in the applicable capability integrated architecture OV-5 been mapped to the NCOW-RMnode tree OV-5 activities? Recommend that applicable capability integrated architecture OV-5 activities be characterized by use case diagrams grouped under the applicable GIG Core Enterprise Services (e.g., Discovery, Messaging, Mediation, Collaboration, etc.) to meet net-centric capabilities requirements for managing net-centric information environment.

Have NCOW-RM OV-5 activities been used to identify requirements for data correctness, data availability, and data processing necessary for posting data/information elements within a specific joint integrated architecture?

Has the SV-4 systems functionality been mapped to the applicable GIG Core Enterprise Services?

Are the information technology standards in the NCOW-RM Target Technical View included in the Draft TV-1 for the applicable capability integrated architecture?

7.3.5.5. Information Assurance

Have applicable information assurance requirements of DoD 8500 Series issuances and DCI Directives been identified for all GIG core enterprise services needed to meet the requirements of the specific joint integrated architecture?

Has the applicable capability received IA certification and accreditation documentation from the appropriate Designated Approval Authority?

7.3.6. Information Support Plan (ISP)

The ISP (formerly called the Command, Control, Communication, Computers, and Intelligence Support Plan (C4ISP)) is intended to explore the information-related needs of an acquisition program in support of the operational and functional capabilities the program either delivers or contributes to. The ISP provides a mechanism to identify and resolve implementation issues related to an acquisition program's Information Technology (IT), including National Security Systems (NSS), infrastructure support and IT and NSS interface requirements. It identifies IT needs, dependencies, and interfaces for programs in all acquisition categories, focusing attention on interoperability, supportability, synchronization, sufficiency and net-centricity concerns. This provides the program manager a mechanism to identify his/her information-related dependencies, to manage these dependencies and to influence the evolution of supporting systems to meet the demands of the system as it evolves to meet the warfighter's needs. In the case where the supporting system will not be available, the ISP should provide the program manager with awareness of this problem in sufficient time to adjust the program in the most cost effective and operationally efficient manner.

The C4ISP has evolved into the ISP as a result of the revision of the CJCS Instruction 3170.01 requirements documentation. The architecture documentation previously captured in the C4ISP is now required in the Joint Capabilities Integration and Development System documents: Initial Capabilities Document, Capability Development Document, and Capability Production Document. The ISP will use the architecture documentation from the Joint Capabilities Integration and Development System documentation and focus on analysis.

7.3.6.1. Review of Information Support Plan (ISP)-Specific Mandatory Policies

DoD Instruction 5000.2, Enclosure 3, Regulatory Information Requirements, Table E3.T2 requires that all acquisition programs (except Defense Space Acquisition Board-

governed programs as noted below), regardless of acquisition category level, submit an ISP at Milestones B and C, and at Program Initiation for ships.

National Security Space Acquisition Policy, Number 03-01, requires Defense Space Acquisition Board-governed programs to submit an ISP.

DoD Instruction 4630.8, Enclosure 4 provides a mandatory ISP format.

CJCS Instruction 6212.01 also provides detailed implementing guidance regarding the ISP format.

7.3.6.2. ISP Integration into the Acquisition Life cycle

A completed ISP answers the following seven questions for information needed to support the operational/functional capability(ies).

What information is needed?

How good must the information be?

How much information? (needed or provided)

How will the information be **obtained** (or provided)?

How quickly must it be received in order to be useful?

Is the information implementation **net-centric?**

Does it comply with DoD information policies?

The following paragraphs describe the ISP-related actions that program managers should take in each acquisition phase.

Before Milestone A

While the ISP is not required until Milestone B, early development of the ISP will assist in development of the program's integrated architecture and Concept for Operations required by the CJCS Instruction 3170.01.

Before Milestone B (or program initiation for ships)

Define all information related-dependencies according to DoD Instruction 4630.8, CJCS Instruction 6212.01, CJCS Instruction 3170.01, and CJCS Manual 3170.01 to ensure information supportability is addressed in the ISP and Capabilities Development Document

Submit the ISP for formal, coordinated Stage I and Stage II reviews according to DoD Instruction 4630.8and CJCS Instruction 6212.01. Submit a final, Stage III, version of the ISP for retention in the OASD(NII) Joint C4I Program Assessment Tool (JCPAT) repository. Click here for ISP examples/samples web sites.

Before Milestone C

Update all information related-dependencies according to DoD Instruction 4630.8, CJCS Instruction 6212.01, CJCS Instruction 3170.01, and CJCS Manual 3170.01to ensure information supportability is addressed in the ISP and Capabilities Production Document.

Submit the updated ISP for formal coordinated Stage I and Stage II reviews according to DoD Instruction 4630.8 and CJCS Instruction 6212.01. Submit a final, Stage III version of the ISP for retention in the OASD(NII) Joint C4I Program Assessment Tool (JCPAT) repository. Click here for ISP examples/samples web sites.

After Milestone C

Submit an updated ISP for each major upgrade (e.g., block or increment)

7.3.6.3. Estimated Preparation Lead Time

Based on past experience with C4ISPs, for a small program with few interfaces, it takes about 6 months to get an ISP ready for a Stage I review. For most programs, ISP preparation for Stage 1 review takes about a year. For very complex programs, like a major combatant ship, it can take between 18 to 24 months. The process is based on development or existence of an architecture.

7.3.6.4. OSD Review

The Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD (NII)) reviews all ISP documents for Acquisition Category I and IA programs, and for other programs in which OASD(NII) has indicated a special interest.

This review is performed on the C4ISP Assessment Tool in the Joint C4I Program Assessment Tool (JCPAT) suite. The JCPAT suite provides paperless, web-based support for ISP document submission, assessor review and comment submission, collaborative workspace, and consolidated review comment rollup.

The DISA JCPAT functional analyst is available to assist users with JCPAT functionality and to establish user accounts. A repository of previous C4ISP and current ISP documents is available for viewing in the JCPAT document repository.

7.3.6.5. Example/Sample Web Links

Program managers and other stakeholders will find the links in Table 8 useful in ISP preparation, program analysis, and oversight.

Web Site	NIPRNET	SIPRNET
DSC's C4ISPlan	http://www.dsc.osd.mil	www.dsc.osd.smil.mil/index.html
DISA's JCPAT	http://jcpat.ncr.disa.mil	jcpat.ncr.disa.smil.mil
NII's JMAAT	Not applicable	147.254.161.70/pai/index.htm
Defense Architecture Repository	https://pais.osd.mil/enterprisearchitectures	Not applicable

Table7.3.6.5.1. Example/Sample Web Links

7.3.6.6. Points of Contacts

Useful points of contact appear in Table 7.3.6.6.1.

Mission Areas	Phone
Land, Space	703-607-0246
Air, PGMs	703-607-0510
Maritime, Missile Defense	703-607-0506
C2,Pay, Personnel, Medical, Logistics	703-602-2716 x153
Intell	703-607-5240
JCPAT Functional Analyst	703-681-2592

Table7.3.6.6.1. Useful Points of Contact

7.3.6.7. Information Support Plan (ISP) Chapter Instructions (13-Step Process for ISP Chapter 2)

The following provides instruction on how to complete each chapter and appendix in the ISP. It contains additional, discretionary guidance beyond that contained in DoD Instruction 4630.8 and CJCS Instruction 6212.01.

ISP Chapter 1. Introduction

Summarize the program's operational scope.

Summarize the program's relationships to relevant Joint Operating Concepts (JOCs) and/or Joint Functional Concepts (JFC) (e.g., focused logistics), as described in the program's Joint Capabilities Integration and Development System documents. Provide an OV-1 (High-Level Operational Concept Graphic) for the basic program and descriptive text. For programs not covered by Joint Capabilities Integration and Development System (JCIDS), analogous documentation may be used.

Summarize the program's relationship to other programs.

Provide a graphic that shows the major elements/subsystems that make up the system being acquired, and how they fit together (Provide an Internal SV-1 (System Interface Description)/(e.g., a system block diagram)).

Analyze threat-specific information that will play a role in capability development, design, testing and operation. This information should be obtained from the appropriate (JCIDS) documents. Information Operations (IO) threats should be analyzed using the Information Operations Capstone Threat Capabilities Assessment, DI-1577-12-03, August 2003. This is the most comprehensive source available for IO-related threat information.

For a weapon system, briefly describe the purpose, design objectives, warhead characteristics, sensors, guidance and control concept (as appropriate), command and control environment, general performance envelope, and primary Information Technology (IT), including National Security Systems (NSS) interfaces.

For a command and control system, describe the system's function, dependencies and interfaces with other IT and NSS systems.

For an Automated Information System (AIS), describe the system's function, its mission criticality/essentiality, dependencies, interfaces with other IT and NSS systems and primary databases supported.

Program Data.

Provide the following program:

Program contact information (program manager, address, telephone, email address, and ISP point of contact).

Program acquisition category: Acquisition Category.

List Milestone Decision Authority: Defense Acquisition Board, Defense Space Acquisition Board, Information Technology Acquisition Board (or component Milestone Decision Authority) or other.

Milestone covered by the specific ISP.

Projected milestone date.

ISP Chapter 2. Analysis

Analysis of the qualitative and quantitative sufficiency of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) support (e.g., hardware, software, processes, etc.) should be accomplished in terms of the operational/functional capabilities that are being enabled.

This analysis requires the following:

An understanding of the operational/functional capabilities and the metrics that define whether they are being performed adequately.

An understanding of what enabling functional capabilities must be performed in order to achieve a higher-level capability (C4ISR functions will almost always be enabling capabilities).

An understanding of which players (nodes) will direct or perform the missions associated with delivering the capabilities.

An understanding of DoD Information Policies.

The information-needs discovery process:

For most systems, the following steps provide an information-needs discovery process that can be used to analyze the system under development. However, other approaches for discovering information needs that apply to the intelligence information needs discovery process are:

Using the stages of the intelligence cycle (collection, exploitation, dissemination, etc.).

Life-cycle stages (Concept Refinement, Technology Development, System Development and Demonstration, etc.).

The following steps (and notes) are based on using the Integrated Architecture developed in accordance with the DoD Architectural Framework, during the JCIDS process. Click here for Global Information Grid (GIG) details.
(http://akss.dau.mil/dag/Guidebook/IG_c7.3.6.7.asp)

Step 1: Identify the warfighting missions and/or business functions within the enterprise business domains that will be accomplished/enabled by the system being procured.

Note: Joint Warfighting missions can be found in Joint Publication 3.0. Click here for Operation, Series 3-0 publications.

Note: AIS programs should consult the DoD Comptroller's Business Management Modernization Program enterprise integrated architectures for each domain. Click here for BMMP details.

Step 2: Identify information needed to enable operational/functional capabilities for each warfighting mission identified in Step 1 by performing functional capability decomposition.

Note: If a Command and Control capability is the top-level driver of the function breakdown, then the OV-4 (Command Relationships) will be a necessary product to help define the functional capabilities needed. The OV-4 will likely require several OV-5 (Activity Model) functional breakdowns to enable each of the command elements identified.

Note: The architecture product most useful in managing the discovery of enabling/enabled capability relationships for each operational/functional capability is the OV-5 (Operational Activity Model). The OV-5 can be used to show the subordinate capabilities that are necessary to achieve a higher-level operational or functional capability. Notice that the OV-5 focuses on "what" rather than "how." See Example Capability Breakdown, Figure 32.

This example illustrates specific items to consider for a weapon system that can be used to get the flavor of what is expected in step 2 for a program/system.

Step 2 Example: Clear Mines from Littoral Area

A. Clear mines from littoral area *(Operational Capability)*

Note: *Quality measures must be assigned in order to assess the acceptability of the operational and enabling capabilities/systems*

1. Plan the clearance effort (1st level enabling capability)
    - a. Obtain necessary intelligence information *(2nd level enabling capability)*
        - 1) Navigation Information (charts, tides and currents, etc)
        - 2) Enemy maritime mining capability *(3rd level capabilities)*
        - 3) Weather information
        - 4) Enemy coastal defense capability
    - b. Collaborate with off board nodes (2ndt level enabling capability)
    - *Insert 3rd and succeeding levels of enabling capability*
2. Search for/locate the mines
    - *Insert 2nd and succeeding levels of supporting capability*
3. Disable/remove/destroy the mine
    - *Insert 2nd and succeeding levels of supporting capability*
4. Share the results of the clearance effort
    - *Insert 2nd and succeeding levels of supporting capability*
5. Receive logistic support.
    - *Insert 2nd and succeeding levels of supporting capability*

Figure 7.3.6.7.1. Example Capability Breakdown

Note: The specific form of this information should capture key information from an OV-5 (Operational Activity Model) and/or other information source (e.g., an outline or hierarchical graph). The important point is that the capability relationships are understood and attributes are identified so that assessments can be made.

Note: Specific items to consider:

For satellite systems include: (e.g. Satellite control)

For communication systems include: (e.g. Net-management)

For business process systems include: (e.g. information contained in databases, other information sources)

For weapons systems include: (e.g. Collection Management Support, Threat or signature support, targeting support, Intelligence Preparation of the Battlefield)

For sensor systems include: (e.g. Collection Management support, Threat or Signature support, Targeting support, Intelligence Preparation of the Battlefield, and Remote Operations)

For platforms consisting of a mix of the above include: (e.g., Collection Management support, Threat or Signature support, Targeting support, Intelligence Preparation of the Battlefield

Step 3: Determine the operational users and notional suppliers of the information needed.

Step 3.a: Provide an OV-2 to identify the operational nodes and elements that drive the communications needed to enable the functional capabilities. For large platforms/systems, this effort should identify the major operational nodes (information drivers) within the platform, as well as nodes that are external to the platform/system with which information will be shared.

Step 3a Example: Clear Mines from Littoral Area

Search Platform (Major Node)

Activities

Information needed to support each activity

Supporting person(s) operating sensors (Internal Node)

Activities

Information needed to support each activity

Person directing search effort (Internal and or External Node)

Activities

Information needed to support each activity

Supporting person(s) involved in coordinating logistics (Internal and /or External Node)

Activities

Information needed to support each activity

Supporting person(s) involved in personnel administration (Internal Node)

Activities

Information needed to support each activity

Intelligence Sources (Major Node)

Activities

Information needed to support each activity

Supporting person(s)/organizations involved in mine neutralization (Major Node)

Activities

Information needed to support each activity

-
-
-

Figure 7.3.6.7.2. Example OV-2 Nodes For Mine Clearance

Step 3.b: Map these nodes (internal and external systems and people) and their activities to the functions identified in OV-5

Step 4: Establish the quality of the data needed to enable the functions identified in OV-5 and performed by the operational nodes in OV-2 (Operational Node Connectivity)

Note: Establish performance measures and determine the level of satisfaction necessary to make the information useful. (Examples: decimal precision for numerical data, NIIRS for imagery, annotated versus raw data, etc)

Note: When radio and other information transport systems are identified as providing support, establish transmission quality parameters and then assess whether the programs/systems intended to be used can meet these criteria.

Note: A factor in determining quality is the user (person or sub-system) (i.e. specifically how does the user intend to use the information).

Step 5: Determine if timeliness criteria exist for the information.

Note: To help establish timeliness, use OV-6C (Operational Event Trace Diagram) to establish event sequence. Considerations include:

Order of arrival of information to enable transaction process(es) (for weapon systems) Latency of data due to speed of flight issues

Currency of data in databases to support operations

Step 6: Determine/Estimate the quantity of information of each type that is needed.

Factors influencing quantity include:

Frequency of request or transmittal.

Size of the information requested. (packet size, image size, file size etc.)

Whether data is individual items or a data stream that is provided for a period of time.

Whether data transmission is “bursty” or continuous over some period of time.

Whether data transmission is random or occurs at some predictable interval

The anticipate spectrum of employment (e.g. Military Operations Other than War or Major Theater of War)

Note: Ultimately this analysis should help estimate the bandwidth needs and should provide an assessment as to whether adequate bandwidth is available. If bandwidth is limited, what actions can be taken to reduce demand or use the bandwidth more efficiently?

Step 7: Discuss the way information will be accessed or discovered.

If data links are involved, identify them and also the message sets that will be implemented.

If a web-based (Global Information Grid (GIG) compliant) means of searching for and retrieving posted data is to be used, describe the approach.

Data stores must exist for your program.

The type of searching capability needed

Note: In many cases, this discussion will involve multiple levels of enabling systems. For example, maybe the enabling system is a Global Command and Control System (GCCS) application. GCCS rides on the SIPRNET. So both levels of this support should be discussed.

Step 8. Assess the ability of supporting systems to supply the necessary information.

Note: Supporting systems include collection platforms, databases, real time reports, messages, networked data repositories, annotated imagery, etc.

Assess the ability to collect, store, and tag (to enable discovery and retrieval) the information

Assess the ability of networks to provide a means to find and retrieve the necessary data.

Assess the ability of the information transport systems to move the volume of data needed.

Assess synchronization in time (i.e., years relative to other system milestones) with supporting programs.

Whether the information will cross security domains.

Note: If systems will in any way tie into the intel Top Secret (TS)/ Sensitive Compartmented Information (SCI) network (JWICS) or utilize TS/SCI info, they will have to comply with Director, Central Intelligence Directives (DCID): DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, June 1999 and DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities, 18 November 2002.

Note: The number of levels of analysis will depend on the detail required to identify the critical characteristics of the information needed to support the program. This should be accomplished for all phases of the acquisition life cycle.

Note: It is anticipated that the other communities such as the intelligence community may have to assist in the determination and analysis of these information needs.

Note: The format in Figure 34 is suggested for capturing the results of the supportability/synchronization assessment:

Step 8 Example: Summary of Synchronization Data

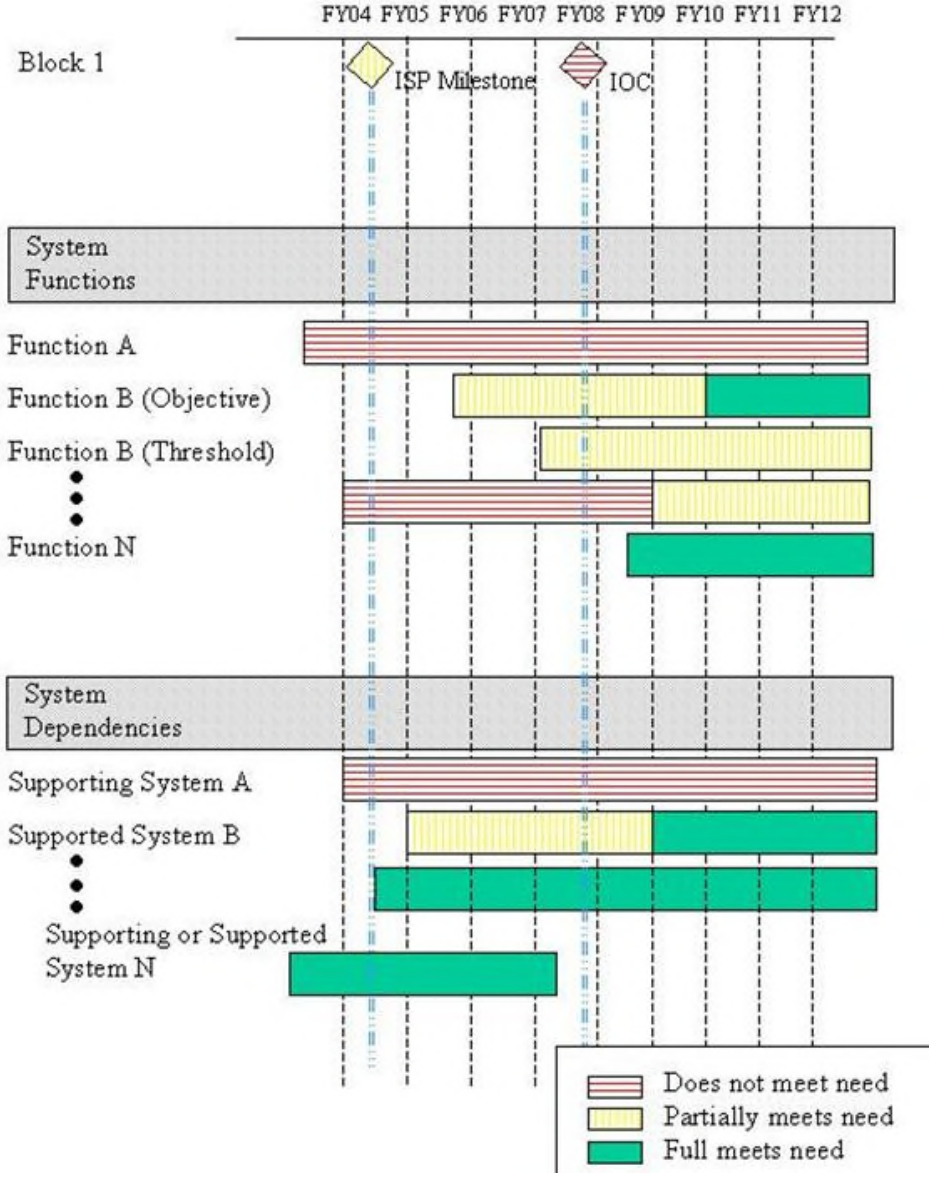

Figure 7.3.6.7.3. Sample Dependency and Information Needs Analysis Summary

Step 9: Assess Radio Frequency (RF) Spectrum needs. Click here for Spectrum details.

Note: DoD Directive 4650.1 establishes spectrum management policy within the Department of Defense. (DoD Instruction 4630.8 and CJCS Instruction 6212.01 require

Spectrum Supportability (e.g., spectrum certification, reasonable assurance of the availability of operational frequencies, and consideration of E3) to be addressed in the ISP. The Services have additional spectrum management policies and procedures.

To support the Spectrum Supportability process, the ISP should document the following:

Requirements for use of the electromagnetic spectrum including requirements for wide bandwidths

Description of the intended operational Electromagnetic Environment (Allows for realistic test and evaluation).

Impact of the loss of a planned spectrum-dependent command, control, or communication link as a result of an unresolved spectrum supportability issue. (To be identified in the issue section of the ISP)

Note: For platforms that employ Radio Frequency (RF) emitters developed by a separate acquisition program, spectrum documentation for those emitters may be cited here as evidence of compliance with Spectrum Supportability regulations.

Step 10. Assess Net-Centricity.

Note: Consider individual Services net-centric policies and procedures that supplement DoD Net-centric policy.

Note: This is an emerging requirement in the analysis required for ISPs. When Net-Centric Enterprise Services (NCES)/Core Enterprise Services (CES) is available, programs will be expected to conduct this as a detailed analysis. Programs should be aware of this developing requirement, as it will become an essential part of determining net-centricity and compliance with the Global Information Grid (GIG).

Step 10a: Using the information provided as a result of Step 7, the program manager should evaluate the program against measurement criteria from the most recent version of the NCOW Reference Model, OV-5. The program manager should identify differences with the reference model as potential issues.

Step 10b: Provide an analysis of compliance with the emerging Net-Centric Enterprise Services (NCES)/Core Enterprise Services (CES).

As the GIG ES develops, its specifications should be cross-walked with the ISP system's planned network service specifications. Identify the issues associated between the CES service specifications and those of the system that is the subject of the ISP. Compliance would mean that the system would connect seamlessly with the defined DoD-level enterprise services.

- *Step 10c:* Assess use of the following:
- Software Compliant Radios (Joint Tactical Radio System). Click here for Software Communications Architecture (SCA) model and policy.
- Internet Protocol Version 6.0 (IPv6).
- DoD Net-Centric Data Management Strategy..
- Global Information Grid (GIG) Bandwidth Expansion relationships.

- Net-centric Enterprise Service (NCES) linkages.

The Net Centric Operations and Warfare Reference Model (NCOW-RM) provides a top-level view of the functions.

Step 10c Example: NCOW-RM, OV-5 (See section 7.2.6 for NCOW-RM explanation and details).

Step 11: Discuss the program's inconsistencies with the DoD Global Information Grid (GIG) Architectures and the program's strategy for getting into alignment.

Identify areas where the latest version of the DoD GIG Architectures does not support information needs. Click here for GIG details.

Step 12: Discuss the program's Information Assurance (IA) strategy.
Reference the Program Protection Plan in this section.

Assess compliance with the DoD Information Assurance end-to-end strategy.

Step 13: Identify information support needs to enable development, testing, and training.

For development phase: Weapon systems include information about potential targets that are necessary to support system development. (Example: target signature data)

For testing: Include information support needs critical to testing (Example: Joint Distributed Engineering Plant (JDEP). Do not duplicate Test and Evaluation Master Plan (TEMP) information except as needed to clarify the analysis. In addition, for information on software safety testing, please refer to section 9.3.1.

For training: Include trainers and simulators that are not a part of the program being developed. Include:

Training facilities that are funded separately that your program intends to use for training support.

Network support that will be needed to meet the training needs of your program.

ISP Chapter 3. Issues.

Present issues as defined in DoD Instruction 4630.8 in a table such as Table 10, or in an outline containing the same data.

Group Operational Issues under the mission impacted, then under the impacted functional capability (for that mission).

When issues involve more than one mission, subsequent missions should be marked with the previous issue number and those fields that remain the same should be marked as such.

Include the following column (or outline) headings:

- Issue Number
- Supporting System
- Issue
- Issue Description

- Source Integrated Architectures (e.g., Command and Control (C2), Focused Logistics, Force Protection, Force Application, Battlespace Awareness, Space, etc.)
- Issue Impact
- Mitigation Strategy or Resolution Path).

Number each issue as "C-#" for critical shortfalls and "S-#" for substantive issue. Click here for DoD Global Information Grid Architectures details.

Issues shall include resolution paths (according to DoD Instruction 4630.8, paragraph E4.4.4) with projected dates to be corrected. If resolution details are not known, a discussion on the approach (including anticipated responsible parties) should be provided.

Operational Issues					
Mission					
Functional Capabilities impacted					
Issue number	Supporting system	Source Architecture	Issue Description	Issue Impact	Mitigation Strategy/Resolution Path (and Time-Frame)
Development Issues					
Testing Issues					
Training Issues					

Table 7.3.6.7.1. Sample Issue Table Format

ISP Appendices

Appendix A. References. Include all references used in developing the ISP. Include Architectures; other relevant program documentation; relevant DoD, Joint Staff and Service Directives, Instructions and Memos; ISPs or ISPs from other programs, any applicable Joint Capabilities Integration and Development System documentation and others as deemed necessary.

Appendix B. Systems Data Exchange Matrix (SV-6).

Appendix C. Interface Control Agreements: Identify documentation that indicates agreements made (and those required) between the subject program and those programs necessary for information support. For example, if System A is relying on information from System B, then this interface dependency must be documented. At a minimum, this dependency should be identified in the ISPs for both System A (the information recipient) and System B (the information provider).

Appendix D. Acronym List: Provide an Integrated Dictionary (AV-2).

Other Appendices. Provide supporting information, as required, not included in the body of the ISP or relevant Joint Capabilities Integration and Development System (Joint Capabilities Integration and Development System) documents. Additional, or more detailed information, used to satisfy DoD Component-specific requirements, should be included as an appendix, and not incorporated in the body of the subject ISP. Additional architecture views used in the ISP analysis will be provided in a separate appendix and referenced in the main body of the ISP.

7.4. Net-Centric Data Strategy

7.4.1. Implementing the DoD Net-Centric Data Strategy

The DoD Net-Centric Data Strategy (May 2003) outlines the vision for managing data in a net-centric environment. Net-centricity compels a shift to a "many-to-many" exchange of data, enabling many users and applications to leverage the same data-extending beyond the previous focus on standardized, predefined, point-to-point interfaces. Hence, the net-centric data objectives are to ensure that all data are visible, available, and usable-when needed and where needed-to accelerate decision cycles. Specifically, the data strategy describes 7 major net-centric data goals as presented in Table 11 below:

Goal	Description
Goals to increase Enterprise and community data over private user and system data	
Visible	Users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets (intelligence, nonintelligence, raw, and processed) are advertised or "made visible" by providing metadata, which describes the asset.
Accessible	Users and applications post data to a "shared space." Posting data implies that (1) descriptive information about the asset (metadata) has been provided to a catalog that is visible to the Enterprise and (2) the data is stored such that users and applications in the Enterprise can access it. Data assets are made available to any user or application except when limited by policy, regulation, or security.
Institutionalize	Data approaches are incorporated into Department processes and practices. The benefits of Enterprise and community data are recognized throughout the Department.
Goals to increase use of Enterprise and community data	
Understandable	Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs.
Trusted	Users and applications can determine and assess the authority of the source because the pedigree, security level, and access control level of each data asset is known and available.
Interoperable	Many-to-many exchanges of data occur between systems, through interfaces that are sometimes predefined or sometimes unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed.
Responsive to User Needs	Perspectives of users, whether data consumers or data producers, are incorporated into data approaches via continual feedback to ensure satisfaction.

Table7.4.1. Net-Centric Data Strategy Goals

The Strategic Planning Guidance FY2006-FY2011 (March 2004) informs DoD Components that, "all efforts to improve information-sharing capabilities will comply with the Net-Centric Data Strategy, the GIG Architecture, and the Net-Centric Operations and Warfare Reference Model." Activities required to enable the Net-Centric Data Strategy have been incorporated into the Net-Centric Operations and Warfare Reference Model. These activities serve to guide architects and program managers in implementing the activities and sub-activities that will establish a net-centric data foundation for their

program. Detailed implementation guidance in the form of Implementation Manuals and Handbooks are under development. The activities are summarized below.

7.4.2. Data Strategy Activities

Data Strategy activities are separated into four key areas: Data Planning, Manage Data Infrastructure, Provide Enterprise Data Assets and Govern Data Activities. These activities can be conducted across the span of milestones; however, the general groupings of these activities will for the most part dictate the phase in which they are conducted.

7.4.2.1. Activity Area 1, "Data Planning"

This activity area describes activities that result in data plans, standards, specifications, guidance, and policy.

7.4.2.2. Activity Area 2, "Manage Data Infrastructure"

This activity area describes activities that pertain to the establishment and management of components that were planned for in the Data Planning Activity Area. In these activities, software/hardware solutions are identified, established, and operated and maintained. Additionally, the infrastructure activities include the development of metadata products that support data sharing within a program, system, or enterprise.

7.4.2.3. Activity Area 3," Provide Enterprise Data Assets"

This activity area describes activities that ensure that data assets can be discovered and accessed in the net-centric environment. This includes providing semantic and/or structural metadata and ensuring that data assets are visible by enterprise search capabilities and that the data asset is physically accessible through common methods employed on the GIG (such as through web-based technologies).

7.4.2.4. Activity Area 4, "Govern Data Activities"

This activity area describes activities that track compliance to policy and guidance and participation in oversight processes. Additionally, this activity area includes advocating the data strategy to stakeholders.

7.4.3 Integration into the Acquisition Life-Cycle

7.4.3.1 Before Milestone A-Data Planning Activities

- ***Define Net-Centric Data Sharing Plan*** *:*

The activity relates to the development of a comprehensive net-centric plan to share data assets within your program/ organization and to the Enterprise. This includes metadata catalog plans, registry plans, interoperability plans, etc. In essence, this Net-Centric Data Sharing Plan should be the program's/organization's plan to accomplish the goals of the DoD Net-Centric Data Strategy. This is a key product and will drive most data activities and architectures.

Responsibilities: **Sponsor/Domain Owners** should develop these plans at a broad, strategic level to ensure that architectures for programs and sub-organizations associated with the Domain include net-centric data components. Depending on the scale of the Program or system, **Program Managers** should develop a more detailed data sharing plan that outlines how their information architecture(s) make their data and processes discoverable, accessible, and understandable to both known and unanticipated users. These Program data sharing plans should ensure that they align with and make use of enterprise net-centric data sharing capabilities such as those envisioned/planned under the Net-Centric Enterprise Services and Business Modernization Management Programs.

- ***Define Data Guidance :***

Evaluate information from sources such as compliance reports, incentive plan reports, policy, and user needs to create net-centric data guidance documents. Data guidance is the policy, specifications, standards, etc, used to drive data activities within the program/organization. It differs from a net-centric data plan in that the plan is more strategic in nature. Data guidance may be a subset of an overall net-centric data sharing plan.

Responsibilities: **Sponsor/Domain Owners** should develop appropriate issuance and standards to ensure that incentives, metrics, and direction are in place to drive the transition to net-centricity. Sponsor/Domain Owners should establish policy and governance to ensure that the Domain's Programs and sub-organizations have a voice in the development of standards, specifications, and processes (e.g. empowering a Program to insert its metadata requirements into an overall Domain metadata model).

- ***Define Net-Centric Data Architectures :***

Build upon existing and revised architectures and plans to describe the architecture to support data sharing objectives. The architecture should depict components that emphasize the use of discovery, services-based approach to systems engineering, use of metadata to support mediated information exchange, web-based access to data assets, etc.

Responsibilities: Both **Sponsor/Domain Owners and Program Managers** should include net-centric concepts, activities, and processes into their architectures. **Sponsor/Domain Owners** should ensure that their Domain-level architectures are developed in a manner that is appropriate for governing under a capabilities-based portfolio management process. **Program Managers** should ensure that net-centric components are integrated into their program architecture products.

7.4.3.2. Before Milestone B--Data Planning

- ***Identify Data Assets:***

Determine what data assets (documents, images, metadata, services, etc) are produced or controlled within a program or organization. This is primarily an inventory of data assets, which should include both structured and unstructured data sources.

Responsibilities: **Sponsor/Domain Owners** should identify major data assets created or managed within their Domain. This asset listing will assist in the development of visibility, accessibility, and understandability strategic plans (i.e. based on the composition of the major data assets within the Domain, the planning products can reflect

the most appropriate approach in supporting net-centric data strategy goals). Likewise, **Program Managers** should inventory the data assets created or managed by the program and use this asset listing to plan their strategy and implementation approach for making these assets net-centric.

- ***Prioritize Data Assets:***

Assess the data asset inventory to identify key data products that are of greatest value to known users and are likely to be of value to unanticipated users. This list should be used to determine data assets a program/organization should make initial efforts at exposing as enterprise data assets.

Responsibilities: **Both Sponsor/Domain Owners and Program Managers** should analyze and prioritize which data assets are most valuable, initially, to be exposed as enterprise data assets.

- ***Define Communities of Interest (COIs):***

Identify appropriate groups of people who should come together to support common mission objectives. COIs are an appropriate construct for defining information exchange formats and metadata definitions as well as vocabularies used to communicate within the COI. This activity does not include the 'establishment' of actual COIs. This is simply the process of identifying COIs that exist or should exist.

Responsibilities: **Sponsor/Domain Owners** should define major COIs that could benefit missions within the Domain (and across Domains). **Program Managers** should identify other COIs that serve the goals of the program and its associated functional areas.

7.4.3.3. Before Milestone C--Manage Data Infrastructure [Determine Infrastructure Requirements]

- ***Manage Discovery Metadata Catalog(s):***

Identifying/establishing and maintaining searchable catalogs used to locate data assets within the program, organization, or enterprise. Metadata stored within these catalogs facilitates discovery and includes descriptive information about each shared data asset.

Responsibilities: **Sponsor/Domain Owners** should establish Domain-level metadata catalogs that allow for the search of data assets across the Domain. Distributed, federated approaches should be used in developing this capability. **Program Managers** should ensure that their data is tagged and posted to metadata catalogs that are tied into the Domain metadata catalog.

- ***Manage Metadata Registry(s):***

Identifying and/or establishing metadata registries that can be used to maintain, manage, and/or search for metadata artifacts such as schema and data definitions. Metadata stored in metadata registries are typically for developers, business analysts, and architects. Metadata registries are a type of metadata catalog specifically designed to support developers/business analysts.

Responsibilities: **Sponsor/Domain Owners** should ensure that metadata products within their Domain (including associated programs and sub-organizations) are registered into

the DoD Metadata Registry. Domain Communities of Interest (COIs) are likely to be structured around the functional areas for which metadata is registered. **Program Managers** should ensure that program metadata is registered in the DoD Metadata Registry and is maintained.

- ***Manage Service Directory(s):***

Identifying and/or establishing service directory(s) that can be used to maintain, manage, and/or search for callable, reusable services from which net-centric capabilities are built. Metadata stored in service directories gives information as to the services available, how to call them, and possibly, expected service levels. Service directories include UDDI Directories used to maintain Web Services information. This is a key component of establishing a service oriented architecture that supports net-centric data tenets.

Responsibilities: **Sponsor/Domain Owners** should ensure that services created or managed within their Domain (including associated programs and sub-organizations) are registered into the DoD Services Registry (TBD as first increment of NCES Discovery). **Program Managers** should ensure that program services are registered in the DoD Services Registry.

- ***Manage Interoperability Components:***

Development of metadata artifacts used to enable the interchange of data and information including document vocabularies, taxonomies, common data models, schema, formats, mediation components, and interface specifications.

Responsibilities: **Sponsor/Domain Owners** should establish Domain-level metadata models to facilitate the loosely-coupled exchange of information between systems. **Program Managers** should develop metadata models (e.g. data structures, schema, etc) pertinent to their program. This includes tagging models, service schema, and mapping models to the Domain metadata model.

- ***Develop/Acquire Data Access Mechanism(s):***

Post data assets to an information sharing application (e.g., end-user web site, a file system, a document repository) or through the use of web services to provide system-to-system access, etc.

Responsibilities: **Sponsor/Domain Owners** should establish shared space, as necessary, to support Program's within its scope. **Program Managers** should ensure that web-enabled services provide access to valuable systems data and processes.

- ***Manage Communities of Interest:***

This activity encompasses establishing Communities of Interest (COI(s)), registering COI(s) in the Enterprise COI Directory and Community of Interest participation. The outcomes of this activity will ensure that COI(s) can be located and managed throughout the enterprise.

Responsibilities: **Both Sponsor/Domain Owners and Program Managers** should establish, register, and maintain identified COIs.

7.4.3.4. Before Full Rate Deployment Decision--Provide Enterprise Data Assets

- ***Provide Discovery Metadata:***

Associate or generate discovery metadata for data assets. This activity is the 'tagging' of data assets to provide value-added information about data assets that can be used to support discovery, accessibility, IA, and understandability.

Responsibilities: **Program Managers** should ensure that discovery metadata is provided for all data assets created/managed by the Program.

- ***Post Discovery Metadata:***

Providing, or posting, discovery metadata to catalogs, registries, etc, that can be searched. It is through 'posting metadata' that metadata catalogs are populated. This activity allows data assets to be discovered (but does not guarantee access to the data asset).

Responsibilities: **Program Managers** should ensure that discovery metadata associated with each data asset is posted to searchable metadata catalogs (established by the Domain and by Programs).

7.4.3.5. Cross Milestone Activities--Govern Data Activities

- ***Participate in GIG Governance:***

Participate in governance activities that enable net-centric data asset sharing. This includes participation in GIG Enterprise Service efforts, net-centric architectural compliance, IT Portfolio Management for net-centricity, etc.

Responsibilities: **Sponsor/Domain Owners** should participate in GIG governance activities to ensure the proper processes are followed and executed within their Domain to enable the net-centric Domain environment.

- ***Enforce Data Guidance:***

Participate in enforcement/compliance activities that assess net-centric architectures against Net-Centric Data Guidance that was developed in the Data Planning process.

Responsibilities: **Both Sponsor/Domain Owners and Program Managers** should enforce established data guidance (including conformance to standards and adherence to DoD/Domain issuances).

- ***Advocate Data Strategy(s):***

This activity involves vetting, publicizing, and institutionalizing the Net-Centric Data Sharing plans and guidance developed in the Data Planning process.

Responsibilities: **Both Sponsor/Domain Owners and Program Managers** should advocate the DoD Net-Centric Data Strategy and Domain-established data guidance.

7.4.4. Supporting Language for IT System Procurements

To ensure support of the goals of DoD Net-Centric Data Strategy, the program manager, through his or her contracting specialists, should include the following sections, as

appropriate, in Request for Proposal/Request for Quotation language for the procurement of IT systems.

- The contractor shall ensure that any IT systems covered in this procurement or identified in this RFP/RFQ support the goals of the DoD Net-Centric Data Strategy dated May 9, 2003.
- Also, the contractor must ensure that any IT systems covered in this procurement or identified in this RFP/RFQ meet the requirements detailed below. Additionally, it is acceptable for vendors and/or integrators to provide functionality (via wrappers, interfaces, extensions) that tailor the COTS system to enable these requirements below (i.e. the COTS system need not be modified internally if the vendor/integrator enables the requirements through external or additional mechanisms. In this case, these mechanisms must be acquired along with the COTS system procurement).
    - ***Access to Data*** : The contractor shall ensure that all data managed by the IT system can be made accessible to the widest possible audience of Global Information Grid (GIG) users via open, web-based standards. Additionally, the system's data should be accessible to GIG users without 1) the need for proprietary client-side software/hardware, or 2) the need for licensed user-access (e.g. non-licensed users should be able to access the system's data independent to the licensing model of the COTS system). This includes all data that is used to perform mission-related analysis and processing including structured and unstructured sources of data such as databases, reports, and documents. It is not required that internal, maintenance data structures be accessible.
    - ***Metadata*** : The contractor shall ensure that all significant business data made accessible by the IT system is tagged with descriptive metadata to support the net-centric goal of data visibility. Accordingly, the system data shall be tagged to comply, at a minimum, with the DoD Discovery Metadata Specification (DDMS). This specification is available at: the DoD Metadata Registry found at http://diides.ncr.disa.mil/mdregHomePage/mdregHome.portal. The system should provide DDMS-compliant metadata at an appropriate level based on the type of data being tagged. It is not required that individual records within databases be tagged; rather it is expected that the database itself or some segment of it is tagged appropriately. Additionally, the contractor shall ensure that all structural and vocabulary metadata (metamodels, data dictionaries) associated with the exposed system data be made available in order to enable understanding of data formats and definitions. This includes proprietary metadata if it is required to effectively use the system data.
    - ***Enterprise Services/Capabilities*** : The contractor shall ensure that key business logic processing and other functional capabilities contained within the IT system are exposed using web-based open standards (e.g. APIs provide for Web Services-based access to system processes and data). The level of business logic exposure shall be sufficient to enable reuse/extension

within other applications and/or to build new capabilities. The contractor shall provide an assessment of how any licensing restrictions affect or does not affect meeting the goals of re-use and exposure as GIG-wide enterprise services.

- ***Optional Components/Modules*** : The contractor shall ensure that all standard and/or optional components of the IT system are identified and procured in a manner that ensures the requirements outlined in this document are met.

7.5 Information Assurance (IA)

7.5.1 Information Assurance (IA) Overview

Most programs delivering capability to the warfighter or business domains will use information technology to enable or deliver that capability. For those programs, developing a comprehensive and effective approach to IA is a fundamental requirement and will be key in successfully achieving program objectives. DoD defines IA as "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities." DoD policy and implementing instructions on information assurance are in the 8500 series of DoD publications. Program Managers and functional proponents for programs should be familiar with statutory and regulatory requirements governing information assurance, and understand the major tasks involved in developing an IA organization, defining IA requirements, incorporating IA in the program's architecture, developing an acquisition IA strategy (when required), conducting appropriate IA testing, and achieving IA certification and accreditation for the program. The information in the following sections will explain these tasks, the policy from which they are derived, their relationship to the acquisition framework, and the details one should consider in working towards effective IA defenses-in-depth in a net-centric environment.

7.5.2 Mandatory Policies

DoD Directive 5000.1, Enclosure 1, Paragraph E1.9, Information Assurance, states:

> *Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems. DoD policy for information assurance of information technology, including NSS, appears in DoD Directive 8500.1, reference (j).*

DoD Instruction 5000.2, Enclosure 4, Paragraph E.4.2, IT System Procedures states: "The program defines the requirement for an Information Assurance Strategy for Mission Critical and Mission Mission Essential IT systems."

> *The DoD CIO must certify (for MAIS programs) and confirm (for MDAPs) that the program is being developed in accordance with the CCA before Milestone approval. One of the key elements of this certification or confirmation is the DoD CIO's determination that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards. (See Table E4.T1. See section 7.8 of this Guidebook for a discussion of CCA compliance.)*

DoD Instruction 5000.2, Enclosure 4, Table E4.T1, CCA Compliance Table. requires that "The program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.

DoD Directive 8500.1, "Information Assurance (IA)": This directive establishes policy and assigns responsibilities under 10 U.S.C. 2224 to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

DoD Instruction 8500.2, "Information Assurance (IA) Implementation": This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.1.

DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System": This instruction implements policy, assigns responsibilities, and prescribes procedures necessary to integrate information assurance (IA) into the Defense Acquisition System; describes required and recommended levels of IA activities relative to the acquisition of systems and services; describes the essential elements of an Acquisition IA Strategy, its applicability, and prescribes an Acquisition IA Strategy submission and review process.

DoD Instruction 5200.40, "DoD Information Technology Security Certification And Accreditation Process (DITSCAP)": This instruction implements policy, assigns responsibilities and prescribes procedures under DoD Directive 8500.1 for Certification and Accreditation (C&A) of information technology (IT), including automated information systems, networks, and sites in the DoD.

- According to DoD Directive 8500.1, all acquisitions of Automated Information Systems (AISs) (to include Automated Information System applications, outsourced IT-based processes, and platforms or weapon systems with connections to the Global Information Grid (GIG) must be certified and accredited according to DoD Instruction 5200.40, DITSCAP.
- See other applicable Certification & Accreditation processes (such as Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information Within Information Systems" for systems processing Sensitive Compartmented Information).

7.5.3 Information Assurance (IA) Integration into the Acquisition Life Cycle

7.5.3.1 Before Milestone A

- Examine program and system characteristics to determine whether compliance with DoD Directive 8500.1 is recommended or required, and whether an acquisition IA strategy is required (Click here to find guidelines on making this determination: IA compliance requirements.)

- Establish an IA organization. Appoint a trained IA professional in writing as the IA Manager. This and other IA support may be organic to the program office, matrixed from other supporting organizations (e.g. Program Executive Office), or acquired through a support contractor.
- Begin to identify system IA requirements. Click here for Baseline IA Controls and IA Requirements Beyond Baseline Controls.
- Develop an acquisition IA strategy, if required. Click here for IA Compliance Decision Tree or click here for an Acquisition IA Strategy Template. Acquisition IA strategies developed in preparation for Milestone A will be more general, and contain a lesser level of detail than acquisition IA strategies submitted to support subsequent Milestone decisions. Click here to see the detailed Acquisition IA Strategy guidelines.

7.5.3.2 Before Milestone B

- If program is initiated post-Milestone A, complete all actions for Milestone A.
- Ensure IA considerations are incorporated in the program's Acquisition Strategy. Click here for example language for Acquisition Strategy IA Considerations.
- Update and submit the acquisition IA strategy. Click here for an Acquisition IA Strategy Template.
- Secure resources for IA. Include IA in program budget to cover the cost of developing, procuring, testing, certifying and accrediting, and maintaining the posture of system IA solutions. Ensure appropriate types of funds are allocated (e.g. Operations & Maintenance for maintaining IA posture in out years).
- Initiate DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Click here for DoD Instruction 5200.40 or other applicable Certification & Accreditation process (such as Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information Within Information Systems" for systems processing Sensitive Compartmented Information).

7.5.3.3 Before Milestone C

- Incorporate IA solutions through:
    - Systems Security Engineering efforts
    - Procurement of IA/IA enabled products. DoD Instruction 5000.2, Section E4.2.7, states that: "When the use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative shall be made." The Enterprise Software Initiative (ESI) includes commercial IA tools and should be utilized as the preferred source for the procurement of IA tools. The ESI Home Page lists covered products and procedures, and also shows DFARS (SUBPART 208.74) and Defense Acquisition System (DoD Instruction 5000.2, E4.2.7) requirements for compliance with the DoD ESI.

    - Implementation of security policies, plans, and procedures
    - Conducting IA Training
- Test and evaluate IA solutions. Click here for IA Testing details.
    - Developmental Test
    - Security Test & Evaluation, Certification and Accreditation activities
    - Operational Test
- Accredit the system under the DITSCAP or other applicable Certification and Accreditation process. For systems using the DITSCAP, DITSCAP Phase III should be completed, and an Approval to Operate should be issued by the Designated Approval Authority. Click here for DoD Instruction 5200.40 discussion of the Approval to Operate and Designated Approval Authority or other applicable Certification & Accreditation process elements (such as (DCID) 6/3 "Protecting Sensitive Compartmented Information Within Information Systems" for systems processing Sensitive Compartmented Information).

7.5.3.4 After Milestone C or before the Full Rate Production Decision Review (or equivalent for MAIS Programs)

- Maintain the system's security posture throughout its life cycle. This includes periodic re-accreditation.
- Assess IA during IOT&E on the mature system.

7.5.4 Estimated Information Assurance (IA) Activity Durations and Preparation Lead Times

Figure 7.5.4.1. shows the relationship between the acquisition framework and typical timeframes for accomplishing key IA activities.

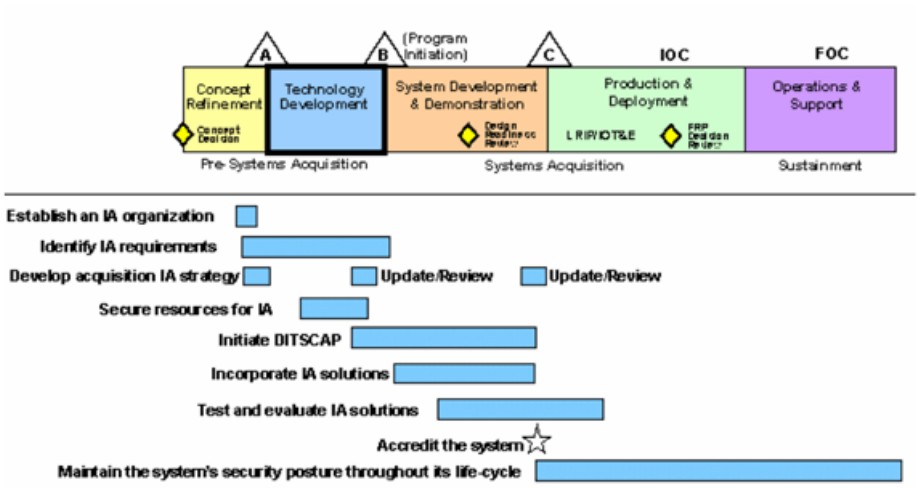

Figure 7.5.4.1. Typical Timeframes for Accomplishing Key IA Activities

Based on experience with a number of acquisition programs (both Major Automated Information Systems and Major Defense Acquisition Programs), an IA strategy for a pre-Milestone B program can be developed, staffed and coordinated, approved by the DoD Component Chief Information Officer and reviewed by the DoD Chief Information Officer in a period of 4-6 months. Typically 3-4 months of this effort is dedicated to defining the system IA architecture, which is a function of the overall system architecture.

For a pre-Milestone C program, a typical IA strategy can be completed, approved, and reviewed in 6 weeks to 3 months, because the system architecture will be more mature. However, there is an increased possibility that development of the strategy at this late date may uncover IA shortfalls because the strategy is being developed after IA-impacting decisions have been made. Click here for acquisition IA Strategy details.

7.5.5 Integrating Information Assurance (IA) into the Acquisition Process

The IA Compliance Decision Tree, Figure 7.5.5.1., is designed to help program managers determine the degree to which the 8500 series applies to any acquisition and whether an Acquisition IA Strategy is required. A tabular depiction of the same information appears in Table 7.5.5.1. IA Compliance by Acquisition Program Type.

Because requirements for IA vary greatly across acquisition programs, program managers should examine acquisition programs carefully to identify applicable IA requirements. The following guidelines derived from DoD Directive 8500.1 apply:

1) Programs that do not involve the use of Information Technology (IT) in any form have no IA requirements. However, program managers should examine programs carefully, since many programs have IT, such as automatic test equipment, embedded in the product or its supporting equipment.

2) Programs that include IT always have IA requirements, but these IA requirements may be satisfied through the normal system design and test regimen, and may not be required to comply with DoD Directive 8500.1. Acquisitions that include Platform IT with no network interconnection to the Global Information Grid fit into this category. However, such programs require an IA Strategy if they are designated Mission Critical or Mission Essential.

3) Acquisitions of Platforms with network interconnections to the Global Information Grid must comply with the IA requirements of DoD Directive 8500.1 and DoD Instruction 8500.2.

4) Acquisitions of Automated Information System applications or outsourced IT processes also must comply with DoD Directive 8500.1 and DoD Instruction 8500.2.

5) Programs that include IT, and that are designated Mission Critical or Mission Essential, require an IA Strategy without regard to the applicability of DoD Directive 8500.1. The DoD Component Chief Information Officer is responsible for approving the IA Strategy. Subsequent to the DoD Component Chief Information Officer approval, in accordance with DoD Instruction 5000.2, the DoD Chief Information Officer must review the IA Strategy.

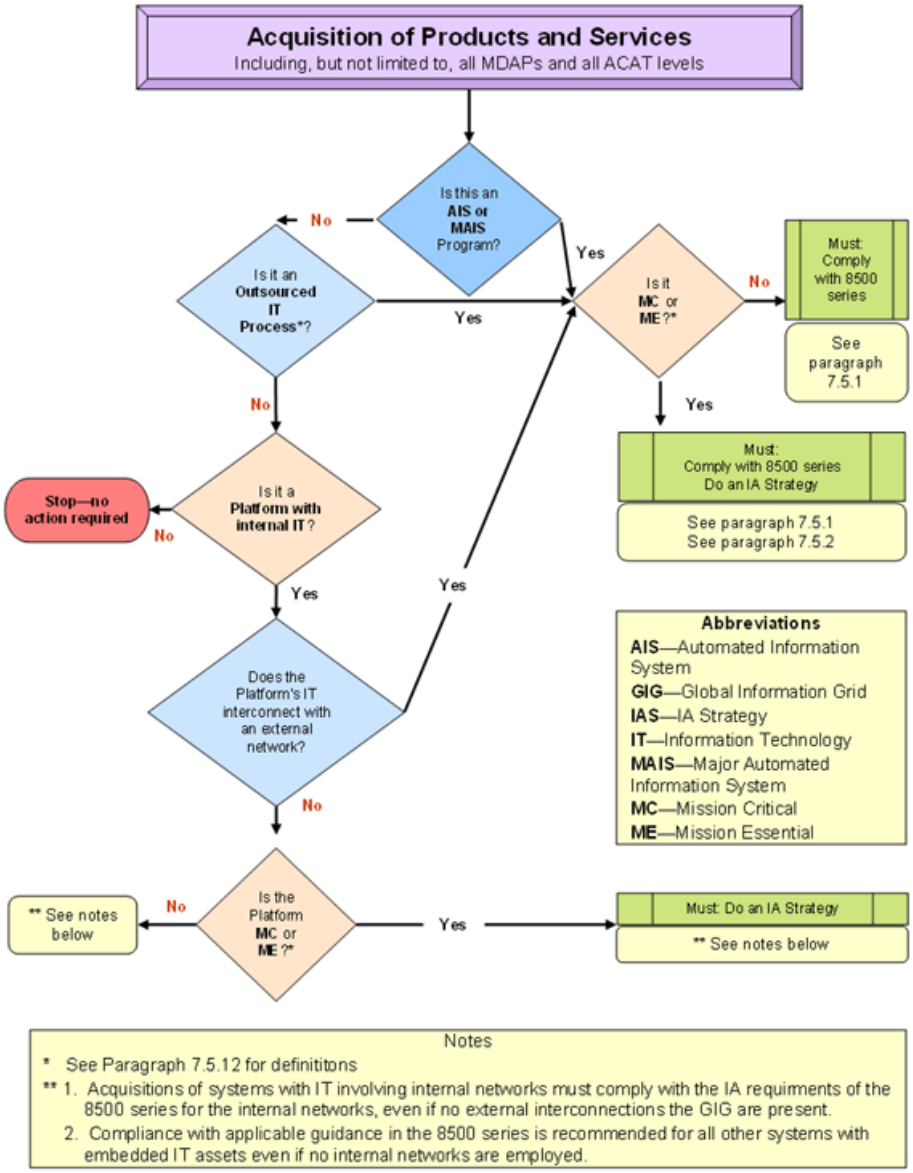

Figure 7.5.5.1. IA Compliance Decision Tree

Acquisition Programs for:		Acquisition IA Strategy	Compliance with 8500 series
No IT		Not Required	Not Required
Non-MC/ME AIS		Not Required*	Required
Non-MC/ME MAIS		Not Required*	Required
MC/ME AIS		Required	Required
MC/ME MAIS		Required	Required
Outsourced IT-based Processes		Not Required*	Required
Outsourced IT-based Processes that are MC/ME		Required	Required
Platform IT products/weapons systems that are, or have:			
MC/ME	Network Interconnections to the GIG		
No	No	Not Required*	*Recommended***
No	Yes	Not Required*	Required
Yes	No	Required	*Recommended***
Yes	Yes	Required	Required

Legend: AIS = Automated Information System
GIG = Global Information Grid
IT = Information Technology
MAIS = Major Automated Information System
MC/ME = Mission Critical/Mission Essential
PM = Program/Project Manager

* Although not required by DoD, the Component may require an Acquisition IA Strategy.
** PMs would be prudent to comply with all DoDI 8500.2 IA controls appropriate to the system

Table7.5.5.1. IA Compliance by Acquisition Program Type

7.5.6. Program Manager (PM) Responsibilities

7.5.6.1. Platform Information Technology (IT) Systems

Program managers for acquisitions of platforms with internal IT, including platforms such as weapons systems, sensors, medical technologies, or utility distribution systems, remain ultimately responsible for the platform's overall Information Assurance (IA) protection. If the Platform IT has an interconnection to the Global Information Grid (GIG), in accordance with DoD Instruction 8500.2, the program manager must identify all assurance measures needed to ensure both the protection of the interconnecting GIG enclave, and the protection of the platform from connection risks, such as unauthorized access, that may be introduced from the enclave. However, connecting enclaves have the primary responsibility for extending needed IA services (such as Identification and Authentication) to ensure an assured interconnection for both the enclave and the interconnecting platform. These IA requirements should be addressed as early in the acquisition process as possible. Program managers for acquisitions of Platforms with IT that does not interconnect with the GIG retain the responsibility to incorporate all IA protective measures necessary to support the platform's combat or support mission functions. The definition of the GIG recognizes "non-GIG IT that is stand-alone, self-contained or embedded IT that is not or will not be connected to the enterprise network." Non-GIG IT may include "closed loop" networks that are dedicated to activities like weapons guidance and control, exercise, configuration control or remote administration of a specific platform or collection of platforms. The primary test between whether a network is part of the GIG or is non-GIG IT is whether it provides enterprise or common

network services to any legitimate GIG entity. In any case, program managers for systems that are not connected to GIG networks would demonstrate prudent judgment by considering the IA program provisions in DoD Directive 8500.1 and DoD Instruction 8500.2, and employing those IA controls appropriate to their system.

7.5.6.2. Automated Information Systems (AIS)

Program managers for acquisitions of AIS applications are responsible for coordinating with enclaves that will host (run) the applications early in the acquisition process to address operational security risks the system may impose upon the enclave, as well as identifying all system security needs that may be more easily addressed by enclave services than by system enhancement. The baseline IA Controls serve as a common framework to facilitate this process. The Designated Approving Authority for the enclave receiving an AIS application is responsible for incorporating the IA considerations for the AIS application into the enclave's IA plan. The burden for ensuring an AIS application has adequate assurance is a shared responsibility of both the AIS application Program Manager and the Designated Approving Authority for the hosting enclave; however, the responsibility for initiation of this negotiation process lies clearly with the Program Manager. Program managers should, to the extent possible, draw upon the common IA capabilities that can be provided by the hosting enclave.

7.5.6.3. Outsourced IT-based Processes

Program managers for acquisitions of Outsourced IT-based Processes must comply with the IA requirements in the 8500 policy series. They are responsible for delivering outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services that present specific and unique challenges for the protection of the Global Information Grid. The program manager for an Outsourced IT-based process should carefully define and assess the functions to be performed and identify the technical and procedural security requirements that must be satisfied to protect DoD information in the service provider's operating environment and interconnected DoD information systems. Acquisition Contracting Officers should be familiar with IA requirements in general.

7.5.7. Information Assurance (IA) Controls

7.5.7.1. Baseline Information Assurance (IA) Controls

DoD Instruction 8500.2, Enclosure 3, establishes fundamental IA requirements for DoD information systems in the form of two sets of graded baseline IA Controls. Program managers are responsible for employing the sets of baseline controls appropriate to their programs. The baseline sets of IA controls are pre-defined based on the determination of the Mission Assurance Category (MAC) and Confidentiality Levels as specified in the formal requirements documentation or by the User Representative on behalf of the information owner. IA Controls addressing availability and integrity requirements are keyed to the system’s MAC based on the importance of the information to the mission, particularly the warfighters' combat mission. IA Controls addressing confidentiality requirements are based on the sensitivity or classification of the information. There are

three MAC levels and three confidentiality levels with each level representing increasingly stringent information assurance requirements. The three MAC levels are identified in Table 7.5.7.1.1.1.

MISSION ASSURANCE CATEGORY			
	DEFINITION	Integrity	Availability
1	These systems handle information that is determined to be **vital to the operational readiness or mission effectiveness of deployed and contingency forces** in terms of both content and timeliness.	HIGH	HIGH
2	These systems **handle information that is important to the support of deployed and contingency forces**.	HIGH	MEDIUM
3	These systems handle information that is necessary for the conduct of day-to-day business, but **does not materially affect support to deployed or contingency forces in the short-term**.	BASIC	BASIC

Table 7.5.7.1.1. Mission Assurance Category (MAC) Levels for IA Controls

The other major component in forming the baseline set of IA controls for every information system is determined by selecting the appropriate confidentiality level based on the sensitivity of the information associated with the information system. DoD has defined three levels of confidentiality, identified in Table 7.5.7.1.1.2.

Confidentiality Level	Definition
Classified	Systems processing classified information
Sensitive	Systems processing sensitive information as defined in DoDD 8500.1, to include any unclassified information not cleared for public release
Public	Systems processing publicly releasable information as defined in DoDD 8500.1 (i.e., information that has undergone a security review and been cleared for public release)

Table 7.5.7.1.2. Confidentiality Levels for IA Controls

7.5.7.2. Baseline Information Assurance (IA) Controls

The specific set of baseline IA controls that the program manager should address is formed by combining the appropriate lists of Mission Assurance Category (MAC) and Confidentiality Level controls specified in the DoD Instruction 8500.2, Enclosure 2. Table 15 illustrates the possible combinations.

Combination	Mission Assurance Category	Confidentiality Level	DoDI 8500.2 Enclosure 4 Attachments
1	MAC 1	Classified	1 and 4
2	MAC 1	Sensitive	1 and 5
3	MAC 1	Public	1 and 6
4	MAC 2	Classified	2 and 4
5	MAC 2	Sensitive	2 and 5
6	MAC 2	Public	2 and 6
7	MAC 3	Classified	3 and 4
8	MAC 3	Sensitive	3 and 5
9	MAC 3	Public	3 and 6

Table7.5.7.2.1. Possible Combinations of Mission Assurance Category and Confidentiality Level

There are a total of 157 individual IA Controls from which the baseline sets are formed. Each IA Control describes an objective IA condition achieved through the application of specific safeguards, or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the objective condition for every IA Control are assignable, and thus accountable. The IA

Controls specifically address availability, integrity, and confidentiality requirements, but also take into consideration the requirements for non-repudiation and authentication.

It is important to exercise due diligence in establishing the MAC level of an information system. The baseline set of IA controls for availability and integrity are purposefully graded to become increasingly stringent for the higher MAC levels. The required resource costs to achieve compliance with the baseline IA controls at the higher MAC levels can be very significant as befits information and information systems on which a warfighter's mission readiness or operational success depends. The IA controls also become increasingly stringent or robust at the higher Confidentiality levels.

7.5.7.3. Information Assurance (IA) Requirements Beyond Baseline IA Controls

There are several additional sources of IA requirements beyond the Baseline IA Controls.

A system being acquired may have specific IA requirements levied upon it through its controlling capabilities document (i.e., Capstone Requirements Document, Initial Capabilities Document, Capabilities Development Document or Capabilities Production Document). These IA requirements may be specified as performance parameters with both objective and threshold values.

All IA requirements, regardless of source, are compiled in a single system Requirements Traceability Matrix. Guidebook Chapter discusses the Requirements Traceability Matrix and other applicable Certification & Accreditation processes (such as Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information Within Information System" for systems processing Sensitive Compartmented Information).

Comment [mcm2]:

7.5.8. Information Assurance (IA) Testing

See section 9.9.2.

7.5.9. Acquisition Information Assurance (IA) Strategy

The primary purpose of the Acquisition IA Strategy is to ensure compliance with the statutory requirements of the Clinger Cohen Act and related legislation, as implemented by DoD Instruction 5000.2 . As stated in Table E4.T1. of that Instruction, the Acquisition IA Strategy provides documentation that "The program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards." The program manager develops the Acquisition IA Strategy to help the program office organize and coordinate its approach to identifying and satisfying IA requirements consistent with DoD policies, standards, and architectures.

The Acquisition IA Strategy serves a purpose separate from the System Security Authorization Agreement (SSAA). Developed earlier in the acquisition life cycle and written at a higher level, the Acquisition IA Strategy documents the program's overall IA requirements and approach, including the certification and accreditation approach (which will subsequently result in an SSAA). The Acquisition IA Strategy must be available for

review at all Acquisition Milestone Decisions, including early milestones when an SSAA would not yet be available.

The Acquisition IA Strategy lays the groundwork for a successful SSAA by facilitating consensus among the Program Manager, Component Chief Information Officer and DoD Chief Information Officer on pivotal issues such as Mission Assurance Category, Confidentiality Level, and applicable Baseline IA Controls; selection of the appropriate certification and accreditation process; identification of the Designated Approving Authority and Certification Authority; and documenting a rough timeline for the certification and accreditation process.

7.5.9.1. Development

Ideally, a Working-level Integrated Product Team (WIPT) should support the development of the Acquisition IA Strategy. The WIPT should consist of subject matter experts familiar with the system being acquired, the intended use of the system, and the operational and system architectures within which the system will function. As the operational and system architectures mature, the WIPT should plan for and coordinate interface details with managers of systems and subsystems with which the system being acquired will interface.

The Acquisition IA Strategy should be a stand-alone document. Although other key documents can be referenced within the Acquisition IA Strategy to identify supplemental or supporting information, the Acquisition IA Strategy should contain sufficient internal content to clearly communicate the strategy to the reader. If a single document is employed by the program to consolidate acquisition documentation, the Acquisition IA Strategy should be included as a separate section of the document.

Configuration control of the Acquisition IA Strategy should be maintained with respect to the program's governing requirements document (Initial Capabilities Document, etc.) and the Information Support Plan (formerly known as the C4ISP). If a governing capabilities document or the Information Support Plan is updated, the Acquisition IA Strategy should be validated or updated accordingly.

The IA Strategy Format Template, while not mandatory, will help you construct an Acquisition IA Strategy document that will satisfy statutory review requirements. Write the document at the unclassified level, and include classified annexes, if required. Factors determining the specific content and level of detail needed can include the following:

- **Acquisition life cycle stage.** Strategies for programs that are early in the acquisition life cycle will be necessarily at a higher level and less definitive than more mature programs. The level of detail in an Acquisition IA Strategy will increase as a program transitions from one acquisition phase to the next. At program initiation, an IA Strategy is not expected to contain all of the information about initial operating capabilities or future system interfaces that will be available at Milestone B or at the full-rate production decision point. Requirements, employment concepts, and architectures for both the system being acquired, and the systems with which it interfaces, will evolve and mature throughout the acquisition life cycle. As the program matures, the IA Strategy should also evolve. The strategy should be maintained with revisions as required

until system retirement and disposal. Click here for acquisition IA Strategy details.

- **Extent of system/network interaction.** Systems with a high degree of system-to-system information exchange, or systems connected to the Global Information Grid will require more comprehensive discussions of IA considerations related to their environment.
- **Mission Assurance Category and Confidentiality Level.** Systems with higher mission assurance categories and higher confidentiality levels will necessarily require more comprehensive strategies than those with lower levels.
- **Developmental systems versus Commercial-Off-the-Shelf (COTS) Items.** Programs acquiring new systems through development will require more robust treatment of the identification, design, systems engineering and testing of IA requirements than non-developmental programs. However, Acquisition IA Strategies for the acquisition of COTS systems should also address the approach employed to ensure that the COTS products meet IA requirements and comply with the product specification and evaluation requirements of DoD Instruction 8500.2, Enclosure 3, paragraph E3.2.5.
- **Evolutionary Acquisitions.** Programs employing evolutionary acquisition should differentiate the identification and satisfaction of IA requirements, certification and accreditation activities, and milestone reviews for each increment planned.
- **Special Circumstances.** In the following specific cases, Acquisition IA Strategy content is limited as noted, in consideration of the unique characteristics of these acquisition programs:
    - **Family of Systems Acquisition Programs.** The Acquisition IA Strategy for these programs should be written at a capstone level, focusing on the integration of IA requirements and controls, coordination of System Security Authorization Agreement boundaries, and ensuring IA resourcing for own and subordinate systems. Click here for acquisition IA Strategy details .
    - **Platform IT with interconnection to an external system or network.** In accordance with DoD Instruction 8500.2, the Acquisition IA Strategy must specifically address IA protection for the interconnection points. Click here for acquisition IA Strategy details.
    - **Platform IT with no interconnection to an external system or network.** The requirement for an Acquisition IA Strategy can be satisfied by inserting the following statement in the program's Clinger Cohen Act compliance table submission: “Platform IT does not have an interconnection to an external network.” DoD Instruction 8500.2, Enclosure 4 provides further guidance on the submission of a Clinger Cohen Act compliance table. Although not required, program managers responsible for this type of acquisition would be prudent to consider and

implement the IA guidance in DoD Directive 8500.1 and DoD Instruction 8500.2. Click here for more on the Clinger Cohen Act.

DoD Components may require additional questions/areas of concerns (e.g. Critical Infrastructure Protection; Privacy Impact, etc.) in separate DoD Component-specific implementing guidance for Acquisition IA Strategy content and submission.

7.5.9.2. Review Requirements

Acquisition IA Strategies must be submitted for approval and review in accordance with Table 7.5.9.2.1., which is based on submission requirements detailed in DoD Instruction 5000.2, Enclosure 4. Sufficient time should be allowed for Acquisition IA Strategy preparation or update, Component CIO review and approval, and DoD CIO review prior to applicable milestone decisions, program review decisions, or contract awards.

Acquisition Category *	Events requiring prior Review	Acquisition IA Strategy Approval	Acquisition IA Strategy Review
ACAT IAM, IAC, and ID; and (if MAIS) ACAT IC	**Milestone A B, C, full rate production decision and acquisition contract award**	**Component CIO**	**DoD CIO**
All other acquisitions	**Milestone A B, C, full rate production decision and acquisition contract award**	**Component CIO or Designee**	**Delegated to Component CIO**

*Acquisition Category (ACAT) descriptions are provided in DoD Instruction 5000.2, Table E2.T1.

Table7.5.9.2.1. IA Strategy Approval and Review Requirements

7.5.9.3. Additional Information

Questions or recommendations concerning the Acquisition IA Strategy or its preparation or the IA strategy template should be directed to the Defense-wide Information Assurance Program Office (OASD(NII)-DIAP).

7.5.9.4. Information Assurance Strategy Template

(PROGRAM NAME)

1. **Program Category and Life Cycle Status:** Identify the Acquisition Category (Acquisition Category) of the program. Identify current acquisition life cycle phase and next milestone decision. Identify whether the system has been designated "Mission Critica" or "Mission Essentia" in accordance with DoD Instruction 5000.2. Include a graphic representation of the program's schedule.

2. **Mission Assurance Category (MAC) and Confidentiality Level:** Identify the system's MAC and Confidentiality Level as specified in the applicable requirements document, or as determined by the system User Representative on behalf of the information owner, in accordance with DoD Instruction 8500.2.

3. **System Description:** Provide a high-level overview of the specific system being acquired. Provide a graphic (block diagram) that shows the major elements/subsystems that make up the system or service being acquired, and how they fit together. Describe the system's function, and summarize significant information exchange requirements (IER) and interfaces with other IT or systems, as well as primary databases supported. Describe, at a high level, the IA technical approach that will secure the system, including any protection to be provided by external systems or infrastructure. PMs should engage National Security Agency (NSA) early in the acquisition process for assistance in developing an IA approach, and obtaining information systems security engineering (ISSE) services, to include describing information protection needs, defining and designing system security to meet those needs, and assessing the effectiveness of system security.

4. **Threat Assessment:** (Include as classified annex if appropriate) Describe the methodology used to determine threats to the system (such as the System Threat Assessment), and whether the IT was included in the overall weapon system assessment. In the case of an AIS application, describe whether there were specific threats unique to this system's IT resources due to mission or area of proposed operation. For MAIS programs, utilization of the "Information Operations Capstone Threat Capabilities Assessment" (DIA Doc # DI-1577-12-03) [1st Edition Aug 03] is required by DoD Instruction 5000.2.

5. **Risk Assessment:** (Include as classified annex if appropriate) Describe the program's planned regimen of risk assessments, including a summary of how any completed risk assessments were conducted. For systems where software development abroad is a possible sourcing option, describe how risk was assessed.

6. **Information Assurance Requirements:** Describe the program's methodology used for addressing IA requirements early in the acquisition lifecycle. Specify whether any specific IA requirements are identified in the approved governing requirements documents (e.g. Capstone Requirements Document, Initial Capabilities Document, Capabilities Design Document, or Capabilities Production Document). Describe how IA requirements implementation costs (including costs associated with certification and accreditation activities) are included and visible in the overall program budget.

7. **Acquisition Strategy:** Provide a summary of how information assurance is addressed in the program's overall acquisition strategy document. Describe how the Request for Proposal (RFP) for the System Development and Demonstration Phase contract was, or will be, constructed to include IA requirements in both the operational and system performance specifications, and integrated into the system design, engineering, and testing. In addition, describe how the RFP communicates the requirement for personnel that are trained in IA. Address

whether the program will be purchasing commercial off-the-shelf IA or IA-Enabled products, and the program's means for verifying that the mandates of National Security Telecommunications and Information Systems Security Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Product" will be followed.

8. **DoD Information Technology Security Certification and Accreditation Process (DITSCAP):** Provide the name, title, and organization of the Designated Approving Authority (DAA), Certification Authority (CA), and User Representative. If the program is pursuing an evolutionary acquisition approach (spiral or incremental development), describe how each increment will be subjected to the certification and accreditation process. Provide a timeline describing the target completion dates for each phase of certification and accreditation in accordance with DoD Instruction 5200.40. Normally, it is expected that DITSCAP Phase 1 will be completed prior to or soon after Milestone B; Phase 2 and 3 completing prior to Milestone C; and Authority to Operate (ATO) issued prior to operational test and evaluation. If the DITSCAP process has started, identify the latest phase completed, and whether an Authority to Operate (ATO) or Interim Authority to Operate (IATO) was issued. If the system being acquired will process, store or distribute Sensitive Compartmented Information (SCI), compliance with Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information Within Information System" is required, and approach to compliance should be addressed.

9. **IA Testing**: Discuss how IA testing has been integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the Test & Evaluation Master Plan.

10. **IA Shortfalls:** (Include as classified annex if appropriate) Identify any significant IA shortfalls, and proposed solutions and/or mitigation strategies. Specify the impact of failure to resolve any shortfall in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability. If the solution to an identified shortfall lies outside the control of the program office, provide a recommendation identifying the organization with the responsibility and authority to address the shortfall. If applicable, identify any Acquisition Decision Memoranda that cite IA issues.

11. **Policy/Directives:** List the primary policy guidance employed by the program in preparing and executing the Acquisition IA Strategy, including the DoD 8500 series, and DoD Component, Major Command/Systems Command, or program-specific guidance, as applicable. The Information Assurance Support Environment web site provides an actively maintained list of relevant statutory, Federal/DoD regulatory, and DoD guidance that may be applicable. This list is available at http://iase.disa.mil/policy.html.

12. **Relevant Associated Program Documents:** Provide statement that this version of the Acquisition IA Strategy is reflective of the Program CRD/ICD/Capability Development Document/CPD dated _____, and the Information Support Plan (ISP) dated _____. [Note: subsequent revisions to

the requirements documents or ISP will require a subsequent revision or revalidation of the Acquisition IA Strategy.]

13. **Point of Contact:** Provide the name and contact information for the program management office individual responsible for the Acquisition IA Strategy document. It is recommended that the program office's formally appointed Information Assurance Manager (as defined in DoD Instruction 8500.2) be the point of contact.

7.5.9.5. Information Assurance (IA) Strategy Considerations

The following text is recommended for tailoring as the IA section of an Acquisition Strategy. The presented "considerations" are examples, but experience has shown that they are common to most programs. The program manager should tailor and include this text as appropriate.

Information Assurance

The _____ PMO has reviewed all appropriate Information Assurance (IA) policy and guidance, and has addressed the implementation of these IA considerations in the _____ Program Information Assurance Strategy. IA requirements shall be addressed throughout the system life cycle in accordance with DoD Directive 8500.1, DoD Instruction 8500.2, DoD Instruction 5200.40, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," *[include: "and Director of Central Intelligence Directive 6/3" but only if system handles SCI]*. The IA Strategy is an integral part of the program's overall acquisition strategy, identifying the technical, schedule, cost, and funding issues associated with executing requirements for information assurance. The following summarizes significant IA considerations impacting the program's acquisition strategy.

IA Technical Considerations. _____ will employ Commercial-Off-The-Shelf (COTS) IA and IA-enabled products as part of the security architecture. These products must be National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) compliant, requiring them to be validated by accredited labs under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP). Similarly, GOTS IA or IA-enabled products employed by the system must be evaluated by the NSA or in accordance with NSA-approved processes. *[and/or other significant technical issues as required]*

IA Schedule Considerations. The IA certification and accreditation timeline includes significant events that impact the overall testing, operational assessment and deployment schedules. Key milestones such as the approval of the Phase I SSAA, Interim Authority to Test, Interim Authority to Operate, and Authority to Connect, as well as the overall certification and accreditation schedule, are integrated into the program's Test & Evaluation Master Plan (TEMP). *[other significant schedule issues as required]*

IA Cost Considerations. IA specific costs include the development/procurement, test & evaluation, and certification & accreditation of the IA architecture. It also

includes operations and maintenance costs related to maintaining the system security posture following deployment. *[identify any high-impact issues]*

IA Funding Considerations. All IA lifecycle costs are adequately funded. *[if not, what and why]*

IA Staffing and Support Issues. The PMO is adequately staffed to support IA requirements, with (X) Government staff assigned full time IA duties. One member of the PMO staff has been appointed Information Assurance Manager for the system, in accordance with DoD Directive 8500.1. Support contractors provide X full-time-equivalents of IA support to the PMO. In addition, [activity X] will provide C&A support to the program. *[other significant staffing and support issues as required]*

7.5.10. DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

In accordance with DoD Directive 8500.1, all acquisitions of AISs (to include MAIS), outsourced IT-based processes, and platforms or weapon systems with connections to the GIG must be certified and accredited in accordance with DoD Instruction 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*.

7.5.11. Software Security Considerations

For the acquisition of software-intensive Information Technology, especially that used in National Security Systems, program managers should consider the significant operational threat posed by the intentional or inadvertent insertion of malicious code.

The Defense Intelligence Agency can perform an analysis to determine foreign ownership, control, and/or influence of vendors bidding for selection to provide information technology, if warranted. If there is sufficient cause for security concerns based on the analysis, the acquiring organization should conduct an independent evaluation of the software.

The Program Manager should identify the software-intensive Information Technology candidates for Defense Intelligence Agency analysis before the Milestone B decision.

7.5.12. Information Assurance (IA) Definitions

The following IA related definitions are provided to assist the reader in understanding IA terminology. For a more comprehensive set of IA definitions, see DoD Directive 8500.1 and DoD Instruction 8500.2, and DoD Instruction 5200.40.

Accreditation. Formal declaration by the Designated Approving Authority that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Acquisition Program. A directed, funded effort that provides new, improved, or continuing materiel, weapon, or information system or service capability, in response to an approved need.

Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Automated Information System (AIS). See DoD Information System.

Availability. Timely, reliable access to data and information services for authorized users.

Certification. Comprehensive evaluation of the technical and non-technical security features of an information technology system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certification Authority (CA). Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying, and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation package.

Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes.

Confidentiality Level. Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has defined three confidentiality levels: classified, sensitive, and public.

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned.

Designated Approving Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.

DoD Information System. The entire infrastructure, organization, personnel, and components for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology-based processes, and platform information technology interconnections.

Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program such as those described in DoD Directive 5000.1. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or fire control); or a

combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave.

Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced information technology - based processes they support, and derive their security needs from those systems. They provide standard Information Assurance capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, tactical networks, and data processing centers.

Outsourced Information Technology (IT)-based Process. For DoD Information Assurance purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Platform Information Technology (IT) Interconnection. For DoD Information Assurance purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration and remote upgrade or reconfiguration.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD process for identifying information security requirements, providing security solutions, and managing information system security activities. Click here to for DoD Instruction 5200.40 or other applicable Certification & Accreditation process (such as Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information Within Information System" for systems processing Sensitive Compartmented Information).

Family of Systems (FoS). A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of

systems can be tailored to provide desired capabilities, dependent on the situation. An example of an FoS would be an anti-submarine warfare FoS consisting of submarines, surface ships, aircraft, static and mobile sensor systems and additional systems. Although these systems can independently provide militarily useful capabilities, in collaboration they can more fully satisfy a more complex and challenging capability: to detect, localize, track, and engage submarines.

Global Information Grid (GIG). Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems. The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. Non-GIG Information Technology (IT) is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data or information for use by other equipment, software, and services.

Click here for GIG details.

Information Assurance (IA) Control. An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality.

Information Assurance (IA) Product. Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

Information Assurance (IA)-Enabled Information Technology Product. Product or technology whose primary role is not security, but which provides security services as an

associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

Information. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Major Automated Information System (MAIS). An acquisition program where: (1) the dollar value estimated by the DoD Component Head is to require program costs (all appropriations) in any single year in excess of $32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of $126 million in FY 2000 constant dollars, or total Lifecycle costs in excess of $378 million in FY 2000 constant dollars, or (2) Milestone Decision Authority designation as special interest.

Milestone Decision Authority (Milestone Decision Authority). The designated individual with overall responsibility for a program. The Milestone Decision Authority shall have the authority to approve entry of an acquisition program into the next phase of the acquisition process and shall be accountable for cost, schedule, and performance reporting to higher authority, including Congressional reporting.

Mission Assurance Category. Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission

assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.

Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance.

Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

Mission Critical (MC) Information System. A system that meets the definitions of "information syste" and "national security system" the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical shall be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management Information Technology (IT) system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense(Comptroller).) A "Mission-Critical Information Technology Syste" has the same meaning as a "Mission-Critical Information System" For additional information, see DoD Instruction 5000.2, Enclosure 4.

Mission Essential (ME) Information System. A system that meets the definition of "information syste" that the acquiring DoD Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the Under Secretary of Defense(Comptroller) A "Mission-Essential Information Technology Syste" has the same meaning as a "Mission-Essential Information System" For additional information, see DoD Instruction 5000.2, Enclosure 4.

National Security System (NSS). Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:

Involves intelligence activities;

Involves cryptologic activities related to national security;

Involves command and control of military forces;

Involves equipment that is an integral part of a weapon or weapons system; or

Subject to the following limitation, is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Outsourced Information Technology-based Process. See DoD Information System.

Platform Information Technology Interconnection. See DoD Information System.

Program Manager (PM). The designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs. the program manager shall be accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority throughout the life cycle.

System of Systems (SoS). A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole. An example of a SoS could be interdependent information systems. While individual systems within the SoS may be developed to satisfy the peculiar needs of a given user group (like a specific Service or agency), the information they share is so important that the loss of a single system may deprive other systems of the data needed to achieve even minimal capabilities.

System Security Authorization Agreement (SSAA). A formal agreement among the Designated Approving Authority(ies), the Certification Authority, the Information Technology (IT) system user representative, and the program manager. It is used throughout the entire DoD Information Technology Security Certification and Accreditation Process (see DoD Instruction 5200.40) to guide actions, document decisions, specify IT security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

User Representative. The individual or organization that represents the user or user community in the definition of information system requirements.

Weapon(s) System. A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

7.6. Electromagnetic Spectrum

7.6.1. Electromagnetic Spectrum Considerations

The program manager must consider the electromagnetic spectrum when delivering capability to the warfighters or business domains. The fundamental questions are if and how the system or equipment being developed will depend on and interact with the electromagnetic spectrum (hereafter referred to as "spectrum"). Other key questions include the following:

- Will the system/equipment require spectrum to operate as it is intended (e.g., to communicate with other systems; to collect and/or transmit data, to broadcast signals, etc.)?
- Will the spectrum the system/equipment needs to operate be available for use in the intended operational environment?
- Will the system/equipment, including commercial-off-the-shelf systems delivered by the program, radiate electromagnetic energy that could be detrimental to other systems or equipment?
- Will the intended operational electromagnetic environment produce harmful effects to the intended system, even if the proposed system does not radiate electromagnetic energy (such as ordnance)?

National, international, and DoD policies and procedures for the management and use of the electromagnetic spectrum direct program managers developing spectrum-dependent systems/equipment to consider spectrum supportability requirements and Electromagnetic Environmental Effects (E3) control early in the development process. Given the complex environment (both physical and political) in which DoD forces operate, and the potential for worldwide use of capabilities procured for DoD, early and thorough consideration is vitally important. The spectrum supportability process ensures the following:

- The spectrum-dependent system/equipment being acquired is designed to operate within the proper portion of the electromagnetic spectrum;
- Permission has been (or can be) obtained from designated authorities of sovereign ("host") nations (including the United States) to use that equipment within their respective borders; and
- The newly acquired equipment can operate compatibly with other spectrum dependent equipment already in the intended operational environment (electromagnetic compatibility).

Because this process requires coordination at the national and international levels, starting the process early helps a program manager address the full range of considerations and caveats, obtain the necessary approvals to proceed through the acquisition process, and successfully deliver capabilities that will work.

E3 control is concerned with the proper design and engineering to minimize the impact of the electromagnetic environment on equipment, systems, and platforms. E3 control applies to the electromagnetic interactions of both spectrum-dependent and non-spectrum-dependent objects within the operational environment. Examples of non-spectrum-dependent objects that could be affected by the electromagnetic environment are ordnance, personnel, and fuels. The increased dependency on and competition for portions of the electromagnetic spectrum have amplified the likelihood of adverse interactions among sensors, networks, communications, and weapons systems.

Ensuring the compatible operation of DoD systems in peace and in times of conflict is growing in complexity and difficulty. DoD has established procedures, described below, to successfully obtain spectrum supportability for, and control the electromagnetic environmental effects impacts upon the equipment, systems, and platforms used by our military forces. While the requirements to obtain spectrum supportability should be addressed early in the acquisition programs, the proper design and engineering techniques to control E3 should be considered throughout the acquisition process to ensure the successful delivery of the operational capability to the warfighter.

7.6.2. Mandatory Policies

- DoD Instruction 5000.2, Enclosure 3, Table E3.T1 (Statutory Information Requirements) requires all systems/equipment that require utilization of the electromagnetic spectrum to obtain spectrum certification compliance through the submission of a DD Form1494, "Application for Equipment Frequency Allocation." Compliance (obtained by receiving host nation approval of the submitted DD1494) is required at Milestone B (or at Milestone C, if there is no Milestone B).
- Title 47, CFR, Chapter III, Part 300.1 requires compliance with the National Telecommunications and Information Administration "Manual of Regulations and Procedures for Federal Radio Frequency Management," and applies to all Federal Agencies that use the electromagnetic spectrum within the United States and U.S. possessions.
- OMB Circular A-11, Part 2, contains the requirement to obtain certification by the National Telecommunications and Information Administration that the radio frequency can be made available before estimates are submitted for the development or procurement of major radio spectrum-dependent communications-electronics systems (including all systems employing satellite techniques) within the United States and U.S. possessions.
- DoD Directive 4650.1, "Policy for the Management and Use of the Electromagnetic Spectrum," contains policy applicable to all DoD Components that prohibits spectrum-dependent systems under development from
    1. Proceeding into the System Development and Demonstration Phase without a spectrum supportability determination unless the Milestone Decision Authority grants specific authorization to proceed; or

2. Proceeding into the Production and Deployment Phase without a spectrum supportability determination unless the Under Secretary of Defense (Acquisition, Technology, and Logistics) or the Assistant Secretary of Defense for Networks and Information Integration grants specific authorization to proceed.

The Directive also requires that spectrum-dependent "off-the-shelf" systems have a spectrum supportability determination before being purchased or procured.

- DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," establishes policy and responsibilities for the management and implementation of the DoD E3 Program. This program ensures mutual electromagnetic compatibility and effective electromagnetic environmental effects control among ground, air, sea, and space-based electronic and electrical systems, subsystems, and equipment, and the existing natural and man-made electromagnetic environment.

7.6.3. Spectrum Management Integration into the Acquisition Life Cycle

Assigned managers should take the following actions to obtain spectrum supportability for spectrum-dependent equipment, and minimize the electromagnetic environmental effects on all military forces, equipment, systems, and platforms (both spectrum-dependent and non spectrum-dependent). Consideration of these critical elements throughout the acquisition process will help to ensure successful delivery of capability to the warfighter.

The assigned manager should include the funding to cover spectrum supportability and control of electromagnetic environmental effects as part of the overall program budget. Section 7.6.4.1 addresses spectrum supportability;

7.6.3.1. Before Milestone A

As early as possible:

- Develop spectrum supportability and electromagnetic environmental effects (E3) control requirements and perform initial spectrum supportability and E3 risk assessments to e nsure Spectrum issues are addressed early in the program acquisition. (Click here for definition of spectrum supportability and E3, and information relating to spectrum supportability processes and E3 control requirements).
- Complete and submit an initial Stage 1 (Conceptual) DD Form 1494 for coordination. Click here for DD Form 1494 processing for Spectrum Certification herein.

7.6.3.2. Before Milestone B (or before the first Milestone that authorizes contract award)

- If the system is spectrum-dependent and has not yet obtained Certification of Spectrum Support from National Telecommunications and Information Administration or the Military Communications-Electronics Board to proceed into

the System Development and Demonstration Phase, the program manager must develop a justification and a proposed plan to obtain spectrum supportability. (DoD Directive 4650.1 requires Milestone Decision Authorities and/or DoD Component Acquisition Executives to provide such a justification and proposed plan to the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, the Director, Operational Test and Evaluation (DOT&E), and the Chair, Military Communications-Electronics Board.)

- Address spectrum supportability and electromagnetic environmental effects (E3) control requirements in the Statement of Work (SOW), Contract Data Requirements List (CDRL), and Performance Specifications.
- Update the spectrum supportability and E3 control requirements according to CJCSM 3170.01to ensure spectrum issues are addressed in the Capability Development Document.
- Ensure completion/update and submission of the DD Form1494. If previously submitted, ensure information is current. Click here for DD Form 1494 processing for Spectrum Certification.
- Define spectrum supportability and E3 control requirements in the Information Support Plan.
- Define in the Test Evaluation Master Plan (1) spectrum supportability and E3 control requirements to be tested during Developmental Test and Evaluation, and (2) the spectrum supportability and E3 assessments to be performed during Operational Test and Evaluation.

7.6.3.3. Before Milestone C

Review and update spectrum supportability and electromagnetic environmental effects control requirementsin the Capability Production Document, the Information Support Plan, and Test Evaluation Master Plan.

If the system is spectrum-dependent and has not yet obtained the spectrum supportability required to allow the system to proceed into the Production and Deployment Phase, the program manager must develop a justification and a proposed plan to obtain spectrum supportability. (DoD Directive 4650.1 requires Milestone Decision Authorities and/or CAEs to provide such a justification and proposed plan to the USD(AT&L)ASD(NII)/DoD(CIO), the DOT&E), and the Chair, MCEB.)

7.6.3.4. After Milestone C

Monitor system changes to determine their impact on requirements for spectrum supportability and electromagnetic environmental effects (E3) control. Changes to operational parameters (e.g., tuning range, bandwidth, emission characteristics, antenna gain and/or height, or output power) or proposed operational locations may require additional spectrum certification actions through an updated DD Form 1494 or require

additional E3 analysis or tests. Program managers should work with their spectrum managers to determine and satisfy additional requirements, as appropriate.

7.6.3.5. Estimated Preparation Lead Time

Spectrum certification must be addressed at milestone reviews as required by DoD Instruction 5000.2. Nominal time to complete the spectrum certification process (time from DD Form 1494 submittal to approval) is normally three to nine months, but often takes longer. Therefore, at a minimum, the program manager should plan to submit the DD Form 1494 three to nine months prior to a Milestone decision. Processing time depends upon quality of data, the number of host nations whose coordination is required, and the size of the staffs at the host nations' spectrum offices. The host nation approval process can be a critical factor in obtaining spectrum certification. It is sometimes a lengthy process, so start early to obtain approval. To avoid unnecessary processing delays, list on the DD Form 1494 **only those nations in which permanent deployment is planned, (i.e., do not list "worldwide deployment" as the intended operational environment)** .

7.6.3.6. Key Review Actions by Assigned Managers

- Define, and update as necessary, applicable electromagnetic environments where systems/equipment are intended to operate;
- Establish electromagnetic environmental effects (E3) control requirements, with special emphasis on mutual compatibility and Hazards of Electromagnetic Radiation to Ordnance guidance;
- Define E3 programmatic requirements to include analyses, modeling and simulation, and test and evaluation;
- Ensure that E3 developmental test and evaluation / operational test and evaluation requirements and spectrum management planning and analyses are addressed in the Test and Evaluation Master Plan, and that resources are identified to support these activities.

7.6.3.7. Electromagnetic Environmental Effects (E3) Control and Spectrum Certification Requirements in the Joint Capabilities Integration and Development System

Both CJCSM 3170.01 and CJCSI 6212.01 require the Capstone Requirements Document, the Capability Development Document, and the Capability Production Document to address spectrum certification and E3 control.

The Joint Staff will employ the following assessment criteria when reviewing the Capstone Requirements Document:

- Does the Capstone Requirements Document address spectrum certification and supportability?
- Does the Capstone Requirements Document address the control of electromagnetic environmental effects (E3)?

According to the Capability Development Document and Capability Production Document template in CJCSM 3170.01 and CJCSI 6212.01, both spectrum supportability and E3 control requirements must be addressed. The Joint Staff will employ the following assessment criteria when reviewing the Capability Development Document and/or the Capability Production Document:

- Does the Capability Development Document and/or the Capability Production Document address spectrum certification, supportability, and host nation approval?
- Does the Capability Development Document and/or the Capability Production Document address the control of E3?
- Does the Capability Development Document and/or the Capability Production Document address the safety issues regarding hazards of electromagnetic radiation to ordnance?

Sample Language. The three sample statements shown below should be included, as applicable, as THRESHOLD requirements. The first applies to communications-electronics equipment and is used to denote compliance with applicable DoD, national, and international spectrum policies and regulations. The second is used to require compatible operation. Finally, the third would be used if ordnance safety were of concern.

> *Spectrum Certification. The XXX System will comply with the applicable DoD, National, and International spectrum management policies and regulations and will obtain spectrum certification prior to operational deployment. DD Form 1494 will be submitted to the Military Communications Electronics Board Joint Frequency Panel. (Threshold)*
>
> *Electromagnetic Environmental Effects. The XXX System shall be mutually compatible and operate compatibly in the electromagnetic environment. It shall not be operationally degraded or fail due to exposure to electromagnetic environmental effects, including high intensity radio frequency (HIRF) transmissions or high-altitude electromagnetic pulse (HEMP). Ordnance systems will be integrated into the platform to preclude unintentional detonation. (Threshold)*
>
> *Hazards of Electromagnetic Radiation to Ordnance. All ordnance items shall be integrated into the system in such a manner as to preclude all safety problems and performance degradation when exposed to its operational electromagnetic environment. (Threshold)*

7.6.3.8. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in the Information Support Plan (ISP)

According to DoD Instruction 4630.8 and CJCSI 6212.01, the ISP must address Spectrum Supportability (e.g., Spectrum Certification, reasonable assurance of the availability of operational frequencies, and consideration of E3 control). Specific items to be addressed are listed in DoD Instruction 4630.8 paragraph 8.2.7.3.3.2, Step 9.

7.6.3.9. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in the Test and Evaluation Master Plan (TEMP)

Within the TEMP, the critical operational issues for suitability or survivability are usually appropriate to address spectrum supportability and E3 control requirements. The overall goals of the test program with respect to spectrum supportability and E3 control requirements are to ensure that appropriate evaluations are conducted during developmental test and evaluation, and that appropriate assessments are performed during operational test and evaluation. These evaluations and assessments should define the performance and operational limitations and vulnerabilities of spectrum supportability and E3 control requirements. See sections 9.9.3. and 9.9.5 for details.

Sample Language. The following are four examples of critical operational issues statements in the TEMP:

- Will the platform/system (or subsystem/equipment) detect the threat in a combat environment at adequate range to allow a successful mission? (Note: In this example, the "combat environment" includes the operational electromagnetic environment.)
- Will the system be safe to operate in a combat environment? (Note: In this example, electromagnetic radiation hazards issues such as hazards of electromagnetic radiation to personnel, ordnance, and volatile materials and fuels can be addressed, as applicable.)
- Can the platform/system (or subsystem/equipment) accomplish its critical missions? (Note: This example determines if the item can function properly without degradation to or from other items in the electromagnetic environment.)
- Is the platform/system (or subsystem/equipment) ready for Joint and, if applicable, Combined operations? (Note: In this example, the item must be evaluated in the projected Joint and, if applicable, Combined operational electromagnetic environment.)

7.6.3.10. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in Performance Specifications

Although the use of E3 Control Requirements extracted from Military Standards (MIL-STD) 461 and 464A and Military Handbook (MIL-HDBK) 237C is not mandatory, these three documents provide crucial guidance that, if followed, should preclude E3 problems with the critical systems provided to the warfighter.

Performance specifications should invoke spectrum supportability and E3 control requirements. MIL-STD-461, which defines E3 control (emission and susceptibility) requirements for equipment and subsystems, and MIL-STD-464A, which defines E3 control requirements for airborne, sea, space, and ground platforms/systems, including associated ordnance, can be used as references. Ordnance includes weapons, rockets, explosives, electrically initiated devices, electro-explosive devices, squibs, flares, igniters, explosive bolts, electric primed cartridges, destructive devices, and jet-assisted take-off bottles.

Sample Language. The following examples address E3 control in subsystem/equipment performance specifications:

> *Electromagnetic Interference (EMI) Control. "The equipment shall comply with the applicable requirements of MIL-STD-461"*
>
> *Electromagnetic Interference (EMI) Test. "The equipment shall be tested in accordance with the applicable test procedures of MIL-STD-461"*

As an alternative, the program manger can tailor system-level E3 control requirements from MIL-STD-461 or MIL-STD-464. Both MIL-STD-461 and MIL-STD-464 are interface specifications. See section 9.9.3. for testing standards and guidance from Director, Operational Test & Evaluation and Development Test and Evaluation. See section 9.9.5. for mandatory and non-mandatory use of DoD Single Stock Point for Specifications and Standards/MILSPEC reform homepage.

7.6.3.11. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in the Statement of Work (SOW)

The following is an example SOW statement to address spectrum supportability and E3 control requirements:

> *The contractor shall design, develop, integrate, and qualify the system such that it meets spectrum supportability and E3 control requirements of the system specification. The contractor shall perform analyses, studies, and testing to establish spectrum supportability and E3 control requirements and features to be implemented in the design of the item. The contractor shall perform inspections, analyses, and tests, as necessary, to verify that the system meets its spectrum supportability and E3 control requirements. The contractor shall prepare and update the DD Form 1494 throughout the development of the system for spectrum dependent equipment and shall perform analysis and testing to characterize the equipment, where necessary. The contractor shall establish and support a spectrum supportability and E3 control requirements Working-level Integrated Product Team (WIPT) to accomplish these tasks. MIL-HDBK-237 may be used for guidance.*

7.6.3.12. Data Item Requirements for Spectrum Supportability and Electromagnetic Environmental Effects (E3) Control Requirements in the Contract Data Requirements List (CDRL)

The following are examples of data item requirements typically called out for spectrum supportability and E3 control requirements in the CDRL:

- DI-EMCS-80199B EMI [Electromagnetic Interference] Control Procedures
- DI-EMCS-80201B EMI Test Procedures
- DI-EMCS-80200B EMI Test Report
- DI-EMCS-81540 E3 Integration and Analysis Report

- DI-EMCS-81541 E3 Verification Procedures
- DI-EMCS-81542 E3 Verification Report
- DI-MISC-81174 Frequency Allocation Data

7.6.4. Spectrum Supportability and Electromagnetic Environmental Effects (E3) Summary

7.6.4.1. Spectrum Supportability

Spectrum certification effects spectrum supportability. The program manager should initiate the spectrum certification process, to ensure spectrum supportability, early in the acquisition cycle.

The purpose of spectrum certification is to:

- Obtain authorization from the National Telecommunications and Information Administration to develop or procure items that use a defined frequency band(s) or specified frequencies to accommodate a specific electronic function(s);
- Ensure compliance with national policies and allocation tables which provide order in the use of the radio frequency spectrum; and
- Ensure spectrum availability to support the item in its intended operational environment.

7.6.4.1.1. Process

A diagram depicting the Spectrum Certification Process is presented below in **Figure 7.6.4.1.1.1.** .

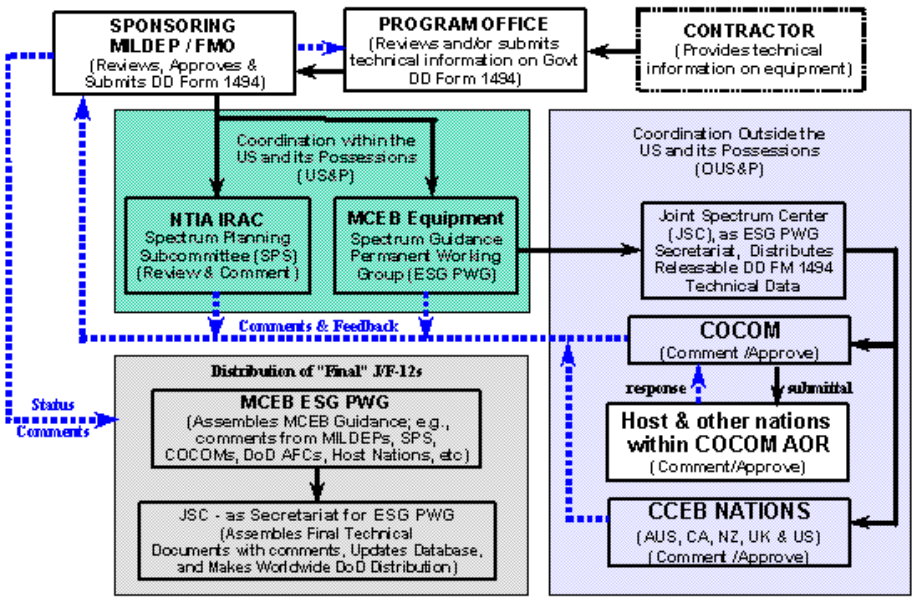

Figure 7.6.4.1.1.1. DoD Equipment Spectrum Certification Process

The Spectrum Certification Process is also called "Frequency Allocation" or the "JF-12 Process." The Program Manager submits DD Form 1494, "Application for Equipment Frequency Allocation," to obtain spectrum certification.

- The DD Form 1494 documents the spectrum-related technical and performance characteristics of an acquisition item to ensure compliance with the applicable DoD, individual national, both U.S. and foreign, and international spectrum management policies and regulations.
- The DD Form 1494 is routed through command channels to the sponsoring Military Department Frequency Management Office: the U.S. Army Spectrum Management Office, the Navy-Marine Corps Spectrum Center, or the Air Force Frequency Management Agency. The Military Department Frequency Management Office then submits the form simultaneously or as required to:
    - The Spectrum Planning Subcommittee of the Interdepartmental Radio Advisory Committee under the National Telecommunications and Information Administration and
    - The Equipment Spectrum Guidance Permanent Working Group under the Frequency Panel of the Joint Staff Military Communications-Electronics Board.

Spectrum Certification within the United States and Its Possessions. The National Telecommunications and Information Administration Spectrum Planning Subcommittee provides a national level review and approval for the DD Form 1494.

Department of Defense Internal Review. Within the Department of Defense, the Equipment Spectrum Guidance Permanent Working Group is responsible for the overall review, coordination and processing of all DoD frequency allocation applications. Within the Equipment Spectrum Guidance Permanent Working Group (formerly called the J-12 Permanent Working Group) the DD Form 1494 receives a tracking number (e.g., J/F-12/XXXX) and is reviewed by the other Military Department Frequency Management Office representatives. The Equipment Spectrum Guidance Permanent Working Group then sends the DD Form 1494 to other entities throughout the Department of Defense for review and comment. The Equipment Spectrum Guidance Permanent Working Group prepares the final J/F-12/XXXX for Military Communications-Electronics Board approval after all internal and external (e.g., National Telecommunications and Information Administration and/or Host Nation(s)) review and coordination has occurred.

Spectrum Certification outside the United States and Its Possessions. Any information intended to be released to a foreign nation must be approved for release by the appropriate DoD Component authority. Once a J/F-12 is approved for release to foreign nations and forums, it is then coordinated through the appropriate Combatant Command or other appropriate military offices, such as a Defense Attaché Office or Military Assistance Group office, with the foreign countries (also called "Host Nations") that have been identified as projected operating locations for the particular equipment. Since Host Nation coordination can be a lengthy and difficult process, the Program Manager should only list those nations on the DD Form 1494 in which permanent deployment is planned.

Per Office of Management and Budget Circular A-11, Part 2, program managers must heed the advice provided by National Telecommunications and Information Administration. In addition, program managers should follow guidance provided by foreign governments (i.e., host nation comments provided in response to the request to coordinate on a J/F-12) and implement suggested changes even if testing and/or operation is intended to occur within the United States but eventual deployment and operation is intended or desired for that host nation.

7.6.4.1.2. Note-to-Holders Mechanism

A "Note-to-Holder" is a mechanism provided within the spectrum certification process to permit minor changes to existing spectrum certification documentation in lieu of generating a completely new, separate application. The types of modifications permitted include:

- Adding the nomenclatures(s) of equipment which have essentially identical technical and operating characteristics as a currently allocated item,
- Adding comments that have been provided by the National Telecommunications Information Administration or host nations,

- Documenting minor modifications, or improvements to equipment that do not essentially alter the operating characteristics (transmission, reception, frequency response), or
- Announcing the cancellation or reinstatement of a frequency allocation.

A Note-to-Holders can be initiated by contacting the appropriate Military Department Frequency Management Office.

7.6.4.1.3. Frequency Assignment

Frequency assignments are issued by designated authorities of sovereign nations, such as telecommunications agencies within foreign countries, and the National Telecommunications and Information Administration for the United States and Its Possessions. Under certain conditions, other designated authorities, such as DoD Area Frequency Coordinators or Unified and Specified Commanders may grant frequency assignments. Equipment that has not been previously granted some level of spectrum certification will normally not receive a frequency assignment. Procedures for obtaining frequency assignments, once the equipment, sub-system, or equipment has become operational, are delineated in regulations issued by the Unified and Specified Commands and/or Military Services.

In most cases, the operational frequency assignments are requested and received after a program has been fielded. However, if the Program Manager has implemented guidance received in response to the submission of a DD Form 1494 during program development (e.g., incorporation of spectrum supportability comments) and designed the system as described in the DD Form 1494, system operators have not historically encountered problems in obtaining operational frequency assignments. Note: Spectrum congestion, competing systems, and interoperability, all may contribute to the operator encountering some operational limitations such as geographical restrictions or limitations to transmitted power, antenna height and gain, bandwidth or total number of frequencies made available, etc. Certification to operate in a particular frequency band does not guarantee that the requested frequency(ies) will be available to satisfy the system's operational spectrum requirements over its life cycle.

7.6.4.2. Electromagnetic Environmental Effects (E3)

7.6.4.2.1. Objective for E3 Control

The objective of establishing E3 control requirements in the acquisition process is to ensure that DoD equipment, subsystems, and systems are designed to be self-compatible and operate compatibly in the operational electromagnetic environment. To be effective, the program manager should establish E3 control requirements early in the acquisition process to ensure compatibility with co-located equipment, subsystems, and equipment, and with the applicable external electromagnetic environment.

7.6.4.2.2. Impacts When E3 Control Is Not Considered

It is critical that all electrical and electronic equipment be designed to be fully compatible in the intended operational electromagnetic environment. The Department of Defense

has experience with items developed without adequately addressing E3. Results include poor performance, disrupted communications, reduced radar range, and loss of control of guided weapons. Failure to consider E3 can result in mission failure, damage to high-value assets, and loss of human life. Compounding the problem, there is increased competition for the use of the spectrum by DoD, non-DoD Government, and civilian sector users; and many portions of the electromagnetic spectrum are already congested with electromagnetic-dependent items. In addition, new platforms/systems and subsystems/equipment are more complex, more sensitive, and often use higher power levels. All of these factors underscore the importance of addressing E3 control requirements early in the acquisition process.

7.6.4.3. Additional Resources

Spectrum management related information is available on the Joint Spectrum Center website. Spectrum compliance is a special interest area on the Acquisition Community Connection website.

7.6.5. Definitions

Key terms pertaining to spectrum supportability and electromagnetic compatibility processes are defined below.

Electromagnetic (EM) Spectrum. The range of frequencies of EM radiation from zero to infinity. For the purposes of this guide, "electromagnetic spectrum" shall be defined to be the range of frequencies of EM radiation that has been allocated for specified services under the U.S. and international tables of frequency allocation, together with the EM spectrum outside the allocated frequency range where use of unallocated frequencies could cause harmful interference with the operation of any services within the allocated frequency range. The terms "electromagnetic spectrum," "radio frequency spectrum," and "spectrum" shall be synonymous.

Electromagnetic Compatibility (EMC). The ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.

Electromagnetic Environment (EME). The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. EME is the sum of electromagnetic interference, electromagnetic pulse, hazards of electromagnetic radiation to personnel, ordnance, and volatile materials, and natural phenomena effects of lightning and precipitation static.

Electromagnetic Environmental Effects (E3). The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic

compatibility (EMC) and electromagnetic interference (EMI); electromagnetic vulnerability (EMV); electromagnetic pulse (EMP);electrostatic discharge, hazards of electromagnetic radiation to personnel (HEMP), ordnance (HERO), and volatile materials (HERF); and natural phenomena effects of lightning and precipitation static (P-Static).

Equipment Spectrum Certification. The statement(s) of adequacy received from authorities of sovereign nations after their review of the technical characteristics of a spectrum-dependent equipment or system regarding compliance with their national spectrum management policy, allocations, regulations, and technical standards. Equipment Spectrum Certification is alternately called "spectrum certification. Note: Within the United States and Its Possessions the requirement for certification of DoD spectrum-dependent equipment is prescribed by OMB Circular A-11, Part 2, and Title 47, CFR, Chapter III, Part 300 (the National Telecommunications and Information Administration "Manual of Regulations and Procedures for Federal Radio Frequency Management) and also applies to all equipment or systems employing satellite techniques.

Host Nations (HNs). Those sovereign nations, including the United States, in which the Department of Defense plans or is likely to conduct military operations with the permission of that nation.

Spectrum Management. The planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference

Spectrum Supportability. The assessment as to whether the electromagnetic spectrum necessary to support the operation of a spectrum-dependent equipment or system during its expected life cycle is, or will be, available (that is, from system development, through developmental and operational testing, to actual operation in the electromagnetic environment). The assessment of "spectrum supportability" requires, at a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation from HNs, and a consideration of EMC. (Note: While an actual determination of spectrum supportability for a spectrum-dependent system within a particular country (i.e., Host Nation) may be possible based upon "spectrum supportability" (e.g., equipment spectrum certification) comments provided by that host nation, the overall determination of whether a spectrum-dependent system has spectrum supportability is the responsibility of the Milestone Decision Authority based upon the totality of spectrum supportability comments returned from those host nations whose comments were solicited.)

Spectrum-Dependent Systems. Those electronic systems, subsystems, devices and/or equipment that depend on the use of the electromagnetic spectrum for the acquisition or acceptance, processing, storage, display, analysis, protection, disposition, and transfer of information.

7.7 Business Modernization Management Program

7.7.1 The Business Modernization Management Program (BMMP)

In addition to the Global Information Grid (GIG)-related programs, the Business Modernization Management Program (BMMP) and its associated Business Enterprise Architecture (BEA) are important to the DoD business domains, their functional proponents, and program managers who are acquiring capabilities for those domains. The Secretary of Defense established the BMMP to provide policy, strategic planning, oversight, and guidance for the Department's BMMP transformation efforts.

The BEA and Transition Plan were approved by the USD(C) in April 2003. The BEA is an extension of the GIG Architecture and is in conformance with the overall GIG Architecture. The BEA extension is a "to-be" architecture: it describes the DoD Business Enterprise of the future and represents a framework of requirements for transforming DoD and business processes. Due to the GIG conformance with the Federal Enterprise Architecture (FEA), programs compliant with the BEA are deemed compliant with the FEA.

See the BMMP Home Page for detailed information regarding the BMMP and the BEA. Program managers should become familiar with the website, including the following information:

(1) Secretary of Defense memorandum, July 19, 2001, establishing the BMMP program (initially called the Financial Management Modernization Program);

(2) Key information about each of the Business Domains; and

(3) USD(C) memoranda establishing guidelines on when and how to obtain USD(C) certification or approval for proposed acquisitions of, or improvements in, Financial Management systems.

(4) USD(C) memorandum, July 16, 2004, expanding the Comptroller certification requirements to include non-financial business systems.

(Note: DoD Instruction 5000.2 captures the requirements that flow from statute and from implementing Comptroller memoranda. These requirements are summarized below under "Mandatory Policies.")

7.7.2. Mandatory Policies

DoD Instruction 5000.2, Operation of the Defense Acquisition System

Section E4.2.8 requires the USD(C) to certify that financial management MAIS acquisition programs comply with the requirements of the BMMP and BEA before the Milestone Decision Authority grants any milestone or full-rate production approval.

Section E4.2.9 states that before a DoD Component can obligate more than $1,000,000 for a defense financial system improvement (i.e., a new, or modification of, a budgetary, accounting, finance, enterprise resource planning, or mixed (financial and non-financial) information system), the USD(C) must determine and certify that the system is being developed or modified, and acquired and managed in a manner that is consistent with

both the BEA and the BMMP Transition Plan. Furthermore, the USD(C) will certify the program to the Milestone Decision Authority before the Milestone Decision Authority gives any milestone or full-rate production approval (or their equivalent).

7.7.3. Integration within the Acquisition Process

The following categories of systems and system initiatives require USD(C) approval before obligation of funds or, when required, milestone approval:

a) All financial management, mixed and non-financial business system initiatives with projected pre-Milestone A (or equivalent) costs greater than $1,000,000.

b) All financial management, mixed and non-financial business systems currently in development, with program costs greater than $1,000,000 and requiring a Milestone A, Milestone B, Milestone C, Full Rate Production, or fielding decision, or requesting a change to approved functional or technical baselines.

c) All financial management, mixed and non-financial systems in sustainment with costs of greater than $1,000,000 for upgrades or enhancements.

For the approvals defined above, the following generic process describes steps that program managers, Domains, BMSI and the USD(Comptroller) will follow to review and approve requests. For acquisition programs, these steps should be accomplished using the Joint Capabilities Integration and Development System and the acquisition process, including appropriate Functional Capabilities Boards (FCBs), WIPTs, IIPTs, OIPTs and Information Technology Acquisition Board (ITAB) meetings. BMMP-related issues identified in the process will be resolved through the IPT process. For MAIS and Milestone Decision AuthorityPs, when an OIPT recommends that a program is ready to proceed for Milestone Decision Authority approval as a result of meeting all requirements, including those encompassed by the BMMP, the USD(C) will provide BMMP certification of the program as soon as possible, but not later than the ITAB meeting. For programs below the scope of MAIS or MDAP, follow Domain and Comptroller procedures.

1. Contact the lead Business Domain for the system improvement.

2. If the Lead and Partner Business Domains support initiation of the project based on an initial portfolio management review, they will provide the program manager a package containing the related Business Domains' and OUSD(C) compliance assessment requirements, including the unique requirements based on the program's business capabilities. The requestor completes the program assessment of (1) architecture and programmatic information required by the BMMP Comptroller Compliance Certification Criteria and the applicable Domain(s) unique compliance assessment requirements, and (2) an evaluation of the program's proposed implementation plan against Component, and BMMP transition plans to ensure compatibility.

3. The Lead Business Domain, in coordination with applicable Partner Domains, reviews and validates the documentation for consistency with the Department's/Domain's business processes and management objectives. Based on this review, the Lead Business Domain will determine one of the following:

- The program/initiative is compliant and there are no compliance issues;
- The program/initiative is compliant but not required since duplicate of other initiatives;
- The program/initiative is non-compliant but acceptable because the Domain(s) determine that mitigations exist to resolve identified issues; or
- The program/initiative is non-compliant, and the Domain(s) will not certify based on non-compliance with BEA/Domain architectures, transition plans, incomplete documentation, or unacceptable issue resolution/mitigation.

4. After coordination and content concurrence between the Business Domains, the Lead Domain forwards the certification package to the BMSI Program Office for evaluation.

5. BMSI, working in consultation with the Domains, reviews the certification package to ensure that it is complete, addresses cross-domain impacts, and supports the Department's enterprise business objectives.

6. BMSI provides a recommendation memorandum, through the Deputy Chief Financial Officer, to the USD (Comptroller) to approve or deny the Program/Initiative. (If BMSI does not recommend certification, BMSI will work with the applicable Domain Owner to resolve issues.)

7.7.4. Comptroller Compliance Certification Criteria

The Comptroller Compliance Certification Criteria are 26 questions that were approved by the BMMP Steering Committee. Certification Decision Packages submitted to obtain USD(C) approval must include the answers to these questions. The answers are generally originated by the program office or the functional proponent within the DoD Component, are validated by the Lead and Partner Business Domain(s), and results of their evaluation are submitted to the BMSI as part of the Certification Decision Package. Examples of the 26 questions include 14 general questions on the program (e.g., Component owner, Program Manager, User Base, Acquisition Type), compliance status with various DoD and Congressional Mandates (e.g., Clinger-Cohen Act and DoD Information Technology Security Certification and Accreditation Process (DITSCAP)), transition planning (interfacing and sunsetting systems and dates), and the Business Domain(s) evaluation of soundness of the program (the economic analysis results and compliance with the BEA and Domain architectures). The 26 questions are available through a link to the BMMP Portal (available by .mil or .gov only) on the System Compliance tab of the BMMP Home Page. A user ID and password are required to access the portal and can be obtained by registering online.

7.7.5. Definitions

The following definitions are taken from the Office of Management and Budget Circular A-127 Revised:

The term " financial system" means an information system, comprised of one or more applications, that is used for any of the following:

- collecting, processing, maintaining, transmitting, and reporting data about financial events;
- supporting financial planning or budgeting activities;
- accumulating and reporting cost information; or
- supporting the preparation of financial statements.

A financial system supports the financial functions required to track financial events, provide financial information significant to the financial management of the agency, and/or required for the preparation of financial statements. A financial system encompasses automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. A financial system may include multiple applications that are integrated through a common database or are electronically interfaced, as necessary, to meet defined data and processing requirements.

The term " non-financial system" means an information system that supports non-financial functions of the Federal government or components thereof and any financial data included in the system are insignificant to agency financial management and/or not required for the preparation of financial statements.

The term " mixed system" means an information system that supports both financial and non-financial functions of the Federal government or components thereof.

The term " financial management systems" means the financial systems and the financial portions of mixed systems necessary to support financial management.

7.8. Clinger - Cohen Act

7.8.1. The Clinger Cohen Act

7.8.1.1. Purpose

This section assists program managers, domain managers and members of the joint staff to understand and comply with the Clinger Cohen Act (CCA). This section is organized into the key requirements of CCA that must be met in order to receive milestone approval. For a more detailed background and comprehensive guidance, please access the CCA Community of Practice.

7.8.1.2. CCA Background

The Information Technology Management Reform Act, now known as the Clinger-Cohen Act of 1996, is designed to improve the way the Federal Government acquires and manages information technology. It requires the Department and individual programs to use performance based management principles for acquiring information technology (IT), including National Security Systems (NSS).

The CCA generated a number of significant changes in the roles and responsibilities of various Federal agencies in managing acquisition of IT, including NSS; it elevated oversight responsibility to the Director, OMB, and established and gave oversight responsibilities to the departmental CIO offices. In DoD, the ASD(NII) has been designated as the DoD CIO and provides management and oversight of all DoD information technology, including national security systems.

7.8.1.3. Definitions

The term "information technology" with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

The term "National Security System" (NSS) means any telecommunications or information system operated by the United States Government, the function, operation, or use of which, (a) involves intelligence activities; (b) involves cryptologic activities related to national security; (c) involves command and control of military forces; (d) involves equipment that is an integral part of a weapon or weapons system; or (e) is critical to the direct fulfillment of military or intelligence missions.

7.8.2. Mandatory Policies

Table 7.8.2.1. details CCA Compliance regulatory requirements, mandatory DoD policy and the applicable program documentation that can be used to fulfill the requirement. This table instantiates information from the DoD Instruction 5000.2 CCA Compliance Table (Table E4.T1), reorders the content to provide for a more logical flow, and adds columns relating applicable milestones and regulatory guidance with each of the requirements.

To navigate via hyperlinks, go to the CCA Requirements table below and select the appropriate hyperlink to get to guidance information. Some CCA requirements are discussed only briefly, and then are hyperlinked to a more complete discussion. Additionally, some of the more detailed requirements will have links to the CCA Community of Practice website which provides more comprehensive understanding of the CCA requirements, their rationale, the associated policy documents, best practices, and lessons learned.

Paragraphs following the table will describe each requirement. Some paragraphs will identify who is responsible for fulfilling and reviewing the requirement, and suggest how the requirement is to be fulfilled. Others will briefly describe the requirement and provide a link to a detailed discussion contained elsewhere.

Note that the requirements in the CCA Compliance Table (E4.T1) in DoD Instruction 5000.2 and Table 7.8.2.1. must be satisfied before milestone approval of any Acquisition Category I and IA program and prior to the award of any contract for the acquisition of a Mission-Critical or Mission-Essential Information Technology system, at any level.

Requirements From the DoDI 5000.2 Clinger-Cohen Act (CCA) of 1996 Table (DoDI Table E4.T1.)			
Information Requirements	**Applicable Program Documentation ****	**Applicable Milestone ******	**Regulatory Requirement**
***Make a determination that the acquisition supports core, priority functions of the Department	Initial Capabilities Document Approval	Milestone A	CJCSI 3170.01
*No Private Sector or Government source can better support the function	AoA(FSA) page XX Acquisition Strategy page XX, para XX	Milestone A & B	CJCSI 3170.01 DoDI 5000.2
***Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology	Approval of the Initial Capabilities Document, Concept of Operations, AoA (FSA), Capability Development Document, and CPD	Milestone A & B	CJCSI 3170.01 DoDI 5000.2
*An analysis of alternatives has been conducted	AoA (FSA)	Milestone A	CJCSI 3170.01 DoDI 5000.2
*An economic analysis has been conducted that includes a calculation of the return on investment; or for non-AIS programs, a Lifecycle Cost Estimate (LCCE) has been conducted	Program LCCE Program Economic Analysis for MAIS	For MAIS: Milestone A & B, & FRPDR (or their equivalent) For non-MAIS: Milestone B or the first Milestone that authorizes contract award	DoDI 5000.2
***Establish outcome-based performance measures linked to strategic goals.	Initial Capabilities Document, Capability Development Document, CPD and APB approval	Milestone A & B	CJCSI 3170.01 DoDI 5000.2
There are clearly established measures and accountability for program progress	Acquisition Strategy page XX APB	Milestone B	DoDI 5000.2
The acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards	Initial Capabilities Document, Capability Development Document, & APB (NR-KPP) ISP (Information Exchange Requirements)	Milestone A, B & C	CJCSI 6212.01 DoDI 5000.2
The program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards	Information Assurance Strategy	Milestone A, B, C, FRPDR or equivalent*****	DoDI 5000.2 DoDD 8500.1
To the maximum extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future increments	Acquisition Strategy page XX	Milestone B or the first Milestone that authorizes contract award	DoDI 5000.2
The system being acquired is registered	Registration Database	Milestone B, Update as required	DoDI 5000.2

Table 7.8.2.1. Requirements from DoD Instruction 5000.2, Table E4.T1., CCA Compliance Table

* For weapons systems and command and control systems, these requirements apply to the extent practicable (40 U.S.C. 1451)

** The system documents/information cited are examples of the most likely but not the only references for the required information. If other references are more appropriate, they may be used in addition to or instead of those cited.

***These requirements are presumed to be satisfied for Weapons Systems with embedded IT and for Command and Control Systems that are not themselves IT systems

**** The purpose of the "Applicable Milestone" column in the table above is to indicate at which Milestone(s) the initial determination should be made regarding each element of Clinger-Cohen Act implementation. For MAIS programs, the DoD CIO must certify CCA compliance before granting approval for Milestone A or B or the Full-Rate Deployment decision (or their equivalent).

***** No contract for the acquisition of a Mission Critical or Mission Essential IT system may be awarded until the DoD CIO has determined that there is in place for the system an appropriate information assurance strategy.

Two other CCA-related topics not addressed in the CCA table in DoDI Instruction 5000.2 are Post-Implementation Review (PIR)/Post Deployment Performance Review (PDPR) and CCA certifications and notifications to Congress required by Section 8084(c) of the Appropriations Act for FY 2004 (Public Law 108-87).

See section 7.9 of this Guidebook for a discussion of PIR/PDPR.

See section 7.8.3.12 of this Guidebook for a discussion of certifications and notification required by Section 8084(c) of the Appropriations Act for FY 2004 (Public Law 108-87).

See section 7.8.3.12 of this Guidebook for a discussion of certifications and notification required by Section 8084(c) of the Appropriations Act for FY 2004 (Public Law 108-87).

7.8.3. Guidance for Complying with the CCA

This section details guidance associated with the CCA Information Requirements listed above. Each section provides an overview of the requirement. Some sections will provide additional guidance about the requirement, while other sections will have links to additional guidance contained in other parts of this Guidebook or to other resources located elsewhere on the web.

7.8.3.1. Determining that the Acquisition Supports the Core, Priority Functions of the Department

Overview: This element of the CCA asks if the function supported by a proposed acquisition is something the Federal government actually needs to perform; i.e., for DoD, is the function one that we (the DoD and/or its Components) must perform to accomplish the military missions or business processes of the Department?

For DoD, this question is answered in the Joint Capabilities Integration and Development System process. Before a functional requirement or new capability enters the acquisition process, the Joint Capabilities Integration and Development System process (See CJCSM 3170.01, Enclosure A) requires the sponsor to conduct a series of analyses (i.e., the Functional Area Analysis, Function Needs Analysis and Functional Solution Analysis). These analyses are normally completed before preparing an Initial Capabilities Document

(ICD). Ideally, these analyses will show that the acquisition supports core/priority functions that should be performed by the Federal Government. Moreover, the analysis should validate and document the rationale supporting the relationship between the Department's mission (i.e., core/priority functions) and the function supported by the acquisition.

Who is Responsible? The Sponsor/Domain Owner with cognizance over the function leads the analysis work as part of the Joint Capabilities Integration and Development System process.

Implementation Guidance: Ensure that the Joint Capabilities Integration and Development System analytical work addresses the CCA question by establishing the linkage between the mission, the function supported, the capability gap and potential solutions. The following questions should be helpful in determining whether a program supports DoD core functions:

Does the program support DoD core/primary functions as documented in national strategies and DoD mission and strategy documents like the Quadrennial Defense Review (QDR), Strategic Planning Guidance (SPG), Joint Operating Concepts (JOC), Joint Functional Concepts (JFC), Integrated Architectures (as available), the Universal Joint Task List (UJTL), domain mission statements, or Service mission statements?

Does Joint Capabilities Integration and Development System (i.e., FAA/FNA/FSA) validate that the function needs to be performed by the Government?

Is the program consistent with the goals, objectives, and measures of performance in the lead Sponsor/Domain owner's Functional Strategic Plan?

7.8.3.2. Determining That No Private Sector or Other Government Source Can Better Support the Function

Overview: This element of the CCA asks if any private sector or other government source can better support the function. This is commonly referred to as the "outsourcing determination." The Sponsor/Domain Owner determines that the acquisition MUST be undertaken by DoD because there is no alternative source that can support the function more effectively or at less cost. Note that for weapon systems and for command and control systems, the need to make a determination that no private sector or Government source can better support the function only applies to the maximum extent practicable. This requirement should be presumed to be satisfied if the acquisition has a Milestone Decision Authority-approved acquisition strategy.

Who is Responsible:

The Sponsor/Domain Owner with cognizance over the function leads the analysis work as part of the AoA(FSA) process.

The program manager updates and documents the supporting analysis in the AoA and a summary of the outsourcing decision in the Acquisition Strategy.

7.8.3.3. Redesigning the Processes that the Acquisition Supports

Overview: This element of the CCA asks if the business process or mission function supported by the proposed acquisition has been designed for optimum effectiveness and efficiency. This is known as Business Process Reengineering (BPR) and is used to redesign the way work is done to improve performance in meeting the organization's mission while reducing costs. The CCA requires the DoD Component to analyze its mission, and based on the analysis, revise its mission-related processes and administrative processes as appropriate before making significant investments in IT. To satisfy this requirement, BPR is conducted before entering the acquisition process. However, when the results of the Joint Capabilities Integration and Development System analysis, including the Analysis of Alternatives, results in a Commercial-Off-The-Shelf (COTS) enterprise solution, additional BPR is conducted after program initiation, to reengineer an organization's retained processes to match available COTS processes. As stated in DoD Instruction 5000.2, for a weapon system with embedded information technology and for command and control systems that are not themselves IT systems, it shall be presumed that the processes that the system supports have been sufficiently redesigned if one of the following conditions exist: (1) the acquisition has a Joint Capabilities Integration and Development System document (Initial Capabilities Document, Capability Development Document or Capability Production Document) that has been approved by the Joint Requirements Oversight Council (JROC) or JROC designee, or (2) the Milestone Decision Authority determines that the Analysis of Alternatives (Functional Solution Analysis) is sufficient to support the initial Milestone decision."

Who is Responsible:

- The Sponsor/Domain Owner with cognizance over the function with input from the corresponding DoD Component functional is responsible for BPR.
- The program manager should be aware of the results of the BPR process and should use the goals of the reengineered process to shape the acquisition.
- The OSD PA&E assesses an Acquisition Category IAM program's Analysis of Alternatives/Functional Solution Analysis to determine the extent to which BPR has been conducted.
- The DoD CIO assesses an Acquisition Category IAM program's Analysis of Alternatives/Functional Solution Analysis to determine whether sufficient BPR has been conducted.

Business Process Reengineering: Benchmarking

Benchmarking is necessary for outcome selection and business process reengineering (BPR). The Sponsor/Domain Owner should quantitatively benchmark agency outcome performance against comparable outcomes in the public or private sectors in terms of cost, speed, productivity, and quality of outputs and outcomes.

Benchmarking should occur in conjunction with a BPR implementation well before program initiation. Benchmarking can be broken into four primary phases:

- **Planning Phase** : Identify the product or process to be benchmarked and select the organizations to be used for comparison. Identify the type of benchmark

measurements and data to be gathered (both qualitative and quantitative data types). One method to gather data is through a questionnaire to the benchmarking organization that specifically addresses the area being benchmarked.

- **Data Collection and Analysis Phase** : Initiate the planned data collection, and analyze all aspects of the identified best practice or IT innovation to determine variations between the current and proposed products or processes. Compare the information for similarities and differences to identify improvement areas. Use root cause analysis to break the possible performance issues down until the primary cause of the gap is determined. This is where the current performance gap between the two benchmarking partners is determined.
- **Integration Phase** : Communicate the findings; establish goals and targets; and define a plan of action for change. This plan of action is often the key to successful BPR implementation. Qualitative data from a benchmarking analysis is especially valuable for this phase. It aids in working change management issues to bring about positive change.
- **Implementation Phase** : Initiate the plan of action and monitor the results. Continue to monitor the product or process that was benchmarked for improvement. Benchmark the process periodically to ensure the improvement is continuous.

EXAMPLE

The Military Health System PEO Joint Medical Information Systems Office was faced with increasing cost and decreasing performance in their 20+ call centers that service 8.3 million military healthcare beneficiaries. To understand the industry standards for call center performance, the PEO staff approached the Gartner Group and the benchmarking services offered by Brady and Associates, a hospital management consultancy. A comparison of the as-is cost and performance with the industry benchmarks suggested that a business case could be made to reengineer the Military Health System call center process and realize both improved service and a significant ROI.

Following completion of the business case, a competitive solicitation was made for consolidated call and help desk services. This would be a performance based services contract using performance measures developed from the benchmarking exercise. The award was made to IBM with incentivized performance metrics as shown in Table 18.

The contracting tool selected was a variation of a firm fixed price contract with established target and ceiling prices. Underruns below the target price and overruns between the target and ceiling price are shared in a ratio bid between the vendor and government. Of note is that this was the first such incentivized-shard risk contract based upon a GSA Schedule and now serves as a template for use by all government agencies.

The results of this reengineering have been dramatic. The consolidated call center is in San Antonio, Texas. Pre-consolidation cost for 20+ centers was $25M. The current cost is $10M per year and customer satisfaction for FY 03 was 98%.

Criteria	*Positive Incentive range*	*Acceptable range*	*Negative Incentive range*
Customer Satisfaction Survey Response Rate1	Above 18%	15 - 18 %	Below 15%
Customer Satisfaction1	Above 90%	85 - 90%	Below 85%
Call Abandonment Rate	Below 3%	3 - 5%	Above 5%
Average Speed of Answer (sec)	Below 20 sec.	20 – 30 sec.	Above 30 sec.
Problem Resolution Rate for **High Priority** problems/requests2	90 % within 60 minutes	89% within 90 min. *with hardware exception of 24 hour best effort repair/replace*	Greater than 90 min. for any problem
Problem Resolution Rate for **Moderate Priority** problems/requests2	75% within 4 hours	89% within in 6 hours *with hardware exception of 24 hour best effort repair/replace*	Greater than 6 hours for any problem
Problem Resolution Rate for **Low Priority** problems/requests2	50% with in 2 business days	89% with in 3 business days or less *with hardware exception of 24 hour best effort repair/replace*	Greater than 3 business days for any problem.
First Contact Resolution	Greater than 80%	64 to 80%	Less than 64%

Table 7.8.3.3.1. Consolidated Military Health System Calldesk Incentivized Performance Metrics

Additional BPR Resources:

- National Partnership for Reinventing Government Benchmarking site: http://govinfo.library.unt.edu/npr/initiati/benchmk/
- Best Manufacturing Practices site: http://www.bmpcoe.org/
- The Brady Group Call Center Benchmarking: http://bradyinc.com
- The Gartner Group: http://www4.gartner.com/Init
- BusinessRanks.com: http://www.businessranks.com

Implementation Guidance: BPR implementation guidance exists in both the private and public sector. In addition to the steps required to conduct a BPR, it is critical that the Sponsor/Domain Owners and Program Managers recognize change management as a key aspect of any successful BPR implementation. Two government sources recommended for BPR implementation guidance are the following:

1. The BPR Internet Resources Kiosk: The BPR Internet Resources Kiosk site provides a set of links to BPR education, tools, and implementation guidance for BPR implementations. It includes a link to the The DoD Process Innovation Site, which includes links to the Turbo BPR tool and the BPR Fundamentals course.

2. The General Accounting Office (GAO) BPR Guide: The GAO has developed a comprehensive framework for assessing BPR implementations that the Department of Defense can adopt to aid programs in conducting their BPR analysis. This framework involves three key parts <link>:

- Part A: Assessing the Agency's Decision to Pursue Reengineering:
- Part B: Assessing New Process Development
- Part C: Assessing Project Implementation and Results

7.8.3.4. Analysis of Alternatives (Functional Solutions Analysis)

Overview: The Office of the Director, Program Analysis and Evaluation (OD/PA&E), provides basic policies and guidance associated with the AoA process. For Acquisition Category ID and IAM programs, OD/PA&E prepares the initial AoA guidance, reviews the AoA analysis plan, and reviews the final analysis products (briefing and report). After the review of the final products, OD/PA&E provides an independent assessment to the milestone decision authority (see DoD Instruction 5000.2, Enclosure 6,E.6.5). See section 3.3 of this guide for a general description of the AoA and the AoA Study Plan.

7.8.3.5. Economic Analysis and Lifecycle Cost Estimates

Overview: An Economic Analysis consists of a Lifecycle cost and benefits analysis and is a systematic approach to selecting the most efficient and cost effective strategy for satisfying an agency's need. See sections 3.6 and 3.7 of this guide for detailed EA and LCCE guidance.

7.8.3.6. Establish Outcome-based Performance Measures

Overview: The CCA requires the use of performance and results-based management in planning and acquiring investments in information technology, including national security systems (IT, including NSS). This section defines measurement terminology, relates it to DoD policy and provides guidance on formulating effective outcome-based performance measures for IT, including NSS investments. As stated in DoDI 5000.2, for a weapon system with embedded information technology and for command control systems that are not themselves IT systems, it shall be presumed that the acquisition has outcome-based performance measures linked to strategic goals if the acquisition has a Joint Capabilities Integration and Development System document (ICD, Capability Development Document or CPD) that has been approved by the JROC or JROC designee.

IT, including NSS outcome-based performance measures are also referred to as measures of effectiveness (MOEs). For clarification, the various uses and DoD definitions of MOEs are provided on the CCA Community of Practice. Regardless of the term used, the Clinger Cohen Act states that the respective Service Secretaries shall:

- Establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the public through the effective use of information technology.
- Ensure that performance measurements are prescribed for information technology programs used by or to be acquired for the executive agency and that the performance measurements measure how well the information technology supports programs of the executive agency.

- Conduct post-implementation reviews of information systems to validate estimated benefits and document effective management practices for broader use.

In summary, we are obligated to state the desired outcome, develop and deploy the solution, and then measure the extent to which we have achieved the desired outcome. For further discussion, see the CCA language in page 24 of Office of Management and Budget Circular A-11, Part 7, Section 300, Exhibit 300, Part I, Section I.C. Additionally, discussions on the statutory basis and regulatory basis for MOEs and their verification are available.

Who is Responsible:

- The Sponsor/Domain Owner with cognizance over the function develops the MOEs as part of the Joint Capabilities Integration and Development System process. This individual should ensure the MOEs are outcome-based and relate to the outcomes identified as benefits in the benefits analysis.
- the program manager should be aware of the MOEs and how they relate to overall program effectiveness and document these MOEs in the Exhibit 300 that is part of DoD's budget submission to OMB.
- The DoD CIO assesses the outcome-based measures in deciding whether to certify CCA compliance for Acquisition Category IA programs.

Implementation Guidance: This section is written to help the functional proponent prepare the MOEs and to help the program managerO understand his/her role in the MOE refinement process. The key to understanding and writing MOEs for IT, including NSS investments is to recognize their characteristics and source. Therefore, MOEs should be:

- Written in terms of desired outcomes
- Quantifiable
- A measure of the degree to which the desired outcome is achieved
- Inclusive of both DoD Component and enterprise performance benefits
- Independent of any solution and should not specify system performance or criteria

To satisfy the requirement that an MOE be independent of any solution and not specify system performance or criteria, the MOE should be established before the Concept Decision that starts the acquisition process. The MOEs guide the analysis and selection of alternative solutions that are discussed in the AoA/FSA during pre-Milestone A. Although the MOE may be refined as a result of the analysis undertaken during this phase, the source of the initial mission/capability MOE is the functional community. The MOE is the common link between the Initial Capabilities Document, the AoA and the benefits analysis.

A primer for this section is found in the Performance Institute's Government Performance Logic Model. The Performance Institute is a private think tank that has developed a logical chain of events that they view as a blueprint for mission achievement. For further guidance on MOEs, see the Information Technology Community of Practice Measures of Effectiveness Area which contains the following additional guidance:

- Joint Capabilities Integration and Development System MOE Development Process
- BEA Domain MOE Development Process

7.8.3.7. Acquisition Performance Measures

Overview: Acquisition performance measures are clearly established measures and accountability for program progress. The essential acquisition measures are those found in the acquisition program baseline (APB): cost, schedule and performance. See section 2.1.1. of this guide for detailed APB guidance.

7.8.3.8. The acquisition is consistent with the Global Information Grid policies and architecture

Overview: The GIG is the organizing and transforming construct for managing information technology (IT) for the Department. See section 7.2, Global Information Grid (GIG), for a detailed guidance on GIG policies and architecture.

7.8.3.9. The program has an information assurance strategy that is consistent with DoD policies, standards and architectures

Overview: Information Assurance (IA) concerns information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection and reaction capabilities. See section 7.5 of this guide for detailed guidance on IA.

7.8.3.10. Modular Contracting

Overview: Under modular contracting, a system is acquired in successive acquisitions of interoperable increments. The CCA is concerned with modular contracting to ensure that each increment complies with common or commercially acceptable standards applicable to Information Technology (IT) so that the increments are compatible with the other increments of IT comprising the system.

Who is Responsible:

The program manager is responsible for ensuring that modular contracting principles are adhered to.

The contracting strategy is addressed in the Acquisition Strategy, which is approved by the Milestone Decision Authority and reviewed by all IIPT members.
Implementation Guidance: See section 4.5.4. of this guide for a discussion of Modular, Open Systems Approach as a systems engineering technique that will support modularity, and section 39.103 of the Federal Acquisition Regulations for a detailed discussion of Modular Contracting.

7.8.3.11. DoD Information Technology (IT) Registry

Overview: The DoD Information Technology Registry supports the CCA inventory requirements and the capital planning and investment processes of selection, control, and evaluation. The Registry contains a comprehensive inventory of the Department's

mission critical and mission essential national security systems and their interfaces. It is web-enabled to.mil users, and has classified and unclassified portions accessible through NIPRNET and SIPRNET. Department of Defense Information Technology (IT) Registry Policy Guidance for 2004, dated December 1, 2003 establishes Registry responsibilities to include update and maintenance of information in the Registry.

Who is Responsible: The Program Manager is responsible for ensuring the system is registered and should follow applicable Component CIO procedures and guidance.

IT Registry Update Procedure: The DoD Information Technology Registry uses a standard, documented procedure for updating its contents. Updates to the Registry are required on a quarterly basis. The rules, procedures, and protocols for the addition, deletion, and updating of system information are available to users once they are registered. Service and Agency CIOs confirm the accuracy of its contents on an annual basis.

Use of the IT Registry for Decision Making: The Registry has recently expanded its support to decision makers managing IT assets. In support of the Federal Information Systems Management Act and the Privacy Act additional fields have been added to the Registry. The Registry also supports the Comptroller's Business Management Modernization Program by providing baseline data on mission critical and mission essential financial systems. Service and Agency CIOs determine the addition or deletion of mission critical and essential systems based on mission needs and ongoing investment decisions.

7.8.3.12. CCA Certification for MAIS Systems

Overview: Section 8083(c) of the Appropriations Act for FY 2004 (Public Law 108-287) requires the Department of Defense (DoD) Chief Information Officer (CIO) to provide a notification of certification report at each acquisition milestone that Major Automated Information Systems (MAIS) are being developed in accordance with Subtitle III of Title 40 of the United States Code (Formally the CCA of 1996).

Who is Responsible:

- The Program Manager is responsible for developing the initial notification of certification report and then delivering it to their component CIO.
- The Component CIO is responsible for submitting the Section 8084(c) CCA certification report to the DoD CIO.
- The DoD CIO certifies MAIS program CCA compliance to the congressional defense committees at each acquisition milestone

Implementation Guidance: Each DoD Component CIO certification must be accompanied by a notification report that shall include:

- A statement that the MAIS is being developed in accordance with Clinger-Cohen Act of 1996

- The funding baseline (prior year and FY 2004 – 2007 including Operational and Maintenance; Procurement, and Research, Development, Test and Evaluation)
- The milestone schedule (denoting milestones and the dates for the milestones already attained, and for future milestones) for each MAIS
- A succinct and clear description of efforts to accomplish each of the following:
    - Business Process Reengineering.
    - An analysis of alternatives.
    - An economic analysis that includes a calculation of the return on investment.
    - Performance measures.
    - An information assurance strategy consistent with the Department's Global Information Grid.

The Section 8084(c) certification report is due from the DoD Component CIO to the DoD CIO at the time of milestone decision request. If a certification and notification report has been previously submitted for the program and if there has been no change regarding a particular issue, then the response for that issue should simply state that there has been no change from the previous submission.

7.9. Post Implementation Reviews

7.9.1. Background

The Government Performance and Results Act (GPRA) requires that Federal Agencies compare actual program results with established performance objectives. In addition, the Clinger-Cohen Act (CCA) requires that Federal Agencies ensure that performance measurements are prescribed for the information technology (IT) to be acquired, that these performance measurements measure how well the IT supports the programs of the Agency. (5 U.S.C. 306; 40 U.S.C. 11313)

DoD Instruction 5000.2, Table E3.T1., refers to this information requirement as a Post-Deployment Performance Review (PDPR) and requires a PDPR for MAIS and MDAP acquisition programs at the Full-Rate Production Decision Review. DoD Instruction 5000.2 cites both GPRA and the Clinger-Cohen Act as the basis for the requirement. An appropriately conducted PIR can satisfy both GPRA and CCA requirements for a post deployment evaluation.

In addition, the Office of Management and Budget (OMB) has prescribed specific procedures for measuring how well acquired IT supports Federal Agency programs. OMB Circular A-130 refers to this performance-measurement requirement for IT as a Post Implementation Review (PIR). An appropriately conducted PIR can satisfy both GPRA and CCA requirements for a post deployment evaluation.

As a result, within the Department of Defense, the PDPR and the PIR are essentially the same thing—they both assess actual system performance against program expectations.

To avoid confusion, the next change to DoDI 5000.2 will rename the PDPR. Since OMB Circular A-130 specifically calls the described performance assessment a PIR, the Instruction will use that term. DoDI 5000.2 will require the PIR for MAIS and MDAP programs. This section of Chapter 7 of the Defense Acquisition Guidebook will provide details of the expected information (to comply with statute) for any PIR.

In practice, a PDPR/PIR *Plan* will be required at the Full-Rate Production Decision Review, and the actual PIR will be conducted after IOC (if possible, before FOC).

Until the official DoDI 5000.2 change takes effect, the two terms, PDPR and PIR, may be used interchangeably. Both terms refer to the same process: the evaluation of how well actual program results have met established performance objectives for any acquisition program.

7.9.2. Overview

This section provides guidance on how to conduct a PIR for a system that has been fielded, and is operational in its intended environment. A PIR verifies the Measures of Effectiveness (MOEs) of the Initial Capabilities Document and answers the question, *"Did the Service/Agency get what it needed, per the Initial Capabilities Document, and if not, what should be done?*

Who is Responsible:

The Sponsor/Domain Owner is responsible for articulating outcome-based performance measures in the form of measures of effectiveness.

The Sponsor/Domain Owner is responsible for planning the PIR, gathering data, analyzing the data, and assessing the results.

the program manager is responsible for maintaining an integrated program schedule that facilitates the PIR on behalf of the Sponsor/Domain Owner.

the program manager is responsible for translating Sponsor/Domain Owner planning into specific PIR implementation events.

What is a PIR:

The PIR is not a single event or test. It is a sequence of activities that when combined, provide the necessary information to successfully compare actual system performance to program expectations. In some cases, these activities can take place over a long period of time. The list in Table 19 indicates that some PIR activities may be accomplished in the context of typical program acquisition activities or system operational processes.

•FOT&E Results	•Annual CFO Report
•Platform Readiness	•Mission Readiness
•CC Exercise	•ROI
•User Satisfaction	•War Games
•IA Assessments	•Lessons Learned

Table 7.9.2.1. Potential PIR Activities

7.9.3. PIR Within the Acquisition Life Cycle

The Sponsor/Domain Owner initially articulates high-level, outcome-based performance measures in the form of measures of effectiveness in the Initial Capabilities Document. Development of the Capability Development Document, CPD, contract, and build specifications follows, each providing increasingly detailed performance outcomes. During integration and test, procedures called out in the Systems Engineering Plan (SEP) should verify compliance with the build specification. The Test and Evaluation Master Plan (TEMP) and associated test products describe verification of compliance with the contract specification during developmental test and evaluation (DT&E) and verification of compliance with the CPD during operational test and evaluation (OT&E). Finally, the PIR benefits analysis evaluates system compliance with the original MOEs documented in the Initial Capabilities Document.

7.9.4. PIR Implications for Evolutionary Acquisition

PIRs provide important user feedback and consequently are a fundamental element of evolutionary acquisition. Optimally, we need to understand how well a recently

completed increment meets the needs of users before finalizing the requirements for a subsequent increment. The opportunity for such feedback depends on the level of concurrency in the schedule.

Additionally, changes in the environment may drive new requirements. The PIR gives both the Sponsor and the program manager empirical feedback to better understand any issues with the completed increment. This feedback enables the acquisition principals to adjust or correct the Capability Development Document/CPD for subsequent increments.

7.9.5. PIR Implementation Steps

1. Schedule the PIR. The PIR should take place post-IOC, after a relatively stable operating environment has been established. A typical time frame is 6 to 12 months after IOC.

2. Assemble a PIR Team. The PIR team should include:

- Functional experts with detailed knowledge of the capability or business area and its processes.
- User representatives, CIO representatives, functional sponsors, and Domain Owners.

3. Assemble and Review Available Information Sources. Data can be gleaned from operations conducted in wartime and during exercises. The lead-time for most major exercises is typically one year and requires familiarity with the exercise design and funding process. Additional sources to consider are:

- Economic calculations to establish the payback period and ROI of business systems (if applicable).
- Qualitative assessments related to expected benefits
- Combatant Commander operational, logistics, and exercise data
- Information Assurance assessments
- Annual CFO Reporting of IT investment measured performance
- Stakeholder satisfaction surveys

4. Conduct the PIR. The PIR should be carried out according to the PIR planning that was reviewed and approved at Full Rate Production Decision Review. Care should be given to ensuring that accurate raw data is captured, and it can be later used for analysis. Based on the PIR plan, the PIR should, at a minimum, address:

- Customer Satisfaction: Is the warfighter satisfied that the IT investment meets their needs?
- Mission/Program Impact: Did the implemented system achieve its intended impact?
- Return on investment calculations, if applicable. Compare actual project costs, benefits, risks, and return information against earlier projections. Determine the causes of any differences between planned and actual results.

5. Conduct the Analysis. The analysis portion of the PIR should answer the question, "Did we get what we needed?" This provides a contrast to the test and evaluation measurements of KPPs that answer the question, "Did we get what we asked for?" This would imply, if possible, that the PIR should assess the extent to which the DoD's investment decision-making processes were able to capture the warfighter's initial intent. The PIR should also address, if possible, whether the warfighter's needs changed during the time the system was being acquired.

The outputs of the analysis become the PIR findings. The findings should clearly identify the extent to which the warfighter got what they needed.

6. Prepare a Report and Provide Recommendations. Based on the PIR findings, the PIR team should prepare a report and make recommendations that can be fed back into the capabilities and business needs processes. The primary recipient of the PIR report should be the Sponsor/Domain Owner who articulated the original objectives and outcome-based performance measures on which the program or investment was based. The results of the PIR can aid in refining requirements for subsequent increments. Recommendations may be made to correct errors, improve user satisfaction, or improve system performance to better match warfighter/business needs. The PIR team should also determine whether different or more appropriate outcome-based performance measures can be developed to enhance the assessment of future spirals or similar IT investment projects.

For further guidance on PIRs, see the Information Technology Community of Practice Post Implementation Review Area. This contains the following additional guidance:

PIR Measurement Framework.

Common Problems with PIR Implementations.

7.9.6. PIR Further Reading

Both government and the commercial sector address the practice of conducting PIRs for materiel, including software and IT, investments. The GAO and several not-for-profit organizations have written on the subject of measuring performance and demonstrating results. The CCA Community of Practice PIR area lists a number of key public and private sector resources that can be used in planning and conducting a PIR.

7.10. Commercial, Off-the-Shelf, Software Solutions

7.10.1. The Impetus for Commercial, Off-the-Shelf (COTS) Solutions

- The goal of the President's Management Agendaand the Department's Quadrennial Defense Review (QDR) is rapid transformation by significantly increasing, where appropriate, the use of commercially available and proven business solutions in the conduct of DoD business.
- One of the Department's goals is to migrate to COTS solutions to fill Information Technology capability gaps.
- The Clinger-Cohen Act of 1996, DoD Instruction 5000.2, Sections 3.5.3. and 3.6.4., and Management Initiative Decision (MID) 905, "Net-Centric Business Transformation and E-Government," all require the use of COTS Information Technology solutions to the maximum practical extent.

7.10.2. Definition

> *Commercial Off-the-Shelf (COTS) is defined as "commercial items that require no unique government modifications or maintenance over the life cycle of the product to meet the needs of the procuring agency."*

[From the Eleventh Edition of GLOSSARY: Defense Acquisition Acronyms and Terms.]

7.10.3. Mandatory Policies

The following bullets quote or paraphrase sections in the DoD 5000 series that specifically address Commercial Off-the-Shelf (COTS):

DoD Directive 5000.1, Section E1.18., states the following:

> "… The DoD Components shall work with users to define capability needs that facilitate the following, listed in descending order of preference:
>
> E1.18.1. The procurement or modification of commercially available products, services, and technologies, from domestic or international sources, or the development of dual-use technologies;"
>
> Hence, commercially available products, services, and technologies are a first priority for acquisition solutions.

DoD Instruction 5000.2, Section 3.5.3., states that "existing commercial off-the-shelf (COTS) functionality and solutions drawn from a diversified range of large and small businesses shall be considered," when conducting the Analysis of Alternatives.

DoD Instruction 5000.2, Enclosure 4, "IT Considerations," Table E4.T1., "CCA Compliance Table," requires that, to be considered CCA compliant, the Department must redesign the processes being supported by the system being acquired, to reduce costs, improve effectiveness and maximize the use of COTS technology.

DoD Instruction 5000.2, Enclosure 4, “IT Considerations,” Section E4.2.7., states that: "When the use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative shall be made."

7.10.4. Modifying Commercial Off-the-Shelf (COTS) Software--Reuse Custom Components

It is important to note that modifying the core code of a COTS product should be avoided. It is possible to add code to the existing product, to make the product operate in a way it was not intended to do 'out-of-the-box.' This, however, significantly increases program and total life cycle costs, and turns a commercial product into a DoD-unique product. The business processes inherent in the COTS product should be adopted, not adapted, by the organization implementing the product. Adopting a COTS product is done through business process re-engineering. This means the organization changes its processes to accommodate the software, not vice versa. In many cases there will be a few instances where business process re-engineering is not possible. For example, due to policy or law, it may be necessary to build or acquire needed reports, interfaces, conversions, and extensions. In these cases, adding to the product must be done under strong configuration control. In cases where a particular COTS product does not provide the entire set of required functionality, a 'bolt-on' could be used. A bolt-on is not part of the COTS software product, but is typically part of a suite of software that has been certified to work with the product to provide the necessary additional functionality. These suites of software are integrated together to provide the full set of needed functionality. Using a 'bolt-on,' however, increases program and total life cycle costs.

Once an individual program or project develops a report, interface, conversion, or extension object, or acquires a ‘bolt-on’ capability, it should be possible for other efforts to share and reuse the solution. An initial operating capability for a repository of these custom software components is now available. It can be accessed via the Reports, Interfaces, Conversions, Extensions Repository in the Enterprise Integration Toolkit. This repository can help adapt COTS products for DoD use and reuse.

See section 7.10.6.3. for a more detailed discussion of reports, interfaces, conversions, and extensions.

7.10.5. Commercial Off-the-Shelf (COTS) Integration into the Acquisition Life Cycle

The actions below are unique to acquiring COTS Information Technology solutions. These activities should occur within a tailored, responsive, and innovative program structure authorized by DoD Instruction 5000.2. The stakeholder primarily responsible for each action is shown at the end of each bullet.

7.10.5.1. Before Milestone A

- Define strategy and plan for conducting business process re-engineering during Commercial Off-the-Shelf (COTS) software implementation phase of the program. (Domain Owner/Principal Staff Assistant)

- Consider COTS and business process re-engineering when developing the Analysis of Alternatives/Functional Solution Analysis. (See sections 3.3. and 7.8.3.4. of this guidebook). (Domain Owner/Principal Staff Assistant)
- Consider commercially available products, services, and technologies when defining initial user needs in the Initial Capabilities Document. (Domain Owner/Principal Staff Assistant)
- When developing the Technology Development Strategy and/or the Acquisition Strategy, consider commercial best practice approaches and address the rationale for acquiring COTS. (Program Manager)
- Consider the Initiation and Acquisition best practices available in the Enterprise Integration Toolkit when contracting for the COTS product and the system integrator (if required). (Domain Owner/Principal Staff Assistant and Program Manager)

7.10.5.2. Before Milestone B

- To the maximum extent possible, redesign business processes to conform to the best practice business rules inherent in the Commercial Off-the-Shelf product. Define a process for managing and/or approving the development of reports, interfaces, conversions, and extensions. (See the Enterprise Integration Toolkit for best practices in the methodologies and techniques to be successful in this phase.) (Domain Owner/Principal Staff Assistant and Program Manager)
- Consider the Implementation, Preparation, and Blueprinting best practices available in the Enterprise Integration Toolkit. (Domain Owner/Principal Staff Assistant and Program Manager)

7.10.5.3. Before Milestone C or Full Rate Production Decision Review

- Ensure scope and requirements are strictly managed and additional reports, interfaces, conversions, and extensions objects are not developed without prior authorization. (Program Manager)
- Consider best practices in the Enterprise Integration Toolkit regarding the implementation phase of the Commercial Off-the-Shelf effort. (Program Manager)
- Ensure adequate planning for Lifecycle support of the program. See section 3.4, Engineering for Lifecycle support, of “Commercial Item Acquisition: Considerations and Lessons Learned”.

7.10.5.4. After Milestone C or Full Rate Production Decision Review

- Conduct ongoing engineering and integration for sustainment activities throughout the lifecycle of the program.

7.10.6. Best Practices, Tools, and Methods

Various methodologies, toolsets, and information repositories have been developed to assist the Program Manager in the implementation of COTS software-based programs. The remainder of this section provides the Program Manager descriptions of best practices, available tools and methods, and critical success factors for use in the acquisition of commercially-based solutions. Additionally, Chapter 4 of this Guidebook, *Systems Engineering*, presents a complete discussion of applicable systems engineering practices, to include a discussion of the Modular, Open Systems Approach.

7.10.6.1. DoD Enterprise Software Initiative

The DoD Enterprise Software Initiative is a joint project designed to implement a software enterprise management process within the Department of Defense. By pooling commercial software requirements and presenting a single negotiating position to leading software vendors, the Enterprise Software Initiative provides pricing advantages not otherwise available to individual Services and Agencies. The Enterprise Software Initiative can use the Defense Working Capital Fund to provide "up-front money" for initial wholesale software buys. This funding process assures maximum leverage of the combined buying power of the Department of Defense, producing large software discounts. Agreement negotiations and retail contracting actions are performed by information technology acquisition and contracting professionals within participating DoD Services and Agencies, as Enterprise Software Initiative "Software Product Managers." The DoD Enterprise Software Initiative Home Page lists covered products and procedures, and also shows Defense Federal Acquisition Regulation Supplement Subpart 208.74 and DoD Instruction 5000.2, E4.2.7, requirements for compliance with the DoD Enterprise Software Initiative.

The DoD Business Initiative Council endorsed the Enterprise Software Initiative and provided DoD Service funding to develop a DoD-wide Software Asset Management Framework. The Council authorized Business Initiative Council Initiative IT11 to extend Software Asset Management to the DoD Component level. The Business Initiative Council also approved extension of the project to establish a Virtual Information Technology Marketplace for online purchasing of Information Technology.

7.10.6.2. SmartBUY

SmartBUY is a federal government-wide commercial software asset management and enterprise-licensing project developed by the General Services Administration in coordination with the Office of Management and Budget.

Its purposes are (a) to create a new, federal agency business process to manage commercial software as an asset, and (b) to obtain optimal pricing and preferred terms and conditions for widely used commercial software products. This effort was formally announced on June 2, 2003 in an Office of Management and Budget memorandum to the federal agencies.

The General Services Administration is the SmartBUY Executive Agent and leads the interagency team in negotiating government-wide licenses for software. The DoD Enterprise Software Initiative Team has been working closely with the SmartBUY

project for several months, and has coordinated the initial SmartBUY commercial software survey response.

7.10.6.2.1. SmartBUY Implementation

The DoD Enterprise Software Initiative Team is developing policy to implement SmartBUY within the DoD. This policy will provide the framework for migrating existing Enterprise Software Initiative Enterprise Agreements to SmartBUY Enterprise Agreements. In the meantime, the Office of Management and Budget memo establishes requirements to be followed by federal departments and agencies. Specifically, federal agencies are to:

Develop a migration strategy and take contractual actions as needed to move to the government-wide license agreements as quickly as practicable; and

Integrate agency common desktop and server software licenses under the leadership of the SmartBUY team. This includes, to the maximum extent feasible, refraining from renewing or entering into new license agreements without prior consultation with, and consideration of the views of, the SmartBUY team.

7.10.6.2.2. SmartBUY Resource

7.10.6.3. Enterprise Integration Toolkit

The Enterprise Integration Toolkit provides program managers with a repeatable Commercial Off-the-Shelf (COTS) implementation process, a knowledge repository that incorporates both government and commercial industry best practices and lessons learned, and a Reports, Interfaces, Conversions, and Extensions (RICE) Repository. The objectives of the Enterprise Integration Toolkit are to assure cost savings within the program, to achieve program speed and efficiency, and to reduce program risk. A user ID and password is required and may be obtained by registering at the website..

The Toolkit is the single point of reference for COTS program product examples and templates, and contains a repository of Education & Training courses and lessons learned. Program managers should use the Enterprise Integration Toolkit to leverage proven approaches and lessons learned in the areas of program initiation, software and system integration services sourcing, contracting, implementation, education and training, information assurance/security, performance metrics and change management. The Toolkit enables program managers to leverage work already done, and to reduce the redundancy, effort, and costs associated with a COTS implementation. (Education & Training represents a significant portion of COTS implementation costs.)

The Enterprise Integration Toolkit also contains a repository of RICE development objects to be used by program managers to leverage work already done, and to reduce redundancy, effort, and costs of Commercial Off-the-Shelf (COTS) implementations. RICE objects represent a significant portion of COTS cost, not only in the initial development, but in on-going maintenance and updating.

During a COTS implementation, there are additional configuration, design, and/or programming requirements necessary to satisfy functional requirements and achieve the desired functionality. These requirements are not supported within the commercial, core

functionality of the COTS product being implemented, and therefore require additional technical development. RICE objects represent the solution to these additional requirements.. This development (or reuse) of RICE objects enables the creation of unique Reports not standard in the product; the creation of Interfaces to external systems; the creation of Conversion programs to transfer data from an obsolete system to the new system; and the creation of Enhancements (or Extensions) to allow additional functionality to be added to the system without disturbing the core software code.

To ensure consistency across programs and within the RICE Repository, RICE is further defined as follows:

Report - A formatted and organized presentation of data.

Interface - A boundary across which two independent systems meet and act on or communicate with each other.

Conversion - A process that transfers or copies data from an existing system to load production systems.

Extension - A program that is in addition to an exiting standard program but that does not change core code or objects.

The Enterprise Integration Toolkit also includes a RICE Repository Concept of Operations that provides program managers with a process for leveraging the value of the RICE Repository. This process describes how to take data from and how to provide data to the repository. It describes the timing for the use of the repository, and at what point and level approvals (Process Owner, Program Manager, Project Sponsor, and Domain Owner) are to be obtained throughout the life cycle of a program.

Program managers should ensure vendors include these repositories in their implementation methodologies. The Enterprise Integration Toolkit's software and systems integration acquisition and contracting processes contain boilerplate language for program managers to use in acquisition documents.

For more detail or additional definitions, to review the CONOPS, or to download the Enterprise Integration Toolkit, go to http://www.eitoolkit.com.

7.10.6.4. Commercial Off-the-Shelf (COTS) Testing

On June 16, 2003, the Director, Operational Test and Evaluation, signed a memorandum issuing the "Guidelines for Conducting Operational Test and Evaluation (OT&E) for Software-Intensive System Increments." The guidelines help streamline and simplify COTS software testing procedures. They assist in tailoring pre-deployment test events to the operational risk of a specific system increment acquired under OSD oversight. For increments that are of insignificant to moderate risk, these guidelines streamline the operational test and evaluation process by potentially reducing the degree of testing. Simple questions characterize the risk and environment upon which to base test decisions, for example, "If the increment is primarily COTS, or government off-the-shelf items, what is the past performance and reliability?"

7.10.6.5. Commercial Off-the-Shelf (COTS) Lessons Learned

As the Department migrates to COTS, the workforce should be educated and trained in COTS software best practices. The objective is to raise the awareness of what is going on in the Government and in the commercial sector relative to the use of COTS software. Best practices and lessons learned should be swiftly imported into DoD and used to improve program outcomes. A good source of lessons learned is the Carnegie Mellon University COTS-based systems lessons learned web site. As indicated earlier, the Enterprise Integration Toolkit also contains a section on lessons learned.

CHAPTER 8

Intelligence, Counterintelligence, and Security Support

8.0 Chapter Overview

8.0.1. Purpose

The purpose of this chapter is two-fold: 1) to focus Program Manager attention on and describe Program Manager responsibilities regarding the prevention of inadvertent technology transfer of dual-use and leading edge military technologies that support future defense platforms and DoD capabilities-based military strategies; and, 2) to provide guidance and describe support available for protecting those technologies.

8.0.2. Contents

This Chapter is divided into six sections as follows:

Section 8.0, Chapter Overview, provides the purpose of this chapter, briefly summarizes the content and organization, and provides a brief discussion on applicability.

Section 8.1, Introduction, ranges from section 8.1.1 to section 8.1.2. It provides an overview of protection considerations, and addresses the planning, legal issues, and information reporting associated with the DoD Research and Technology Protection (RTP) effort.

Section 8.2, Intelligence, ranges from section 8.2.1 to section 8.2.2. It contains information on intelligence support to acquisition programs and intelligence supportability.

Section 8.3, Pre-Acquisition Protection Strategy for RDT&E Activities, ranges from section 8.3.1 to section 8.3.4. It covers procedures for RTP at RDT&E facilities.

Section 8.4, Acquisition Protection Strategy for Program Managers, ranges from section 8.4.1 to section 8.4.11.2. It contains procedures for protecting acquisition program technologies and information.

Section 8.5, Specialized Protection Processes, ranges from section 8.5.1 to section 8.5.6.2. It describes procedures in system security engineering, counterintelligence (CI), anti-tamper (AT), information assurance, horizontal analysis and protection, and RTP assessments and inspections that apply to protection activities, both at RDT&E sites and within acquisition programs.

8.0.3. Applicability

This chapter describes procedures for identifying and protecting DoD research and technologies, to include designated science and technology information (DS&TI) and critical program information (CPI), in accordance with DoD Directive 5000.1, DoD Instruction 5000.2, DoD Directive 5200.39, and DoD 5200.1-R. DS&TI and CPI are defined in DoD Directive 5200.39 and in section 8.1.1.

The guidance applies to all activities, phases, and locations (to include contractor locations) where DS&TI and CPI are developed, produced, analyzed, maintained, employed, transported, stored, or used in training, as well as during its disposal.

This Chapter does not apply to acquisitions by the DoD Components that involve a special access program (SAP) created under the authority of E.O. 12958. The unique nature of SAPs requires compliance with special security procedures of DoD Directive O-5205.7. If the program or system contains CPI, the SAP Program Manager will prepare and implement a Program Protection Plan (PPP) prior to transitioning to collateral or unclassified status. Security, intelligence, and CI organizations should assist the SAP Program Manager in developing the PPP. The PPP will be provided to the offices responsible for implementing protection requirements before beginning the transition.

8.0.4. Documents Discussed in Chapter 8

The documents discussed in Chapter 8 are listed below in Table 8.0.4.1. This table lists the documents that are prepared when the program manager or RDT&E site director determines they are necessary, and includes identification of and electronic links to the sections of Chapter 8 that contain the guidance for the preparation of each document.

Table 8.0.41. Documents Discussed in Chapter 8

Document	**Prepare if:**	**Discussion on Preparation**
Program Protection Plan (PPP)	The acquisition program has Critical Program Information (CPI)	8.4.6. DoDD 5200.39
Technology Assessment/Control Plan (TA/CP)	The acquisition program may have, or will have, foreign participation	8.4.3. DoDD 5530.3
Delegation of Disclosure Authority Letter (DDL)	The acquisition program has foreign participation	8.4.8.3. DoDD 5530.3
Counterintelligence Support Plan (CISP)	- For all major RDT&E activities and - For an acquisition program with Critical Program Information (CPI)	8.3.1.2. 8.3.2.1. 8.3.4. 8.5.2.
Multidiscipline CI (MDCI) Threat Assessment	The program has Critical Program Information; the MDCI threat assessment is prepared by the supporting CI activity	8.4.6.2. 8.4.7.
Security Classification Guide (SCG)	The program contains classified information or controlled	8.4.6.5. DoD 5200.1-R

	unclassified information	8.4.6.5.
System Security Authorization Agreement (SSAA)	System Security Authorization Agreement (SSAA) defined in paragraph 7.5.12.	8.5.4. Chapter 8
System Security Management Plan (SSMP)	the program manager chooses to use a SSMP to plan the program's system security effort	8.5.1.1. 8.5.1.2.
Anti-Tamper Plan	AT measures are applied	8.5.3.3. 8.5.3.1.
Information Exchange Agreements	The acquisition program has foreign participation	8.3.2.2. 8.4.3.
Program Protection Implementation plan (PPIP)	the program manager decides to use a PPIP as part of the contract	8.4.9.3.
DD Form 254, DoD Contract Security Classification Specification	When the program manager includes security controls within the contract or the contract will involve classified information.	8.4.9.7. DoD 5220.22-M

8.0.5. Support from Functional Offices

To properly accomplish activities described in this chapter, the Program Manager needs the cooperation and support of related functional offices. Support to the acquisition community from the intelligence, counterintelligence, and security communities involves a number of staff organizations and support activities that may be unfamiliar to members of the acquisition community. Table 8.0.5.1. lists the functional offices that may support the program manager in various tasks discussed in Chapter 8. This table identifies (and links to) the sections of Chapter 8 that describe various situations involving these offices. The individual assigned responsibility for coordinating intelligence support, counterintelligence support, or Research and Technology Protection (RTP) within a program office, laboratory, T&E center, or other RDT&E organization should identify the proper contacts in these organizations prior to initiating program planning.

Table 8.0.5.1. Functional Offices Discussed in Chapter 8

Functional Offices	Chapter 8 References
Security Support Office • Protection Planning For RDT&E Activities • Assignments, Visits, and Exchanges of Foreign Representatives • Collaboration • Foreign Collection Threat	8.3.2.1. 8.3.2.2 8.4.5.2 8.4.6.2 8.4.11

• Execution of the PPP	
Counterintelligence Support Organization • Counterintelligence Support During Pre-Acquisition • Collaboration • Multidiscipline CI (MDCI) Threat Assessment • Execution of the PPP • Counterintelligence Support Plan	8.3.4. 8.4.5.2. 8.4.6.2. 8.4.7. 8.4.11 8.5.2
Foreign Disclosure Officer • Safeguarding DoD RDT&E Information • Programs with Foreign Participation • Collaboration • Technology Assessment / Control Plan (TA/CP) • Providing Documentation to Contractors	8.3.1.2. 8.4.3. 8.4.5.2. 8.4.8. 8.4.9.6.
Intelligence Support Organization • Intelligence	8.2.
Intelligence Requirements Certification Office • Intelligence Certification	8.2.2.
Government Industrial Security Office • Support from Cognizant Government Industrial Security Offices	8.4.9.7.
Anti-Tamper Support Organization • Anti-Tamper	8.5.3.
DoD Executive Agent for Anti-Tamper • Anti-Tamper	8.5.3.
Operations Security (OPSEC)	8.4.5.2.

• Collaboration	
Defense Security Service • Counterintelligence Support During Pre-Acquisition	8.3.4.

8.1. Introduction

8.1.1. General Information

The DoD actively seeks to include allies and friendly foreign countries as partners in the research, development, test and evaluation (RDT&E); production; and support of defense systems. The Department of Defense encourages early involvement with allied and friendly foreign partners. Such cooperative foreign government partnerships should begin at the requirements definition phase, whenever possible. Successful execution of cooperative programs will promote the desirable objectives of standardization, commonality, and interoperability. The U.S. Government and its foreign government partners in these endeavors will benefit from shared development costs, reduced costs realized from economies of scale, and strengthened domestic industrial bases. Similarly, the DoD plays a key role in the execution of security cooperation programs that ultimately support national security objectives and foreign policy goals. U.S. defense system sales are a major aspect of security cooperation.

Increasingly, the U.S. Government relies on sophisticated technology in its defense systems for effectiveness in combat. Further, technology is recognized as a force multiplier and will continue to improve the warfighter's survivability. Therefore, it is not only prudent, but also practical to protect technologies deemed so critical that their exploitation will diminish or neutralize a U.S. defense system's effectiveness. Protecting critical technologies preserves the U.S. Government's research and development resources as an investment in the future, rather than as an expense if technology is compromised and must be replaced prematurely. It also enhances U.S. industrial base competitiveness in the international marketplace.

When necessary and successfully applied, procedures and guidance in this chapter are designed to protect Designated Science and Technology Information (DS&TI) and Critical Program Information (CPI) against compromise, from RDT&E throughout the acquisition life cycle (including property disposal), at all involved locations or facilities. DS&TI is research and technology classified information and research and technology CUI identified by RDT&E site directors to receive specialized CI and security support. CPI, in an acquisition program, may be classified information or CUI about technologies, processes, applications, or end items that if disclosed or compromised, would degrade system combat effectiveness, compromise the program or system a\capabilities, shorten the expected combat effective life of the system, significantly alter program direction, or require additional research, development, test, and evaluation resources to counter the impact of the compromise. CPI includes, but is not limited to, CPI inherited from another program and CPI identified in pre-system acquisition activities or as a result of

non-traditional acquisition techniques (e.g., Advanced Concept Technology Demonstration, flexible technology insertion).

- The teamwork engendered by this chapter provides intelligence support to the analysis phase of capabilities integration and development prior to Milestone A. The teamwork also selectively and effectively applies research and technology protection (RTP) countermeasures and counterintelligence (CI) support to the program, resulting in cost-effective activities, consistent with risk management principles, to protect DS&TI as well as CPI.
- Anti-Tamper (AT) techniques and application of system security engineering (SSE) measures allow the United States to meet foreign customer needs for advanced systems and capabilities while ensuring the protection of U.S. technological investment and equities. AT techniques and SSE measures are examples of protection methodologies that DoD programs use to protect critical system technologies.

8.1.2. Protection Overview

DS&TI and CPI may include classified military information, which is considered a national security asset that will be protected and shared with foreign governments only when there is a clearly defined benefit to the United States (see DoD Directive 5200.39). It may also include Controlled Unclassified Information (CUI), which is official unclassified information that has been determined by designated officials to be exempt from public disclosure, and to which access or distribution limitations have been applied in accordance with national laws and regulations. It may also include unclassified information restricted by statute, such as export controlled data.

Both DS&TI and CPI require protection to prevent unauthorized or inadvertent disclosure, destruction, transfer, alteration, reverse engineering, or loss (often referred to as “compromise”).

DS&TI should be safeguarded to sustain or advance the DoD technological lead in the warfighter’s battle space or joint operational arena.

The CPI, if compromised, will significantly alter program direction; result in unauthorized or inadvertent disclosure of the program or system capabilities; shorten the combat effective life of the system; or require additional research, development, test, and evaluation (RDT&E) resources to counter the impact of its loss. See DoD Directive 5200.39 for DS&TI and CPI definitions.

The theft or misappropriation of U.S. proprietary information or trade secrets, especially to foreign governments and their agents, directly threatens the economic competitiveness of the U.S. economy. Increasingly, foreign governments, through a variety of means, actively target U.S. businesses, academic centers, and scientific developments to obtain critical technologies and thereby provide their own economies with an advantage. Industrial espionage, by both traditionally friendly nations and recognized adversaries, proliferated throughout the 1990s.

Information that may be restricted and protected is identified, marked, and controlled in accordance with DoD Directives 5230.24 and 5230.25 or applicable national-level policy and is limited to the following:

- Information that is classified in accordance with Executive Order 12958, and
- Unclassified information that has restrictions placed on its distribution by:
- U.S. Statutes (e.g., Arms Export Control Act, Export Administration Act);
- Statute-driven national regulations (e.g., Export Administration Regulations, International Traffic in Arms Regulations); and
- Related national policy (e.g., Executive Order 12958, National Security Decision Directive 189).

Incidents of loss, compromise, or theft of proprietary information or trade secrets involving DS&TI and CPI, are immediately reported in accordance with Section 1831 et seq. of Title 18 of the United States Code, DoD Instruction 5240.4, and DoD Directive 5200.1. Such incidents are immediately reported to the Defense Security Service (DSS), the Federal Bureau of Investigation (FBI), or the applicable DoD Component CI and law enforcement organizations. If the theft of trade secrets or proprietary information might reasonably be expected to affect DoD contracting, DSS should notify the local office of the FBI.

8.2. Intelligence

8.2.1. Threat Intelligence Support

Acquisition programs should be supported by a current and validated threat assessment provided by the Defense Intelligence Agency (DIA) or Service Intelligence Production Centers. Major Defense Acquisition Programs are required to utilize DIA-validated threat assessments to support program development in accordance with DoD Directive 5105.25. These threat assessments can take the form of:

- A Capstone document that addresses current and future threats to a defined U.S. warfighting capability; or
- A system-specific threat assessment for programs subject to Defense Acquisition Board review.

The Defense Intelligence Community should maintain continuous contact with the acquisition community to ensure awareness of developing threat information. Program managers should identify Critical Foreign Capabilities that could adversely impact on operational utility or employment of their system.

8.2.1.1. Capstone Threat Assessment

Capstone Threat Assessments should address current and future (10- and 20-year projections) foreign developments that challenge U.S. warfighting capabilities (i.e., precision strike warfare, undersea warfare, space operations, surveillance, and reconnaissance). Since most Capstone Threat Assessments require input from multiple

Defense Intelligence elements, DIA edits and integrates the inputs into a single, coherent validated document.

8.2.1.2. System-Specific System Threat Assessment

The Defense Intelligence Agency (DIA) provides validation for System Threat Assessments, prepared by the appropriate Service, to support major defense acquisition programs. Appropriate Defense Intelligence organization(s), identified by DIA, prepare the System Threat Assessment. The assessment should be kept current and validated. The assessment should be system specific to the degree of system definition available at the time the assessment is being prepared. The assessment should address projected adversary capabilities at system IOC and at IOC plus 10 years. The recommended System Threat Assessment format includes the following elements:

- An executive summary that includes key intelligence judgments and significant changes in the threat environment;
- Discussion of the operational threat environment, adversary capability(s) that may effect operation of the system, system specific threat, reactive threat, and technologically feasible threats. Reference to the Capstone Threat Assessments will be made where possible to streamline the System Threat Assessment;
- A section that addresses developments related to the program manager's Critical Foreign Capabilities; and
- A section that identifies intelligence gaps related to the Critical Foreign Capabilities or of a more over-arching nature.

8.2.1.3. Threat Validation

For MDAPs subject to DAB review, DIA provides validation for System Threat Assessments. DIA validation ensures that all relevant data is considered and appropriately used by author(s) of the assessment.

DIA may also validate other threat information. DIA must validate threat information contained in Joint Capabilities Integration and Development System documents in accordance with Joint Staff guidance.

8.2.1.4. Support to Test and Evaluation

The TEMP should define specific intelligence requirements to support program test and evaluation. DIA should coordinate with the entire Defense Intelligence Community to provide appropriate intelligence support to the Test and Evaluation Community.

8.2.2. Intelligence Certification

DoD Instruction 4630.8 requires the Joint Staff to provide ASD(NII) with an intelligence certification of Information Support Plans (ISPs). The J-2 element of the Joint Staff will facilitate the Intelligence Certification with collaborative inputs from DoD Components. Program managers should be aware of the requirements for Intelligence Certification, and should ensure that ISP preparation considers the certification criteria outlined below.

Overarching Criteria. The Intelligence Certification evaluates intelligence information requirements in ISPs for completeness, supportability, and impact on joint intelligence strategy, policy, and architectural planning. General descriptions of these criteria categories follow:

- **Completeness**. Completeness refers to the extent to which the ISP addresses requirements *for* intelligence support (such as analytical products required, targeting support, imagery, etc.) and program compliance with requirements *by* intelligence (such as interoperability with intelligence systems, compliance with intelligence security standards, etc.).
- **Supportability**. Supportability refers to the availability, suitability, and sufficiency of the required intelligence support. Intelligence Certification analysts will compare a program's stated or derived intelligence support needs with the expected intelligence capabilities that are projected throughout a program life cycle. The ability to adequately assess supportability depends upon the completeness of support requirement declaration.
- **Impact on Intelligence Strategy, Policy, and Architecture Planning**. Impact, within this context, refers to the identification of additional inputs to or outputs from the intelligence infrastructure. Requirements for intelligence support may be transparent with regard to the intelligence support infrastructure if planned products, information, or services are already projected to be available, suitable, and sufficient throughout a program life cycle. In other cases, programs may require new types of support or have increased standards for existing support. These additional inputs or outputs may require changes across the Doctrine, Organization, Training and Education, Materiel, Logistics, Personnel, or Facilities (DOTMLPF) spectrum. These potential changes impact intelligence strategy, policy, and architecture planning. The impact assessment provides a mechanism for providing critical feedback to the defense and national intelligence communities to highlight potential shortfalls in current or planned intelligence support.

Additional Criteria. The certification also evaluates intelligence-related systems with respect to open system architecture, security, and intelligence interoperability standards. (J-6 Interoperability certification is conducted in a separate, but related process, and is documented in CJCSI 6212.01.)

Those personnel with a Joint Worldwide Intelligence Communications System terminal can access the specific procedures and criteria for the Intelligence Certification on the Intelligence Requirements Certification Office homepage (under “Certification Process”). By telephone, additional information may be obtained by calling the Intelligence Requirements Certification Office at 703-695-4693.

8.3. Pre-Acquistion Protection Strategy for RDT&E Activities

8.3.1. General

Protection may apply to all seven subcategories of RDT&E (see DoD 7000.14-R, Volume 2B). DoD Directive 5200.39 recognizes the normally unrestricted nature of

fundamental research, as identified in National Security Decision Directive (NSDD) 189, and as further stipulated for Basic Research in Executive Order 12958. The term "fundamental research" refers generally to Basic Research (6.1) and Applied Research (6.2), and is defined in the International Traffic in Arms Regulations (ITAR).

8.3.1.1. Purpose

The purpose of pre-acquisition protection is to prevent unauthorized disclosure of DoD RDT&E information. CI and security specialists provide a wide range of services to ensure personnel assigned to RDT&E sites are aware of threats from foreign intelligence services, other foreign interests, or anyone involved in unauthorized acquisition of DoD information. For example, one of these services can be to ensure requirements for authorized foreign involvement are met and that personnel administering such programs are well versed in those requirements.

8.3.1.2. Safeguarding DoD RDT&E Information

Working together, RDT&E laboratories and centers, and CI, security, foreign disclosure, OPSEC, and intelligence organizations should use an interactive process (such as an IPT) to safeguard DS&TI from compromise in order to sustain or advance the DoD technological lead in the future battle space.

The RDT&E commanding officer, site director, or their designee (referred to hereafter as "site director") identifies and prioritizes their DS&TI, and communicates the results to CI, security, foreign disclosure, operations security (OPSEC), and intelligence organizations.

- The site director, in consultation with the supporting CI organization, prepares a site-specific CI Support Plan (CISP) for each RDT&E site as well as academic and commercial facilities supporting the effort.
- Intelligence organizations provide information concerning technical capabilities that adversaries could use to gain information on specific RDT&E programs or projects.
- Site directors, in coordination with security, intelligence, and CI specialists, should ensure that assigned personnel receive tailored threat briefings.

8.3.2. Protection Approaches

RDT&E conducted within the DoD, as well as by DoD contractors, is covered by the following policies:

- Disclosure of both classified military information and unclassified technical data (DoD Directive 5230.11, "Disclosure of Classified Military Information (CMI) to Foreign Governments and International Organizations;" DoD Directive 5230.24, "Distribution Statements on Technical Documents;" DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," International Traffic in Arms Regulation, and Export Administration Regulations).

- Control of foreign visitors (DoD Directive 5230.20, "Visits, Assignments, and Exchanges of Foreign Nationals").
- Export control (DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions").

For effective protection, the site director (and gaining Program Manager) should integrate these policies into an overall protection strategy, to ensure the identification of DS&TI, the identification of the applicable safeguards, and the effective application of those safeguards. The CISP aids the formulation of an effective protection program at each RDT&E site. Site directors make these policies effective within the RDT&E environment through training and awareness programs.

8.3.2.1. Protection Planning For RDT&E Activities

To conduct effective RTP planning, each RDT&E site director should:

- Review the site RDT&E program periodically and/or whenever there is a significant change in the program.
- Identify information within the RDT&E program that has already been marked for safeguarding (e.g., export control, distribution statement, special handling caveat).
- Identify and prioritize that information as DS&TI.
- Ensure information identified as DS&TI is appropriately marked and disseminated (e.g., export control, distribution statement, special handling caveat).
- Select appropriate countermeasures to protect the DS&TI and identify CI support to be provided.
- Prepare a CISP, with supporting organizations (e.g., CI, security, foreign disclosure, OPSEC, intelligence), tailored to focus protection resources on the identified DS&TI. (The CISP identifies the DS&TI and serves as the "contract" between the individual RDT&E site director and the responsible CI support activity.)
- Communicate the DS&TI to CI, security, foreign disclosure, OPSEC, and intelligence organizations, as appropriate.

8.3.2.2. Assignments, Visits, and Exchanges of Foreign Representatives

The site director should:

- Ensure that assignments, visits, and exchanges of foreign nationals are processed through appropriate channels.
- Ensure that a contact officer has been appointed for each foreign national and is informed of authorized disclosures.
- Establish a process prior to the visit, wherein the relevant technical Point of Contact (POC) and appropriate security and CI personnel communicate the

purpose of the visit by the foreign national and the technology and/or program information to be discussed.

- Ensure the process for approving visits by foreign nationals includes dissemination of appropriate disclosure rules and restrictions to RDT&E personnel being visited.
- Ensure that foreign nationals are visually identifiable as required by DoD Directive 5230.20.
- Establish a process for archiving information about foreign national visits, including but not limited to, information about the visitor, reason for the visit, information disclosed, and any anomalous event that occurred during the visit.
- Ensure proposed DS&TI releases are reviewed and approved using provision(s) of an Information Exchange Program Agreement (formerly Data Exchange Agreement) prior to release.
- Ensure copies of all international agreements (including MOUs, Information Exchange Program Agreements, and Delegations of Disclosure Letters (DDLs)) relevant to their programs and related systems are maintained and readily accessible to all program personnel as well as supporting CI and security personnel.

8.3.2.3. Export Control

The site director should:

- Establish a process whereby RDT&E personnel determine whether technical data or commodities at RDT&E facilities have been approved for export to foreign countries.
- Establish a focal point at each RDT&E site to determine whether a license for deemed exports is required when a foreign national visits the facility.

8.3.3. Information Assurance

All IT network and systems storing, processing, or transmitting DS&TI should be accredited in accordance with DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)"as described in Chapter 7, Networks and Information Integration.

8.3.4. Counterintelligence Support During Pre-Acquisition

The site director, in consultation with the supporting CI activity, should develop a CISP for each RDT&E site as described in section 8.5.2.

To support the RDT&E site directors, DoD Component CI agencies should:

- Assign CI specialists to support DoD RDT&E activities on or off military installations. The assigned CI specialist(s) will:
    - Provide full-time, tailored, protection support to major DoD RDT&E sites. ("On-call" support will be provided to other DoD RDT&E sites.)

- Provide, in coordination with the Defense Security Service (DSS), CI support to DoD contractors and academic institutions working with DoD DS&TI.

- Ensure that appropriate security, research management, foreign disclosure, OPSEC, and acquisition program personnel are continuously appraised of foreign intelligence or other threat information relating to their RDT&E site and/or research project.
- Disseminate CI information and products to contractor facilities under DSS cognizance and to other locations and officials that DSS may designate.
- Keep DSS informed of any threat to DS&TI and/or CPI that involve contractors under the cognizance of DSS. Providing classified threat information to contractors will be coordinated with DSS.
- Provide requested threat information to assist defense contractors in developing and updating their Technology Control Plans and protection of DoD DS&TI.

8.4. Acquisition Protection Strategy for Program Managers

8.4.1. Pre-Acquisition Considerations

Program protection planning begins with the Joint Capabilities Integration and Development System as described in CJCS Instruction 3170.01 and in Part 3 of this Chapter. It is integral to the overall acquisition strategy, which is typically developed prior to formal designation of an acquisition program. The program manager identifies the resources needed (e.g., personnel, fiscal) to accomplish the evaluation and initiate protection as early as possible, but no later than entry into Milestone B.

8.4.2 Acquisition Program Protection - Initiation to Implementation

CPI is the foundation upon which all protection planning for the program is based, and the reason all countermeasures are implemented. Effective program protection planning begins by the program manager reviewing the acquisition program to determine if it contains CPI. If a program manager has not been appointed, the responsible commander/manager or program executive conducts this review. This examination should consider DS&TI previously identified by DoD laboratories, CPI inherited from another program, or CPI that results from non-traditional acquisition techniques (i.e., Advanced Concept Technology Demonstration or flexible technology insertion).

- The program manager (or other official as noted above), with the assistance of a working-level IPT (WIPT), determines the existence of CPI.
- If a program contains CPI, program protection planning is required (see 8.4.5). The program manager (or other official as noted above), with the assistance of a WIPT and/or appropriate support activities, is responsible for developing and implementing a Program Protection Plan (PPP).
- The PPP will be developed, as required, beginning in the Technology Development phase, and will be available to the Milestone Decision Authority at Milestone B and all subsequent milestones during the life cycle of the program.

The PPP is revised and updated once every three years, or as required by changes to acquisition program status or the projected threat.

- If there is no CPI associated with the program (either integral to the program or inherited from a supporting program), the program manager so informs the Milestone Decision Authority, Program Executive Officer, or DoD Component Acquisition Executive, as appropriate, and a PPP is not required.
- The next step is for the program manager, through the program management staff, to translate protection requirements into a PPP. This is usually accomplished by a working-level IPT (WIPT) following the process outlined in section 8.4.6. Program protection activities described in sections 8.5.1 to 8.5.6.2 are tailored and performed prior to each milestone to provide the required countermeasures during each acquisition phase.
- After the protection planning foundation is laid, the program proceeds through the milestones and phases of the acquisition process. The program follows an event-based schedule that implements the protection strategy and completes the actions outlined in the PPP.

8.4.3. Programs with Foreign Participation

When a determination is made that any of the following conditions exist, a Technology Assessment/Control Plan (TA/CP) and a Delegation of Disclosure Authority Letter (DDL) should be prepared as annexes to the PPP:

- Foreign participation in system development is possible;
- An allied system will be used;
- The system to be developed is a candidate for foreign sales or direct commercial sales;
- The system will be used in multinational operations; or
- The program will involve cooperative R&D with allied or friendly foreign countries.

Under any of the above conditions, the Foreign Disclosure Officer (FDO) should be involved and informed. With respect to cooperative R&D programs, a Summary Statement of Intent (SSOI), which includes a summarization of the TA/CP, is needed prior to obtaining authority to negotiate the International Agreement that is statutorily required to conduct the program.

If foreign involvement is initiated prior to the appointment of a program manager, the DoD Component generating the capability need should prepare the TA/CP and DDL for Joint Requirements Oversight Council validation and Milestone Decision Authority approval. The program manager, when appointed, should review the requirements for the PPP, TA/CP, DDL, and supporting documentation, and direct the preparation as appropriate.

8.4.4. Risk Management

The overall risk management effort could be a seamless transition between the two following applications, thus allowing a common vernacular for both. Risk management interfaces with acquisition strategy and technology protection. In the current larger scope, risk management has at least two applications.

8.4.4.1. Risk Management in Systems Engineering

In systems engineering, risk management examines all aspects of the program as they relate to each other, from conception to disposal. This risk management approach integrates design (performance) requirements with other Lifecycle issues such as manufacturing, operations, and support.

The program manager should establish a risk management process within systems engineering that includes risk planning, risk assessment (identification and analysis), risk management, and risk monitoring approaches to be integrated and continuously applied throughout the program, including the design process.

This type of risk assessment includes identification and analysis of potential sources of risk, to include cost, schedule, and performance, and is based on such factors as: the technology being used and its relationship to design; manufacturing capabilities; potential industry sources; and test and support processes.

8.4.4.2. Risk Management in Program Protection

In program protection, when viewed within the global context of security, risk management is concerned with technology transfer and is a systematic methodology to identify, evaluate, rank, and control inadvertent loss of technology. In this respect, it is based on a three-dimensional model: the probability of loss, the severity if lost, and the countermeasure cost to mitigate the loss. As such, risk management is a key element of a program manager's executive decision-making - maintaining awareness of technology alternatives and their potential sensitivity while making trade-off assessments to translate desired capabilities into actionable engineering specifications.

To successfully manage the risk of technology transfer, the program manager should:

- Identify contract vehicles which involve the transfer of sensitive data and technology to partner suppliers;
- Evaluate the risks that unfavorable export of certain technologies could pose for the program; and
- Develop alternatives to mitigate those risks.

8.4.5. Program Protection Planning

When the acquisition program contains CPI, the program manager should initiate a program protection planning process that includes the following steps:

- Identify and set priorities on those operational or design characteristics of the system that result in the system providing unique mission capabilities.
- Identify and prioritize CPI related to distinctive system characteristics in terms of their importance to the program or to the system being developed. (CPI includes

defense technologies and their support systems as defined in DoD Directive 5200.39.)

- Identify specific program locations where CPI is developed, produced, analyzed, tested, maintained, transported, stored, or used in training.
- Identify the foreign collection threat to the program. (MDCI Threat Assessments are discussed in section 8.4.7)
- Identify program vulnerabilities to specific threats at specific times and locations during all phases of the acquisition cycle.
- Identify time- or event-phased RTP countermeasures to be employed by the program manager to reduce, control, or eliminate specific vulnerabilities to the program to ensure a minimum level of protection for CPI.
- Identify anti-tamper (AT) techniques (see section 8.5.3) and system security engineering (SSE) measures (see section 8.5.1) required to protect CPI. Ensure these AT and SSE techniques are included the system's design specifications, subsequent technical drawings, test plans, and other appropriate program documentation.
- Identify elements that require classification and determine the phases at which such classification should occur and the duration of such controls. The resulting program Security Classification Guide is issued by the program Original Classification Authority (OCA).
- Identify protection costs associated with personnel, products, services, equipment, contracts, facilities, or other areas that are part of program protection planning, and countermeasures. These costs are reflected in the program Planning, Programming, and Budgeting Execution System documentation.
- Identify the risks and benefits of developing, producing, or selling the system to a foreign interest, as well as the methods used to protect DS&TI and/or CPI if such an arrangement is authorized. Determine if an export variant is necessary (see section 8.5.1.5).
- Identify contractual actions required to ensure that planned systems security engineering, AT techniques, information assurance, information superiority, classification management and/or RTP countermeasures are appropriately applied by defense contractors at contractor locations (see section 8.5.6). Care should be taken to ensure that measures do not adversely impact the technology of future foreign partners.
- Coordinate with program managers of supporting programs to ensure that measures taken to protect DS&TI and/or CPI are maintained at an equivalent level throughout DoD and its supporting contractors.

After completing the protection planning process, the program manager, assisted by applicable CI and security support activities, ensures implementation of countermeasures to protect the DS&TI and/or CPI at each location and activity identified in the protection

planning process. The protection planning process is a dynamic and continuous element, and should remain amenable to appropriate revision.

8.4.5.1. Critical Program Information (CPI)

CPI may include components; engineering, design, or manufacturing processes; technologies; system capabilities and vulnerabilities; and other information that give the system its distinctive operational capability. (Example: A system characteristic might be the small radar cross section. The CPI are those unique program elements that make the small radar cross-section possible.)

When DS&TI are inherited from a technology project and incorporated into an acquisition program, the DS&TI should be identified as program CPI.

8.4.5.1.1. Identifying CPI

To develop the list of CPI, a WIPT should refer to a functional decomposition already performed by the program office, or if necessary, perform a "functional decomposition" of the program or system, as follows:

- Analyze the program or system description and those specific components or attributes that give the system its unique operational capability.
- Analyze each subcomponent until a specific element is associated with each system capability.
- When a specific element is isolated, evaluate its potential as CPI by applying the following questions; an affirmative answer will qualify the item as CPI. If a foreign interest obtained this item or information:
    - Could a method be developed to degrade U.S. system combat effectiveness?
    - Could it compromise the U.S. program or system capabilities?
    - Would it shorten the expected combat-effective life of the system or significantly alter program direction?
    - Would additional RDT&E resources be required to develop a new generation of the U.S. system that was compromised?
    - Would it compromise the U.S. economic or technological advantage?
    - Would it threaten U.S. National Security?
- In addition to the elements organic to the system, the program manager should consider any engineering process, fabrication technique, diagnostic equipment, simulator, or other support equipment associated with the system for its identification as a possible CPI. Special emphasis should be placed on any process that is unique to the system being developed. The program manager and program engineer should evaluate each area and identify any activity distinctive to the U.S. industrial and technological base that limits the ability of a foreign interest to reproduce or counter the system.

8.4.5.1.2. Refining CPI

Once all system CPI has been identified, additional refinement may be necessary. Key considerations in this refinement follow:

Describe CPI in terms understandable by those not in the scientific or engineering field (e.g., use terms from the Militarily Critical Technology List (MCTL) or National Disclosure Policy). The fact that a particular technology is on a technology control list does not mean that particular technology is a CPI.

- Provide specific criteria for determining whether CPI has been compromised.
- Indicate any CPI related to a treaty-limited item.
- Indicate if this CPI is being or may be used by any other acquisition program or system.
- Prioritize CPI to ensure that the most important information is emphasized during protection cost analysis. That process addresses the following three questions:
    - What is the threat to U.S. National Security?
    - What is the extent to which the CPI could benefit a foreign interest?
    - How difficult is it for a foreign interest to exploit the information?

8.4.5.1.3. Inherited DS&TI and CPI

The program manager should identify and prioritize DS&TI and/or CPI for any component, subsystem, technology demonstrator, or other independent research program that will be incorporated into the program manager's program. The using program manager should ensure such CPI is addressed in the subsystem PPP. Conversely, the program manager of a subsystem program with CPI should ensure that their CPI is included in the major program PPP.

- The program manager of a new system will ensure that CPI shared or gained from a subsystem is protected in the new system to at least the same level of protection afforded in the subsystem program.
- A program manager of a system that incorporates a subsystem not reviewed to identify CPI should request the subsystem program office to review their program and supply the resulting information and/or documentation.
- When supporting activities defined as acquisition programs have not developed a PPP to protect their CPI, the program manager incorporating the technology in question should request the subsystem program manager to develop and provide an approved PPP.

8.4.5.2. Collaboration

The program manager is responsible for developing, approving, and implementing a PPP, normally through a WIPT. The program manager may establish a research and technology protection WIPT or include the appropriate personnel on an existing WIPT to assist in preparing the PPP and its supporting documentation.

CI and security support activities and program protection staff elements should assist the program manager in identifying CPI.

The following personnel or organizational representatives are normally represented in the research and technology protection (RTP)WIPT:

- Program office engineering and/or technical staff
- System user representative
- Maintenance and logistics representative
- Organizational or command security manager
- Counterintelligence
- Intelligence
- Operations security
- Foreign disclosure
- Base, installation, or post physical security staff
- Organization RTP staff representative
- Information Assurance Manager and/or information systems security manager

The program manager should ensure close coordination and cooperation between the security, foreign disclosure, intelligence, operations security, CI, physical security, and RTP offices and the program office staff during development of a PPP.

8.4.6. Program Protection Plan (PPP)

The PPP is the program manager's single source document used to coordinate and integrate all protection efforts designed to deny access to CPI to anyone not authorized or not having a need-to-know and prevent inadvertent disclosure of leading edge technology to foreign interests. If there is to be foreign involvement in any aspect of the program, or foreign access to the system or its related information, the PPP will contain provisions to deny inadvertent or unauthorized access.

The program manager establishes and approves the PPP for an acquisition program as soon as practicable after validation of the Initial Capabilities Document and the determination that CPI exists.

Preparation and implementation of a PPP is based on effective application of systematic risk management methodology, not risk avoidance. Costs associated with protecting CPI are balanced between protection costs and potential impact if compromised. In some cases, residual risks may have to be assumed by the program; such decisions rest with the Milestone Decision Authority, based upon the recommendation by the program manager.

The following guidance describes the process used to prepare a PPP when one is required:

- Any program, product, technology demonstrator, or other item developed as part of a separate acquisition process, and used as a component, subsystem, or modification of another program, should publish a PPP.
- Effectiveness of the PPP is highly dependent upon the quality and currency of information available to the program office.
    - Coordination between the program office and supporting CI and security activities is critical to ensure that any changes in the system CPI, threat, or environmental conditions are communicated to the proper organizations.
    - Intelligence and CI organizations supporting the program protection effort should provide timely notification to the program manager of any information on adverse foreign interests targeting their CPI without waiting for a periodic production request.

The PPP is classified according to content.

The degree of detail in the PPP should be limited to information essential to plan and program the protection of CPI, and to provide an executable plan for implementing the associated countermeasures throughout the pre-acquisition and acquisition phases. While there is no specific format for PPPs, they normally include the following:

- System and program description;
- All program and support points of contact (POCs);
- A prioritized list of program CPI;
- Multidiscipline Counterintelligence (MDCI) threat assessment to CPI;
- Vulnerabilities of CPI;

All RTP countermeasures (e.g., AT techniques, SSE) and Militarily Critical Technology List (MCTL) citations for applicable DS&TI or CPI;

- All RTP associated costs, by Fiscal Year, to include PPP development and execution;
- CI support plan (CISP);
- Current Security Classification Guide (SCG);
- Foreign disclosure, direct commercial sales, co-production, import, export license or other export authorization requirements, and/or TA/CP; and
- Delegation of Disclosure Authority Letter, if appropriate.

The following sections provide specific guidance related to some PPP topics listed above.

8.4.6.1. System and Program Descriptions

System Description. Since most acquisition programs combine existing, proven technology, as well as information with state-of-the-art technology, the system description included in a PPP provides the reviewer with a clear indication of the capabilities and limitations of the system being acquired, including simulators and other

supporting equipment. The purpose of the system description is to set the stage for identifying CPI. The system description should be based on the approved Initial Capabilities Document and Capability Development Document and include:

- Anticipated employment of the system within the battle space, along with the strategic, operational, or tactical impact of the system; and
- Specific characteristics that distinguish the system from existing systems, other systems under development, or that provide the system with unique operational or performance capability.

Program Description. This section is a short summary of the organization and structure of the office responsible for developing and fielding the acquisition system. Early in the acquisition process, that information may be somewhat limited. Detail should be added as participants in the program are identified and as their role in program protection activities becomes known. The program description should briefly describe the following:

- The program management chain of command, including the Program Executive Officer, DoD Component Acquisition Executive, and/or Milestone Decision Authority for the program and supporting programs;
- The locations, points of contact (POCs), and telephone numbers of prime contractors, sub-contractors, vendors, DoD sites, Federal agencies, Government Owned - Contractor Operated and DoD RDT&E activities and/or facilities that will handle, store, or analyze CPI-related material;
- DoD Component and/or other DoD organization partners that are equity holders; and
- Likelihood that these technologies or this program will transition to another DoD Component / DoD organization in the future.

8.4.6.2. Foreign Collection Threat

Foreign collection threat assessment used by the program office in planning protection for the CPI should be based upon a National-level intelligence estimate known as a "MDCI Threat Assessment."

- The MDCI threat assessment is prepared and produced as a stand-alone document by the applicable DoD CI analysis center (see section 8.4.7);
- The MDCI threat assessment should not be confused with a System Threat Assessment (STA); the MDCI threat assessment identifies foreign interests having a collection requirement and a capability to gather information on the U.S. system being developed;
- Sudden changes in the operational threat should be reviewed as they occur to determine if the changes are due to successful foreign intelligence collection;
- The program manager and WIPT should compare results of the MDCI threat assessment with the CPI and vulnerabilities to determine the level of risk to the program; and

- The WIPT should integrate environmental factors and arms control-related issues that might reduce the ability of foreign interests to collect information at a given location in the MDCI threat assessment, where applicable.

A threat exists when:

- A foreign interest has a confirmed or assessed requirement for acquiring specific classified or sensitive defense information or proprietary or intellectual property information;
- A foreign interest has the capability to acquire such information; and/or
- The acquisition of such information by the foreign interest would be detrimental to U.S. interests.

Confirmed or assessed identification of foreign collection requirements provide indicators of probable sources or methods employed to satisfy a collection requirement.

CI and security support activities assist the program office in preparing collection requirements and production requests to applicable DoD Component intelligence or CI analysis centers.

- CI and security support activities should submit the request to the intelligence center that normally supports the program manager; and
- An informational copy is sent to the intelligence analysis center of any other DoD Component involved in the program to facilitate a single and unified position on the collection threat. CIFA is also provided a copy.

8.4.6.3. Vulnerabilities

Vulnerability is the susceptibility to compromise of a program to a threat in a given environment. Vulnerabilities to the program's CPI are based upon one or more of the following:

- How CPI is stored, maintained, or transmitted (e.g., electronic media, blueprints, training materials, facsimile, modem);
- How CPI is used during the acquisition program (e.g., bench testing, field testing);
- Emanations, exploitable signals, or signatures (electronic or acoustic) that are generated or revealed by the CPI (e.g., telemetry, acoustic energy, radiant energy);
- Where CPI is located (e.g., program office, test site, contractor, academia, vendor);
- Types of OPSEC indicators or observables that are generated by program or system functions, actions, and operations involving CPI;
- Conferences, symposia, or foreign travel that the program manager and staff members participate in or plan to be involved in;

- The level of human intelligence or insider threat that is evident or projected at the program management location or other locations where CPI will be located;
- Foreign disclosures that are planned, proposed, or staffed for release; and
- Degree of foreign participation that is currently pursued or being planned for the program or locations where CPI will be located.

The program manager should prioritize identified vulnerabilities;

- Prioritization is based upon the consequences if CPI is lost or compromised, and the level of difficulty for a foreign interest to exploit the information; and
- Factors to be considered include the adverse impact on the combat effectiveness of the system, the effect on the combat-effective lifetime, and the cost associated with any modifications required to compensate for the loss.

8.4.6.4. RTP Countermeasures

These are measures employed to eliminate or reduce the vulnerability of CPI to loss or compromise, and include any method (e.g., AT techniques, information assurance) that effectively negates a foreign interest capability to exploit CPI vulnerability.

RTP countermeasures are developed to eliminate vulnerabilities associated with an identified threat to CPI based upon the authoritative, current, and projected threat information in the MDCI threat assessment. RTP countermeasures will:

- Be applied in a time- or event-phased manner (e.g., for certain periods of time, until milestones within program development).
- Be implemented until they are no longer required. They are terminated or reduced as soon as practicable after the threat, CPI, or environmental changes lead to a reduction or elimination of the vulnerabilities or a negation of the threat. For example, arms control countermeasures might be implemented only while the facility is vulnerable to a mandated arms control treaty inspection or an over flight by foreign inspectors.
- Address DoD Information Technology Security Certification and Accreditation Process (DITSCAP) compliance for all information technology systems and/or networks.

The program manager should establish a countermeasures program based upon threat, risk management, OPSEC methodology, and vulnerability assessments. The program manager should determine the costs associated with countermeasure application or implementation, and compare them to the risk associated with loss or compromise of the CPI. Whenever countermeasures to reduce, control, or eliminate a CPI vulnerability will not be developed, the program manager should provide a justification for that decision in the countermeasures section of the PPP.

If the acquisition program does not have an assigned or contracted security organization, applicable CI and security support activities should assist the program office in developing a draft countermeasures concept based upon the program manager's guidance.

The program manager should designate the element of the program office responsible for publishing the PPP.

Additional RTP countermeasure considerations include the following:

- Countermeasures recommended to eliminate or reduce vulnerabilities associated with CPI at government and contractor facilities, may not be waived while the affected facilities are vulnerable to arms control treaty inspections or over flights by foreign interests.
- The requirement for contractor compliance with the government-approved PPP is included in the government solicitation and the resulting contract(s) (see section 8.4.9).
- Training in protection of research and technology information and security awareness is integral to the countermeasures effort.
    - Following approval of the PPP, the program manager should implement a training program to inform all program members of the requirements in the PPP and, if applicable, the requirements and guidelines established in the DDL, which is a U.S.-only document.
    - Emphasis is placed on encrypting the transmission of electronic messages, facsimile transmissions, and telephone transmissions relating to CPI, underpinning technologies, and other CUI related to programs containing DS&TI or CPI. These transmissions should be via Federal Information Processing Standard 140-2 compliant encryption.
- Countermeasures are dynamic. As the threat, CPI, or environment changes, the countermeasures may also change. The program manager should update the PPP as system vulnerabilities change, and thus reduce the cost of and the administrative burden on their program.

8.4.6.5. Security Classification Guide (SCG)

When necessary, the program manager must develop a SCG in accordance with DoD 5200.1-R. The SCG addresses each CPI, as well as other relevant information requiring protection, including export-controlled information and sensitive but unclassified information.

All controlled unclassified information, information identified as For Official Use Only (FOUO) as defined in DoD 5400.7-R, or information with other approved markings that require dissemination controls (e.g., DoD Directive 5230.24 and DoD Directive 5230.25, is exempt from mandatory disclosure under the Freedom of Information Act and will be identified in the SCG.

The SCG will be reviewed, and amended when necessary, as part of each milestone review or as otherwise required by DoD 5200.1-R

8.4.6.6. Protection Costs

Cost data associated with countermeasures and other RTP efforts are compiled by the RTP WIPT, tabulated by acquisition phase, and included in the PPP. Cost accounting

only addresses the costs specific to the implementation of the PPP and excludes projected costs for operating with classified information. (See section 8.4.9.5.)

Costs should be displayed by security discipline (e.g., physical security, personnel security, industrial security) and category (e.g., equipment, services, personnel). Cost data for each phase should be as specific as possible. Additionally, actual annual costs for the previous phase should be compiled and compared with the projected annual cost for the current acquisition phase. Significant deltas showing differences between projected and actual cost data should be explained. This information is used for justifications required by the Planning, Programming, and Budget System.

The Acquisition Program Baseline includes costs related to PPP implementation.

8.4.7. Multidiscipline CI (MDCI) Threat Assessment

When an acquisition program containing CPI is initiated, the program manager should request a MDCI threat assessment from the servicing CI organization. The MDCI threat focuses on how the opposition sees the program and on how to counter the opposition's collection efforts. The MDCI analyst, in addition to having an in-depth understanding and expertise on foreign intelligence collection capabilities, must have a good working knowledge of the U.S. program. Therefore, CI organizations need information that describes the CPI and its projected use to determine the foreign collection threat to an acquisition program.

The MDCI threat assessment will provide the program manager with an evaluation of foreign collection threats to specific program or project technologies, the impact if that technology is compromised, and the identification of related foreign technologies that could impact program or project success. The MDCI threat assessment is updated every two years throughout the acquisition process. Changes are briefed to the program or project manager within 60 days.

When gathering information to meet the needs described in this Chapter, intelligence and CI organizations must comply with DoD Directive 5240.1 and DoD 5240.1-R. Information gathered by non-intelligence community entities must comply with DoD Directive 5200.27.

8.4.7.1. Threat Analysis Request

The program manager's request to the CI organization for a threat assessment normally contains the following information and is classified as appropriate:

- Program office, designator, and address;
- Program manager's name and telephone number;
- POC's name, address, and telephone number;
- Supporting or supported programs' or projects' names and locations;
- Operational employment role, if any;
- List of CPI;

- Relationship to key technologies or other controlled technology lists of the Departments of Defense, Commerce, and/or State;
- CPI technical description, including distinguishing characteristics (e.g., emissions; sight or sensor sensitivities) and methods of CPI transmittal, usage, storage, and testing;
- Use of foreign equipment or technology during testing (if known);
- Anticipated foreign involvement in the development, testing, or production of the U.S. system;
- Contractor names, locations, POCs, and telephone numbers, as well as the identification of each CPI used at each location; and
- Reports of known or suspected compromise of CPI.

8.4.7.2. Preliminary MDCI Threat Assessment

After the request is submitted, the Component CI organization provides a preliminary MDCI threat assessment to the program manager within 90 days. A preliminary assessment is more generic and less detailed than the final assessment. It is limited in use since it only provides an indication of which countries have the capability to collect intelligence on the U.S. system or technology as well as the possible interest and/or intention to collect it. The preliminary MDCI assessment may serve as the basis for the draft PPP.

8.4.7.3. Final MDCI Threat Assessment

The program manager submits the draft PPP for approval only after the final MDCI threat assessment has been received from the applicable DoD Component CI and/or intelligence support activity. Normally, the MDCI threat assessment is returned to the requesting program office within 180 days of the CI and/or intelligence organization receiving the request.

The MDCI threat assessment answers the following questions about CPI:

- Which foreign interests might be targeting the CPI and why?
- What capabilities does each foreign interest have to collect information on the CPI at each location identified by the program office?
- Does evidence exist to indicate that a program CPI has been targeted?
- Has any CPI been compromised?

8.4.8 Technology Assessment / Control Plan (TA/CP)

8.4.8.1 General

The policy on TA/CP is in DoD Directive 5530.3

Prior to formal negotiation, the program manager prepares a TA/CP, or similar document, as part of the PPP for all acquisition programs with international involvement. The

TA/CP is included in the PPP when it is determined that there is likely to be foreign involvement in the development program or when there will be foreign access to the resulting system or related DS&TI or CPI, by virtue of foreign sales, co-production, follow-on support, exchange program, training, or multinational exercises or operations. Much of the information required for the preparation of the TA/CP can be obtained from the Initial Capabilities Document/Capability Development Document, the Analysis of Alternatives, the acquisition strategy, and the justification and supporting information used in preparing those documents.

8.4.8.2. Purpose

The program manager uses the TA/CP to do the following:

- Assess the feasibility of U.S. participation in joint programs from a foreign disclosure and technical security perspective.
- Prepare guidance for negotiating the transfer of classified information and critical technologies involved in international agreements.
- Identify security arrangements for international programs.
- Provide a basis for the DDL that contains specific guidance on proposed disclosures.
- Support the acquisition decision review process.
- Support decisions on foreign sales, co-production, or licensed production, commercial sales of the system, or international cooperative agreements involving U.S. technology or processes.
- Support decisions on the extent and timing of foreign involvement in the program, foreign sales, and access to program information by foreign interests.

When it is likely there will be foreign involvement in the program, or foreign access to the resulting system or related information, it is advantageous for the program manager to prepare the TA/CP after completing the identification of DS&TI, CPI, and security classification guidance. The TA/CP analysis often assists in developing vulnerabilities and proposed RTP countermeasures. Policies governing the foreign disclosure of intelligence information are in Director of Central Intelligence Directives (DCIDs) 1/7 and 5/6, information security products and information in National Security Telecommunications and Information Systems Security (NSTISS) Policy Number 8, and nuclear information governed by the Atomic Energy Act. These documents must be consulted when these types of information are involved in an acquisition program.

8.4.8.3. Content

The TA/CP is composed of four sections: the "Program Concept"; the "Nature and Scope of the Effort and the Objectives"; the "Technology Assessment"; and the "Control Plan." Those TA/CP subsections are the basis for preparing the DDL.

Program Concept. This section requires a concise description of the purpose of the acquisition program. It should describe, in the fewest words possible, the purpose of the

system and the system threat or the military or technical requirements that created the need for the system. The description must be consistent with the PPP.

Nature and Scope of Effort and the Objectives. This section briefly explains the operational and technical objectives of the program (e.g., co-production, cooperative research and development) and discusses any foreign participation or involvement. If foreign participation or involvement or the release of information to support potential foreign sales is considered likely, the phasing and disclosures at each phase should be described briefly. The milestones, foreign entities expressing interest, and summary of expected benefits to the U.S. should also be covered. The POC for all aspects of the TA/CP must be identified, including address, telephone numbers, and facsimile numbers.

Technology Assessment. The third section is the most important part of the TA/CP. It analyzes the technology involved in the program, its value, and the consequences of its compromise. It should provide conclusions regarding the need for protective security measures and the advantages and disadvantages of any foreign participation in the program, in whole or in part, and should describe foreign sales. The assessment should be specific concerning the phased release of classified and unclassified information that supports potential foreign involvement and foreign sales. Since preparation of this section requires a joint effort involving program management, security, intelligence, and foreign disclosure personnel, it may be a task for the RTP WIPT.

When the TA/CP is prepared in the early stages of program protection planning, emphasis should be placed on describing the value of the technology and systems in terms of military capability, the economic competitiveness of the U.S. industrial base and technology, susceptibility to compromise, foreign availability, and likely damage in the event of compromise.

This assessment should result in a conclusion on whether a cooperative program, co-production, or foreign sale will result in clearly defined operational or technological benefits to the United States, and whether these benefits would outweigh any damage that might occur if there should be a compromise or unauthorized transfer. Specific reasons must be provided.

This assessment should identify and explain any critical capability, information, or technology that must be protected. It may reveal that an adjustment to program phasing is necessary so critical information is released only when absolutely necessary. It should identify any CPI that may not be released due to the impact on the system's combat effectiveness. Additionally, it will identify the need for special security requirements such as a program-specific security plan to govern international involvement. The assessment should also evaluate the risk of compromise, based on the capability and intent of foreign participants or purchasers to protect the information, and the susceptibility of the system to compromise if not protected.

Finally, the assessment should discuss any known foreign availability of the information, system, or technology involved; previous release of the same or similar information, system, or technology to other countries; and, when foreign involvement or sales are recommended, its release to other participants.

Control Plan. The fourth section, together with the technology assessment, provides the basis for guidance on negotiating technical and security aspects of the program, and development of disclosure guidelines for subsequent sales and foreign participation in the program.

The Control Plan should describe actions that are to be taken to protect U.S. interests when foreign involvement or sales are anticipated. Those actions should be specific and address specific risks, if any, as discussed in the technology assessment. Actions might include withholding certain information, stringent phasing of releases, or development of special security requirements.

The plan should also identify any design or engineering changes that may be necessary or desirable to ensure the protection of CPI. The plan should describe how security provisions of an agreement and/or applicable regulations are to be applied to the specific program, agreement, or sale.

In preparation of the Control Plan, special consideration should be given to the export restrictions on sensitive technologies and materials amplified in DoD Instruction S-5230.28 and the National Disclosure Policy Committee's Policy Statement on "Foreign Release of Low Observable and Counter Low Observable Information and Capabilities (U)".

Delegation of Disclosure Authority Letter (DDL). The program manager must prepare a DDL as part of a recommendation for foreign involvement, disclosure of the program to foreign interests, request for authority to conclude an international agreement, or a decision to authorize foreign sales. NOTE: The DDL is not releasable to Foreign Nationals.

The DDL should provide detailed guidance on releasability of all elements of the system, to include its technology and associated information. The Security Classification Guide (SCG) will be consulted during the preparation of the DDL to establish its classification.

The program manager develops the DDL in accordance with DoD Directive 5230.11 enclosure 4. The applicable designated disclosure authority should agree with its content. The DDL is provided to the Milestone Decision Authority and the Office of the USD(P) for approval at each milestone. Until the DDL has been approved by the originating activity's designated disclosure authority, the Milestone Decision Authority, and the Office of the USD(P), there should be no promise to release, nor should there be actual release of, sensitive information or technology.

8.4.9. Contracting and Resources

Program protection planning may be outsourced and included in a contract. That contract activity may include initial program and system evaluation as well as program protection planning that leads to specific RTP countermeasures. Early planning is necessary to ensure that funds are programmed and budgeted to provide timely required contract support.

Program protection activities should begin prior to contract award. Delaying the process may result in safeguards being difficult to accomplish or being omitted from contracts. The program's underpinning DS&TI, and inherited or determined CPI, should be factored

into the program's overall acquisition strategy. The program manager is responsible for this planning and should prepare a budget for all security costs within the Planning, Programming, Budgeting, and Execution (PPBE) process and the program's Acquisition Program Baseline. It is more cost effective for security to be "baked in" early rather than "bolted on" later.

8.4.9.1. Early Coordination

As discussed in section 8.4.2, RTP is a subject for early coordination by the program manager's staff and contracting personnel to ensure contractual documents contain essential protection requirements. Early coordination is fundamental for having adequate coverage in contractual documents and to thus avoid additional and unnecessary costs due to late application of RTP requirements. The expected range of protection requirements and projected resources required should be estimated to ensure research and acquisition planning documents address RTP. RTP is also a subject for early coordination by FDOs.

8.4.9.2. Pre-Contract Award

The pre-award phase includes pre-solicitation, solicitation, source selection evaluation, and other pre-award activities.

Acquisition organizations generally have local instructions and related checklists to aid the program management staff in completing the actions necessary to arrive at a legal and successful contract award. Such instructions and checklists should be written and reviewed to ensure they address program protection activities and requirements.

The program manager should define program protection requirements early enough to be included in the draft request for proposal (RFP).

- The initial program management staff, with the assistance of the program protection POC, provides the responsible contracting office with information describing the nature and extent of program protection requirements that apply to the contemplated contract and estimates for the resources necessary to contractually execute the program. (See the information listed in subsection 8.4.6.)
- The program manager includes a program protection section in the RFP and should ensure that the appropriate Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) clauses have been activated for RTP (e.g., DFARS 242.402).

Once the proposals are received in response to the RFP, they will be evaluated using specified source selection criteria. The resulting evaluation should address the proposed ways of satisfying program protection requirements. The evaluation should also consider the cost to execute each proposed approach to satisfy the contractor portion of the PPP. An RTP specialist should be available to assist in the source selection process when proposals are required to address program protection requirements.

Approaches in the selected contractor's proposal documents should be incorporated into the contract. Action should be taken to ensure RTP provisions in the proposal are fully implemented by the prime contract.

The program manager should require the contractors to coordinate with the program office staff and CI support staff, all proposals to market or otherwise obtain a commercial export license to sell portions of the system being acquired or like systems to foreign countries. The PM should formalize this requirement in all Statements of Work for acquisition systems. A lack of coordination by the contractors may result in inadvertent transfer of critical military technology to unauthorized foreign nationals.

8.4.9.3. Post Contract Award

It is not unusual for contract modifications to be made reflecting fiscal or other program changes. As with pre-award actions, the program manager should ensure that the program office RTP representative works with the program management staff and the contracting officer if RTP changes are required.

A primary post award activity is "baselining" the contract. RTP actions are addressed in this activity and, if applicable, identified as a reportable item in the baseline. When used, the contractor program protection implementation plan (PPIP) forms a principal source for the contract RTP baseline.

The contracting officer representative (COR) is formally identified during post award activities and becomes the focal point, along with the program manager, for administering contract requirements, including RTP. The COR and the program manager need to understand how RTP is important to successful achievement of protecting the program cost, schedule, and performance objectives. The COR should discuss the security requirements with the FDO.

8.4.9.4. Contractor Performance Monitoring

The COR, along with the program manager and contracting officer (CO), are key to ensuring that RTP requirements are accomplished, particularly if there are any modifications to the contract. The RTP POC should monitor performance and schedule of RTP activities. As part of the program manager staff, the RTP POC works through the program manager, COR, and CO in accomplishing RTP goals. Any proposed contract modifications regarding foreign involvement should also be discussed with the FDO.

Planning for performance monitoring begins with RFP activities, pre-award issues, and continues with the contract baselining and any necessary re-baselining.

The contract baseline, once documented, will be the prime contractor performance measurement tool. That baseline is compared with periodic performance reports that address work accomplished as well as costs incurred and related task funding. When the work breakdown structure is developed, any RTP action identified in the statement of work, preliminary acquisition planning activities, or the RFP, is identified as a "reportable item"

8.4.9.5. Contractor Costs

To properly support contract activities, RTP costs are identified as part of the initial program definition and structuring. Those cost estimates are then used in the early contract development process, starting with drafting of the RFP.

Cost estimates are identified by category (i.e., personnel, products, services, equipment) to include any information systems requirements. Within each category of RTP costs, the items are further identified by security discipline.

Costs for implementing industrial security are included in the overhead portion of contractor costs. DoD security countermeasures are typically included in level-of-effort costs for DoD agencies. These costs should not be included in the PPP since they are not additive costs to the acquisition program. The baseline for standard security actions is determined before identifying program-specific RTP costs.

RTP costs for implementing foreign disclosure and/or national disclosure policies are also identified by the categories listed in the paragraphs above.

8.4.9.6. Providing Documentation to Contractors

The program manager, in coordination with the RTP POC and the contracting officer, determines when prime contractors, and subcontractors supporting the RTP effort, need access to CPI documentation. If a foreign contractor is involved, the Foreign Disclosure Officer (FDO) must participate in the coordination.

When a contractor is to be granted access to classified information, sensitive information, controlled unclassified information, For Official Use Only information, export-controlled data, or unclassified technical data, the contract will provide authorization for access to contractor facilities by the responsible government industrial security office (DSS or the DoD Component-cognizant security authority). That authorization is necessary to permit surveys, inspections, advice or assistance visits, or inquiries, which are necessary to ensure protection of sensitive information and implementation of RTP activities at prime, subcontractor, and/or vendor facilities.

Whenever possible, threat information (i.e., MDCI threat assessment) is shared with the cognizant contractor Facility Security Officer to ensure their understanding of the threat.

8.4.9.7. Support from Cognizant Government Industrial Security Offices

The contract DD Form 254, "DoD Contract Security Classification Specification," should specifically identify RTP assessments and reviews to be conducted by the responsible government industrial security office (e.g., DSS). The program manager should complete the DD 254 to reflect RTP protection measures and requirements. A copy of the DD 254 should be provided to the cognizant government security office (i.e., the appropriate DSS field office) so they may assist in RTP protection efforts. Organizations responsible for RTP reviews should:

- Conduct or participate in reviews and assistance visits at contractor facilities and contractor activities at government facilities. Reviews at contractor facilities in the United States assess compliance with contractually-imposed RTP measures, when contract provisions authorize such reviews and visits.

- Disseminate evaluation reports to appropriate acquisition program officials (e.g., Program Executive Officers, program managers, user organization officials). Unless specifically prohibited, the program manager provides reports to appropriate contractor personnel.

8.4.10. RTP Costing and Budgeting

Ultimately, the success of an acquisition program will depend on protecting the research and technology upon which the acquisition is based. RTP requirements should be incorporated into initial program funding and subsequent budget submissions to ensure adequate resources are committed at program initiation.

When RTP professionals are part of the program costing and budgeting processes, RTP requirements can be addressed during programming and budgeting cycles.

8.4.10.1. RTP Costing

Program resource managers are responsible for developing a Work Breakdown Structure and Cost Analysis Requirements Description as part of the overall costing process. The Cost Analysis Requirements Description is developed in concert with the Work Breakdown Structure and serves as the costing portion of the Work Breakdown Structure. Costs for material, personnel/labor, training, etc., are incorporated into a requirements document to define overall RTP costs. Security, counterintelligence, and intelligence professionals should be integrated into the program costing process at the earliest opportunity.

A separate Work Breakdown Structure category provides managers with visibility into RTP costs and actual funding available to support the RTP effort. A separate Work Breakdown Structure category is recommended for RTP requirements such as anti-tamper, system security engineering, information assurance, and the program protection implementation plan (PPIP).

8.4.10.2. RTP Budgeting

Once RTP cost requirements are properly estimated and documented, the next step in the process is their submission and validation as part of the program budgeting process. All RTP costing requirements are coordinated with the program resource manager who prepares budget submissions to the program manager.

Often, a validation board is assembled to review program costing requirements. This board validates the cost (verifies the methodology used to project the costs) and prioritizes program cost requirements. When RTP cost proposals are submitted, RTP professionals should be present to support these proposals to the validation board. RTP professionals should serve as advisors to the program manager for RTP costs coming from other organizations or from contractors.

Once a program budget is approved and the RTP requirement funded, establishing a separate RTP funding line item could be useful in tracking funds that are distributed to support RTP requirements.

RTP POCs who manage funding and/or the implementation of the PPIP are required to annually update their funding requirements and contribute to the overall program budget submission process. RTP costs will be validated each year.

8.4.11. Execution of the PPP

The program manager has the primary responsibility for PPP execution. Specific functions and actions may also be assigned to supporting security, CI, and intelligence organizations, as well as supporting acquisition organizations and defense contractors. Proper PPP execution depends on allocation of resources for planned RTP countermeasures and communication of the RTP countermeasures plan to applicable contractors, as well as to acquisition, security, CI, and intelligence activities supporting the program.

8.4.11.1. Distribution of the PPP

Once the PPP is approved, the program manager ensures all activities that are assigned RTP actions in the PPP receive a copy of the approved plan or those portions pertaining to their tasks. Organizations that should be considered for PPP distribution include the following:

- Program contractors having CPI under their control.
- Responsible government industrial security offices (i.e., DSS offices supporting the program at contractor sites covered by the PPP and/or the PPIP).
- DoD test ranges and centers applying CPI countermeasures.
- CI activities supporting program sites having CPI countermeasures applied.

If the program manager decides to limit distribution of the entire PPP, then, as a minimum, the CPI and RTP countermeasures portions should be distributed to the appropriate organizations.

8.4.11.2. Assessment of PPP Effectiveness

The program manager, assisted by security and CI activities, assesses PPP effectiveness, and the RTP countermeasures prescribed therein, as part of the normal program review process. Such assessments are planned considering the overall program schedule, the time-phased arrival or development of CPI at specific locations, and the schedule to revise the PPP.

8.5 Specialized Protection Processes

8.5.1 System Security Engineering

8.5.1.1 General

If the program manager decides to use system security engineering (SSE) it can be the vehicle for integrating RTP into the systems engineering process. Systems engineering activities prevent and/or delay exploitation of DS&TI and/or CPI in U.S. defense systems and may include Anti-Tamper (AT) activities (see section 8.5.3). The benefit of SSE is

derived after acquisition is complete by mitigation of threats against the system during deployment, operations, and support. SSE may also address the possible capture of the system by the enemy during combat or hostile actions.

8.5.1.2. System Security Engineering Planning

The program manager's System Engineering Plan (SEP) is the top-level management document used to describe the required systems engineering tasks. The System Security Management Plan (SSMP) is a detailed plan outlining how the SSE manager (SSEM) and the contractors will implement SSE, and may be part of the SEP.

The SSMP, prepared by the program manager, establishes guidance for the following tasks:

- Analysis of security design and engineering vulnerabilities; and
- Development of recommendations for system changes, to eliminate or mitigate vulnerabilities through engineering and design, any characteristics that could result in the deployment of systems with operational security deficiencies.

The SSMP is applicable to the acquisition of developmental or existing systems or equipment.

MIL-HDBK-1785 establishes the formats, contents, and procedures for the SSMP. Data Item Description (DID), DI-MISC-80839, SSMP, is applicable.

A System Security Engineering Working Group (SSEWG) defines and identifies all SSE aspects of the system, develops SSE architecture, reviews the implementation of the architecture, and participates in design validation. The SSEWG is formed as early in the acquisition process as possible, but not later than the Technology Development phase of the acquisition. The SSEWG is comprised of acquisition program office personnel; supporting CI, intelligence, and security personnel; system user representatives; and other concerned parties. The SSEWG provides recommendations to the program manager.

8.5.1.3. System Security Engineering Process

SSE supports the development of programs and design-to-specifications providing Lifecycle protection for critical defense resources. Activities planned to satisfy SSE program objectives are described in the SSMP.

SSE secures the initial investment by "designing-in" necessary countermeasures and "engineering-out" vulnerabilities, and thus results in saving time and resources over the long term. During the system design phase, SSE should identify, evaluate, and eliminate (or contain) known or potential system vulnerabilities from deployment through demilitarization.

The SSE process defines the procedures for contracting for an SSE effort and an SSMP. Implementation requires contractors to identify operational vulnerabilities and to take action to eliminate or minimize associated risks.

Contract Data Item Descriptions (DIDs) and Contract Data Requirements Lists (CDRLs) may be tailored to the acquisition program in order to obtain contractor-produced plans or studies that satisfy specific program needs.

8.5.1.4. Military Handbook 1785

MIL-HDBK-1785 contains procedures for contracting an SSE effort and an SSMP. The format and contents are outlined in the appropriate Data Item Descriptions (DIDs) listed in MIL-HDBK-1785.

The proponent for the handbook is Commander, Naval Air Systems Command, ATTN: AIR-7.4.4., 22514 McCoy Road, Unit 10, Patuxent River, MD 20670-1457.

8.5.1.5. Security Engineering for International Programs

SSE should include an assessment of security criteria that sets limits for international cooperative programs, direct commercial sales, and/or foreign military sales (FMS) cases. From this assessment, engineering and software alternatives (e.g., export variants, AT provisions) should be identified that would permit such transactions.

8.5.2. Counterintelligence Support Plan

The CISP defines specific CI support to be provided to the RDT&E facility or acquisition program and provides the servicing CI personnel with information about the facility or program being supported.

- A tailored CISP is developed for every DoD RDT&E activity and for each DoD acquisition program with identified CPI;
- RDT&E site directors, security managers, and supporting CI organizations are responsible for developing a CISP for each RDT&E facility;
- Program managers and their supporting security and CI organizations are responsible for developing a CISP for each acquisition program with CPI. The CPI will be prioritized and listed in the CISP;
- The CISP is signed by local CI and site management personnel, the program manager, and the local DSS representative, as appropriate. The CISP will specify which of the CI services will be conducted in support of the facility or program, and will provide the CI personnel with information about the program or facility to help focus the CI activities. A copy of the signed plan is provided to the DoD Component CI headquarters;
- The CISP will be reviewed annually, or as required by events. It will be used as the baseline for any evaluation of the program or facility and its supporting CI program; and
- Any updated CISP is redistributed to those providing support.

8.5.2.1. CI Actions at RDT&E Activities

Component CI agencies have identified a core listing of CI services that are recommended for each CISP.

- If there is DS&TI at a RDT&E site, the site director-approved CISP is provided to the DoD Component CI specialists working at the RDT&E site;

- If there is CPI at a RDT&E site, the program manager-approved CISP is provided to the DoD Component CI specialists working at the site and will become an annex to the site CISP;
- If DS&TI or CPI is identified at a DoD contractor facility, the program manager, CI specialist, the DSS CI specialist, and the contractor develop a CISP annex to define CI support to the contractor; and
- If RDT&E site management identifies DS&TI or CPI requiring specialized CI support beyond what is covered in the project or program CISP, that additional support is documented as an annex to the site CISP.

Component CI personnel keep the project or program manager CI POC informed of threat and other information that could adversely impact the DS&TI or CPI. The CI POC is responsible for keeping the program manager or site director apprised of current CI activities.

When more than one Component CI agency has an interest at the same RDT&E site or contractor facility, teaming, and cooperation should occur at the lowest possible organizational level. If a conflict occurs that cannot be resolved by the DoD Components, information on the conflict is sent to the Deputy Undersecretary of Defense (Counterintelligence and Security), OUSD(I), for review and resolution.

8.5.2.2. Counterintelligence Support to Acquisition Programs

Component CI organizations should identify a CI specialist to acquisition program managers with CPI. The CI specialist should:

- Participate in the RTP WIPT that develops the PPP and is responsible for developing the CISP and obtaining the MDCI Threat Assessment for the program;
- Ensure CI RTP requirements flow to CI and security personnel at locations where the CPI is used, handled, stored, or tested;
- Ensure the program manager and the program office staff are aware of current threat information; and
- Provide specialized CI support to all locations pursuant to the CISP.

Field CI personnel should:

- Provide CI RTP support when the weapons system or other platform becomes operational for as long as CPI is designated; and
- Provide CI support for as long as the CPI is so designated.

8.5.3 Anti-Tamper

8.5.3.1 General

- Program managers should develop and implement Anti-Tamper (AT) measures to protect DS&TI and/or CPI in U.S. defense systems developed using co-development agreements; sold to foreign governments; or no longer within U.S. control (e.g., theft, battlefield loss). AT techniques may be applied to system

performance, materials, hardware, software, algorithms, design, and production methods, or maintenance and logistical support. Although protective in nature, AT is not a substitute for program protection or other required security measures;

- AT adds longevity to a critical technology by deterring reverse engineering. AT also provides time to develop more advanced technologies to ensure previously successful hostile exploitation of a defense system does not constitute a threat to U.S. military forces and capabilities. Although AT may not completely defeat exploitation, it will make hostile efforts time-consuming, difficult, and expensive;
- AT is initiated as early as possible during program development, preferably in the program concept refinement and technology development phases, in conjunction with the identification of program DS&TI and/or CPI:
    - AT is also applicable to DoD systems during a Pre-Planned Product Improvement (P3I) upgrade or a deployed system technology insertion; and
    - Additionally, AT should be specifically addressed in all transfer or sales of fielded systems and in direct commercial sales to foreign governments.
- AT resource requirements may affect other aspects of a program, to include end item cost, schedule, and performance;
- AT also involves risk management. A decision not to implement AT should be based on operational risks as well as on acquisition risks, to include: AT technical feasibility, cost, system performance, and scheduling impact;
- The DoD Executive Agent for AT resides with the Department of the Air Force, which is responsible for:
    - Managing AT Technology Development;
    - Implementing Policy;
    - Developing an AT databank / library;
    - Developing a Technology Roadmap;
    - Providing Proper Security Mechanisms; and
    - Conducting AT Validation.
- The AT Executive Agent sets up a network of DoD Component AT points of contact to assist program managers in responding to AT technology and/or implementation questions. Additionally, DoD Component POCs coordinate AT development and create a shared common databank / library; and
- Since AT is a systems engineering activity, AT is strengthened when integrated into a program sub-system(s), and is more cost effective when implemented at program onset.

8.5.3.2. Application of AT

- With the aid of the DoD Component AT POC, the program manager should determine the appropriate number of AT layers to be employed on the program using a risk assessment of the CPI. The evaluation may indicate there is no requirement to apply AT techniques. However, a final decision should not be made until completing thorough operational and acquisition risk analyses;
- AT applicability should be assessed for each major modification or P3I upgrade to the production system and for any FMS of fielded systems or direct commercial sale. It is feasible that AT may be inserted into the modified or upgraded systems when protection is required. AT may be discontinued when it is determined the technology no longer needs protection; and
- The program manager recommendation whether or not to implement AT should be approved by the Milestone Decision Authority and documented in the Program Protection Plan (PPP).

8.5.3.3. AT Implementation

- The program manager should document the analysis and recommendation in the classified AT plan (an annex to the PPP), of whether or not to use anti-tamper measures. The PPP with the AT annex should be included in the submission for Milestone B, and updated for Milestone C. The AT Executive Agent, or any DoD Component-appointed AT Agent, provides an evaluation of the AT plan and a letter of concurrence to the Milestone Decision Authority;
- The AT classified annex to the PPP contains AT planning. The planning detail should correspond to the acquisition phase of the program;
- The AT annex includes, but is not limited to, the following information:
    - Identification of the critical technology being protected and a description of its criticality to system performance;
    - Foreign Teaming and foreign countries / companies participating;
    - Threat assessment and countermeasure attack tree;
    - AT system level techniques and subsystem AT techniques investigated;
    - System maintenance plan with respect to AT;
    - Recommended solution to include system, subsystem and component level;
    - Determination of how long AT is intended to delay hostile or foreign exploitation or reverse-engineering efforts;
    - The effect that compromise would have on the acquisition program if AT were not implemented;
    - The estimated time and cost required for system or component redesign if a compromise occurs;
    - The program manager recommendation and the Milestone Decision Authority decision on AT; and

    - The program AT POC.
- AT is reflected in system specifications and other program documentation; and
- AT, whether implemented or not, should be a discussion item during Milestone B, Milestone C (Low-Rate Initial Production), and Full-Rate Production Decision Reviews:
    - At Milestone B, the program manager should address AT in conceptual terms and how it is to be implemented. Working AT prototypes, appropriate to this stage of program development, should be demonstrated. Deliverables at Milestone B include: a list of critical technologies/information; a MDCI threat analysis; a list of identified vulnerabilities; identified attack scenarios; impacts if exploited; available AT techniques; and a preliminary AT Plan. These deliverables are submitted and incorporated into the AT Annex of the PPP; and
    - At Milestone C, the program manager should fully document AT implementation. Deliverables at Milestone C include: all deliverables from Milestone B and any updates; an analysis of AT methods that apply to the system, including cost/benefit assessments; an explanation of which AT methods will be implemented; and a plan for verifying and validating (V&V) AT implementation. These deliverables are submitted and incorporated into the AT annex of the PPP. Testing during developmental test and evaluation (DT&E) and operational test and evaluation (OT&E) is highly encouraged for risk reduction.

8.5.3.4. AT Verification and Validation (V&V)

AT implementation is tested and verified during DT&E and OT&E.

The program manager develops the validation plan and provides the necessary funding for the AT V&V on actual or representative system components. The V&V plan, which is developed to support Milestone C, is reviewed and approved by the AT Executive Agent, or any Component-appointed AT Agent, prior to milestone decision. The program office conducts the verification and validation of the implemented AT plan. The AT Executive Agent witnesses these activities and verifies that the AT plan is implemented into the system and works according to the AT plan. The program manager and the AT Executive Agent may negotiate for parts of the system that have undergone anti-tamper measures to be tested at the AT Executive Agent's laboratories for further analysis. The validation results are reported to the Milestone Decision Authority.

8.5.3.5. Sustainment of AT

AT is not limited to development and fielding of a system. It is equally important during life cycle management of the system, particularly during maintenance.

AT measures should apply throughout the life cycle of the system. Maintenance instructions and technical orders should clearly indicate that AT measures have been implemented; indicate the level at which maintenance is authorized; and include warnings that damage may occur if improper or unauthorized maintenance is attempted.

To protect CPI, it may be necessary, as prescribed by the DDL, to limit the level and extent of maintenance a foreign customer may perform. This may mean that maintenance involving the AT measures will be accomplished only at the contractor or U.S. Government facility in the U.S. or overseas. Such maintenance restrictions may be no different than those imposed on U.S. Government users of AT protected systems. Contracts, purchase agreements, memoranda of understanding, memoranda of agreement, letters of agreement, or other similar documents should state such maintenance and logistics restrictions. When a contract that includes AT protection requirements and associated maintenance and logistics restrictions also contains a warranty or other form of performance guarantee, the contract terms and conditions should establish that unauthorized maintenance or other unauthorized activities:

- Should be regarded as hostile attempts to exploit or reverse engineer the weapon system or the AT measure itself; and
- Should void the warranty or performance guarantee.

The U.S. Government and U.S. industry should be protected against warranty and performance claims in the event AT measures are activated by unauthorized maintenance or other intrusion. Such unauthorized activities are regarded as hostile attempts to exploit or reverse engineer the system or the AT measures.

8.5.3.6. Guidelines for AT Disclosure

The fact that AT has been implemented in a program should be unclassified unless the appropriate original classification authority of the DoD Component, in consultation with the program Milestone Decision Authority, decides that the fact should be classified.

The measures used to implement AT will normally be classified, including any potential special handling caveats or access requirements. The AT implementation on a program should be classified from SECRET / US ONLY (minimum) to SECRET / SAR per the AT security classification guide. Classified AT information, including information concerning AT techniques, should not be disclosed to any unauthorized individual or non-U.S. interest pursuant to decisions made by appropriate disclosure authorities.

Disclosure decisions should take into account guidance and recommendations from the program OCA, in consultation with the program Milestone Decision Authority, and those of USD(AT&L). The program Milestone Decision Authority coordinates all foreign disclosure releases involving AT with the cognizant foreign disclosure authority and security assistance office, as appropriate. An exception to National Disclosure Policy may be warranted for co-development programs, foreign military sales, or direct commercial sales.

8.5.4. Information Assurance

All information systems (including network enclaves) storing, processing, or transmitting DS&TI must comply with the requirements of DoD Directive 8500.1 "Information Assurance (IA)" and implement the appropriate IA controls from DoD Instruction 8500.2 "Information Assurance Implementation". Accordingly, these systems will be accredited in accordance with DoD Instruction 5200.40 "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)". The DITSCAP establishes a

standard process, set of activities, general task descriptions, and a management structure to certify and accredit IT systems throughout the system life cycle. A product of the DITSCAP, the System Security Authorization Agreement (SSAA), documents the agreement between the project manager, the Designated Approval Authority (DAA), the Certification Authority (CA), and the user representative concerning schedule, budget, security, functionality, risk, and performance issues. Applicable SSAAs will be included as annexes to the PPP. Associated costs will be recorded in the PPP by fiscal year. For information systems where the program office is not the owner of the system but simply a user of the system, the PPP should include a copy of the system's Approval to Operate (ATO) issued by the system DAA.

It is important to differentiate between the implementation of information assurance with regards to program support systems processing DS&TI and other CPI, as opposed to the implementation of information assurance in the system being acquired. For example, a hypothetical acquisition program office acquiring a new weapons system (or AIS) may have an information system that supports the storing, processing and transmitting of DS&TI. The information assurance requirements and certification and accreditation requirements for that support system are totally separate and distinct from those of the weapons system being acquired. Chapter 7, Acquiring Information Technology and National Security Systems, provides specific guidance on the identification and implementation of information assurance requirements for all systems being acquired.

8.5.5. Horizontal Analysis and Protection

The objective of horizontal analysis and protection activities is to ensure consistent, cost-effective application of similar RTP safeguards for similar DS&TI and/or CPI throughout DoD.

- CIFA conducts horizontal analysis to determine whether similar technologies are being used in different programs;
- Program managers, Program Executive Officers, and Milestone Decision Authorities should assist in these analyses to ensure that similar technologies are safeguarded with the same level of protection, (i.e., horizontal protection); and

The USD(I), the USD(AT&L), and the DOT&E provide oversight of the effectiveness of horizontal analysis and protection as outlined in DoD Directive 5200.39.

8.5.5.1. Horizontal Analysis

The CIFA-conducted horizontal analysis should address the following:

- System enabling technologies (DS&TI and/or CPI) and their additional applications, whether for similar or dissimilar tasks;
- RTP safeguards planned or provided;
- Intelligence estimates of competitive foreign acquisition efforts; and
- Reports of completed investigations of compromises, espionage cases, and other losses.

DoD Components should establish processes that support horizontal analysis and protection activities. DoD Components should:

- Identify system enabling technologies and their additional applications, whether for similar or dissimilar tasks;
- Review security classification guides of existing programs or projects when developing a CISP or PPP to determine classification of similar technologies used in other programs or under development; and
- Catalogue, analyze, group, and correlate protection requirements within approved PPPs or CPI for DS&TI involving similar enabling technologies. Provide the data collected to the CIFA for their use.

8.5.5.2. Horizontal Protection

CIFA will provide their analysis report to the site director for emerging technologies and/or to the program manager for their application within an acquisition program. Site directors or program managers should ensure their respective CISP and PPP are modified when required based upon results of the horizontal analysis.

CIFA will coordinate all reported or discovered discrepancies with the appropriate DoD Components for resolution at the lowest possible organizational level.

When necessary, CIFA will report unresolved or inconsistent applications of RTP safeguards to the USD (AT&L), DOT&E, and USD (I) for resolution. Copies of these reports will be provided to the DoD Inspector General (IG).

8.5.5.3. Reporting Requirements

Compromise of DS&TI or CPI will be reported through CI channels to CIFA and the USD(I), in accordance with DoD Instruction 5240.4

8.5.6. RTP Assessments and Inspections

Periodic assessments and inspections of RTP activities (encompassing all DoD RDT&E budget categories) are necessary to ensure effective RTP is being planned and implemented. The DoD Component responsible for the RDT&E site or the acquisition program is responsible for these assessments and inspections (DoD Directive 5200.39).

8.5.6.1. Assessments

DoD Components periodically assess and evaluate the effectiveness of RTP implementation by RDT&E site directors and program managers as well as the support provided by security, intelligence, and CI to RDT&E sites and acquisition programs with DS&TI or CPI.

8.5.6.2 Inspections

The DoD Inspector General (IG) has established a uniform system of periodic inspections, using the existing DoD Components' inspection processes for RDT&E sites, to ensure compliance with directives concerning security, RTP, and CI practices.

The DoD IG has developed RTP inspection guidelines for use by DoD and DoD Component Inspectors General to enhance consistent application of directives that apply to RTP directives and related issuances.

DoD Component IGs conduct periodic inspections, using the DoD IG inspection guidelines, of RDT&E sites and acquisition programs for compliance with RTP directives. These inspections assess program manager compliance with section 8.4.11.2, Assessment of PPP Effectiveness. Participating Inspectors General may modify or customize the DoD IG inspection guidelines to account for Military Department-specific approaches to security, technology protection, and counterintelligence.

The DoD IG conducts periodic audits of DoD Component IG inspections for compliance with RTP directives and related issuances.

CHAPTER 9

Integrated Test and Evaluation

9.0 Overview

9.0.1. Purpose

This chapter will help the program manager develop a robust, integrated T&E strategy to assess operational effectiveness and suitability and support program decisions.

9.0.2. Contents

Section 9.1 provides an introduction of general topics associated with T&E. Section 9.2 then presents an overview of the T&E support and oversight provided by the Offices of the Director, Operational Test and Evaluation (DOT&E); and the Under Secretary of Defense for Acquisition, Technology, and Logistics/Defense Systems/Systems Engineering (USD(AT&L)/DS/SE). The next few sections focus on specific types of T&E: Developmental Test and Evaluation, Operational Test and Evaluation, and Live Fire Test and Evaluation. Section 9.6 covers T&E planning and specifically addresses the T&E Strategy and the Test and Evaluation Master Plan. Section 9.7 covers T&E Reporting; section 9.8 presents best practices; and section 9.9 covers special topics. Section 9.10 closes with details of preparing a Test and Evaluation Master Plan.

9.1 Introduction to Test and Evaluation (T&E)

DoD Instruction 5000.2 requires that test and evaluation programs be structured to provide accurate, timely, and essential information to decision makers for programs in all acquisition categories throughout the system lifecycle. As the means to this goal, T&E is to identify and learn about deficiencies (technical or operational) so that they can be resolved prior to production and deployment. DT&E supports: the systems engineering process to include providing information about risk and risk mitigation; assessing the attainment of technical performance parameters; providing empirical data to validate models and simulations and information to support periodic technical performance and system maturity evaluations. Operational Assessments (OAs) are conducted early in a program to provide insight into potential operational problems and progress toward meeting desired operational effectiveness and suitability capabilities. OT&E is conducted to determine system operational effectiveness, suitability, and survivability. LFT&E permits the evaluation of system survivability in the context of vulnerability to realistic threat munitions and/or system lethality against realistic threat targets. This chapter provides DoD guidance to program managers for use in planning and executing an integrated T&E program within their programs.

The program manager should develop a robust, integrated T&E strategy for developmental test and evaluation (DT&E), operational test and evaluation (OT&E), and live fire test and evaluation (LFT&E) to validate system performance and ensure that the product provides measurable improvement to operational capabilities. However, the integrated approach should not compromise DT&E, OT&E, or LFT&E objectives. The program manager, in concert with the user and test communities, without compromising

rigor, is required to integrate modeling and simulation (M&S) activities with government and contractor DT&E, OT&E, LFT&E, system-of-systems interoperability and performance testing into an efficient continuum. Testing shall be event driven within the program's overall acquisition strategy, and allow for a realistic period of time in which to accomplish the planned T&E events, including report preparation. The program manager should develop a robust DT&E effort to ensure the goal of achieving a successful OT&E outcome. The program manager is required to develop metrics (hardware and software), in the form of T&E success criteria and OT&E entrance criteria in consultation with the OTA, to use in monitoring program maturity and to support decisions to progress through the development cycle. T&E Working-level Integrated Product Teams (T&E WIPT), may include representatives from Program Management Offices, T&E agencies, operational users, the OSD staff, DoD Component staffs, the intelligence community, and other agencies as necessary to assist in this task.

9.1.1. Evolutionary Acquisition

The T&E Strategy of a system acquired using evolutionary acquisition shall address each increment intended for fielding. In general, T&E that has previously confirmed the effectiveness and suitability of a previous increment need not be repeated in its entirety to confirm that the subsequent increment still provides those mission capabilities previously confirmed. However, regression testing to reconfirm previously tested operational capabilities and/or suitability might be required if the subsequent increment introduces a significantly changed hardware or software configuration, or introduces new functions, components, or interfaces that could reasonably be expected to alter previously confirmed capabilities.

9.1.2. Joint Capabilities Integration and Development System

Joint Capabilities Integration and Development System implementation is based on Joint Operating Concepts and Joint Integrating Concepts to define gaps, overlaps, and redundancies in joint mission capability, which in turn could result in a new materiel solution. We can expect to see effects of Joint Capabilities Integration and Development System on T&E, such as the need for more system-of-systems testing. T&E will need to assess whether systems deliver their intended capability within the applicable functional capabilities area. There will be a need to consider realistic test environments to represent the functional capabilities area, to assess an individual system's contribution to joint mission capability.

9.1.3.. Relationship of Joint Capabilities Integration and Development System Documents to T&E

9.1.3.1. Initial Capabilities Document (ICD)

The broad, time-phased, operational goals and requisite mission capabilities found in the Initial Capabilities Document drive the initial T&E Strategy development that becomes codified in the Test and Evaluation Strategy (TES). Because the Initial Capabilities Document statement of desired capabilities is broad, the TES may also be a broad, general discussion of the program's T&E Strategy. (See CJCSI 3170.01.)

9.1.3.2. Capability Development Document

The Capability Development Document builds on the Initial Capabilities Document by refining the integrated architecture and providing more detailed operational mission performance parameters necessary to design the proposed system. As the Capability Development Document is being developed to support Milestone B, and typically program initiation, the T&E WIPT concurrently transforms the TES, using the maturing Capability Development Document as a basis, into a more comprehensive T&E Strategy that is documented in the Test and Evaluation Master Plan (TEMP). This process involves adding details (specific, desired, operational capabilities; T&E events (DT&E, OT&E, and LFT&E) adding to the broad, initial T&E Strategy; Critical Operational Issues; refining the management structure and composition of the T&E WIPT; identifying resource requirements more precisely; etc.) as they become available. Because the Capability Development Document normally is not approved until around the time of Milestone B, the T&E WIPT will most likely have to work from a draft version, since the initial TEMP is also due at Milestone B.

9.1.3.3. Capability Production Document (CPD)

The final step in the capabilities refinement process is the Capability Production Document development, with the Capability Production Document due at Milestone C. The refined, desired operational capabilities and expected system performance contained therein are used by the T&E WIPT to update the TEMP for the Milestone C decision and for subsequent updates later in Production and Deployment, such as the full rate production decision review. At Milestone C, the technical testing begins to focus on production testing, such as Production Qualification Testing, to demonstrate performance of the production system in accordance with the contract. Operational testing focuses on evaluating the system's operational effectiveness, suitability, and survivability.

9.1.4. Network-Centric Operations

Implementation of the Department's transformation strategy, calling for shifting to an information-age military, will result in fewer platform-centric and more network-centric military forces. This requires increased information sharing across networks.

The network-centric concept applies to a DoD enterprise-wide information management strategy that includes not only military force operations but also all defense business processes, such as personnel actions, fuel purchases and delivery, commodity buying, deployment activities, acquisition and development. Key tenets of the strategy include: handle information only once, post data before processing it, users access data when it is needed, collaborate to make sense of data, and diversify network paths to provide reliable and secure network capabilities.

The shift away from point-to-point system interfaces to network-centric interfaces brings implications for the T&E community. For example, previously, emphasis has been on testing interoperability between two or more platforms and their capability to exchange specifically required information. With network-centric operations, the emphasis will gradually shift to testing an integrated architecture for information processing necessary to achieve required force capabilities. The challenge to the test community will be to

represent the integrated architecture in the intended operational environment for test. Furthermore, the shift to network-centric capabilities will evolve gradually, no doubt with legacy point-to-point interfaces included in the architectures. Program managers, with their Program Executive Officer support, are strongly encouraged to work with the operating forces to integrate operational testing with training exercises, thereby bringing more resources to bear for the mutual benefit of both communities.

It is imperative that the T&E community engages the user community to assure that test strategies reflect the intended operational architectures and interfaces within which the intended capabilities are to be tested and evaluated.

9.1.5. Integrated T&E Philosophy

Integrating T&E consists of many aspects, all designed to optimize test scope and minimize cost. For example, separate contractor developmental testing might be combined with governmental developmental test and evaluation, with control being exercised by a combined test organization. Live testing might be integrated with verified, validated, and accredited simulators or computer driven models and simulations, to optimize the amount of live testing required. Another aspect is integrating developmental test and evaluation with operational test and evaluation into a continuum that reduces testing resource requirements and time, or conducting concurrent DT and OT when objectives and realism are compatible. Another approach is to combine DT and OT, discussed in paragraph 9.3.3 below, into a single test event, with data provided to developmental and operational evaluators equally. There is no single solution that is optimum for all programs, but each program should consider these approaches during initial T&E planning.

9.1.6. Systems Engineering and T&E

Systems engineering is discussed in depth in Chapter 4 of this Guidebook. In essence, systems engineering is a process to transform required operational capabilities into an integrated system design solution. As the design solution evolves, a verification component of the systems engineering process must provide confidence that the design solution properly addresses the desired capabilities, as intended.

T&E is the mechanism for accomplishing verification in the SE process and characterizing technical risk of achieving a proper final design solution.

9.1.7. Environment, Safety, and Occupational Health

The T&E Strategy and TEMP should address the program manager's analysis of residual Environmental, Safety and Occupational Health (ESOH) risks and control measures, to include safety releases, for the system or item. The intent is to ensure that, prior to OT&E and fielding, the testers and users understand the ESOH hazards, the control measures adopted by the program manager, and the residual risks accepted by the program manager. Early participation of ESOH expertise on the T&E WIPT is recommended to assure appropriate issues are addressed during test planning and execution.

The program manager must ensure compliance with National Environmental Policy Act (NEPA)/E.O. 12114 requirements, particularly as they affect test ranges and operational areas. The T&E Strategy and TEMP should include NEPA/E.O.12114 documentation requirements, and describe how analyses will be conducted to support test site selection decisions.

DoD Instruction 5000.2, E5.1 requires the program manager to provide safety releases to developmental and operational testers prior to any test using personnel. A Safety Release communicates to the activity or personnel performing the test the risks associated with the test, and the mitigating factors required, ensuring safe completion of the test. A secondary function of the process is to ensure that due diligence is practiced with respect to safety in the preparation of the test by the sponsor. A Safety Release is normally provided by the program manager after appropriate hazard analysis. Safe test planning includes analysis of the safety release related to test procedures, equipment, and training. A full safety release is expected before IOT&E.

9.2. OSD Responsibilities

There are three organizations within the Office of the Secretary of Defense that have policy and oversight responsibilities for T&E within the Department. They are (1) the Director, Operational Test and Evaluation (DOT&E), who is the Principal Staff Assistant and advisor to the Secretary and the Deputy Secretary of Defense for the responsibilities and functions described below, and within the System Engineering Directorate of Defense Systems OUSD(AT&L), (2) the Deputy Director, Developmental Test and Evaluation (DT&E) who is responsible for developing DT&E policies and procedures, and (3) the Deputy Director, Assessments and Support (AS) who has direct interface with program managers on DT&E. These offices share or coordinate on the following responsibilities:

- Provide advice and make recommendations to the Secretary and Deputy Secretary of Defense and the USD(AT&L) and support OIPTs and DABs/ITABs for programs on the OSD T&E Oversight List;
- Develop, in consultation with the DoD Components, the OSD T&E Oversight List;
- Ensure the adequacy of test strategies and plans for programs on the OSD T&E Oversight List;
- Attend design readiness reviews;
- Monitor and review DT&E, OT&E, and LFT&E events of oversight programs;
- Participate in the operational test readiness process by providing recommendations about a system's readiness for OT&E;
- Provide independent performance, schedule, and T&E assessments to the DAES process; and
- Provide representatives to the T&E WIPT of oversight programs to assist program managers in developing their T&E Strategy and preparing the Test and Evaluation Strategy (TES) and Test and Evaluation Master Plan (TEMP).

9.2.1. Specific Responsibilities of the Director, Operational Test and Evaluation (DOT&E)

Specific responsibilities of the DOT&E are listed in DoD Directive 5141.2. For additional information on the DOT&E office and its functions, go to http://www.dote.osd.mil/.

9.2.2. Specific Responsibilities of the Office of the Deputy Director, Developmental Test and Evaluation (DD,DT&E)

Two offices in Defense Systems, both reporting to the Director, Systems Engineering, have DT&E responsibilities. The DS/SE/DTE office responsibilities are described on their website. The DS/SE/Assessments and Support (AS) office has direct interface with program managers. This office formally receives, staffs, and concurs on the TES and the TEMP, both described in section 9.6. Additionally, SE/AS recommends TES and TEMP approval to OIPT leaders, and advises OSD executive leadership on the adequacy of the DT&E of acquisition programs and the readiness of the program for IOT&E.

9.2.3. OSD T&E Oversight List

The DOT&E and the D, DS jointly, and in consultation with the ASD(NII), the DoD Component T&E executives, and other offices as appropriate, publish an annual OSD Test and Evaluation Oversight List. Programs on the list can be designated for DT&E, OT&E, and/or LFT&E oversight. Any program, regardless of Acquisition Category level, can be considered for inclusion, and can be added to or deleted from the list at any time during the year. The current list can be obtained at the DOT&E Website). OSD criteria for determining whether or not a program should be on formal T&E oversight include:

- Acquisition category level;
- Potential for becoming an acquisition program (such as an Advanced Concept Technology Demonstration project or pre-MDAP);
- Stage of development or production;
- Whether program is subject to DAES reporting;
- Congressional and DoD interest;
- Programmatic risk (cost, schedule, performance);
- Past history of the developmental command with other programs;
- Relationship with other systems as part of a system-of-systems; and
- Technical complexity of system.

9.3. Developmental Test and Evaluation

9.3.1. DT&E Guidelines

A well planned and executed DT&E program supports the acquisition strategy and the systems engineering process, providing the information necessary for informed decision making throughout the development process and at each acquisition milestone. DT is the

verification and validation of the systems engineering process and must provide confidence that the system design solution is on track to satisfy the desired capabilities. The T&E strategy should be consistent with and complementary to the Systems Engineering Plan. The T&E functional team should work closely with the system design team to facilitate this process. Rigorous component and sub-system developmental test and evaluation (DT&E) ensures that performance capability and reliability are designed into the system early. DT&E then should increase to robust, system-level and system-of-systems level testing and evaluation, to ensure that the system has matured to a point where it can meet IOT&E and operational employment requirements.

Robust DT&E reduces technical risk and increases the probability of a successful OT&E. During early DT&E, the test responsibility may fall to the prime contractor who will focus testing on technical contract specifications. To ensure that the systems engineering verification and validation relates back to user required capabilities, it is appropriate for government testers to observe the contractor testing and, when appropriate, to facilitate early involvement and contribution by users in the design and test processes. The program manager's contract with industry should support an interface between government testers and users with the contractors' testing. Commercial items, regardless of the manner of procurement, undergo DT&E to verify readiness to enter IOT&E, where operational effectiveness, suitability, and survivability for the intended military application are demonstrated. Programs should not enter IOT&E unless the DoD Components are confident of success.

Program managers are required to develop and fund a T&E Strategy that meets the following objectives:

- Perform verification and validation in the systems engineering process;
- Develop an event-driven T&E Strategy, rather than a schedule-driven one, to ensure program success (required, DoD Instruction 5000.2);
- Identify technological capabilities and limitations of alternative concepts and design options under consideration to support cost-performance tradeoffs (required by DoD Instruction 5000.2). The intent is to avoid locking onto one solution too early;
- Identify and describe design technical risks (required by DoD Instruction 5000.2). The T&E Strategy should naturally flow from the systems engineering processes of requirements analysis, functional allocation, and design synthesis. For further explanation of this systems engineering flow-down, refer to paragraph 9.1.6 of this Guidebook;
- Stress the system under test to at least the limits of the Operational Mode Summary/Mission Profile, and for some systems, beyond the normal operating limits to ensure the robustness of the design (required by DoD Instruction 5000.2). This will ensure expected operational performance environments can be satisfied;
- Assess technical progress and maturity against Critical Technical Parameters (CTPs), including interoperability, documented in the TEMP (required by DoD Instruction 5000.2). As part of an event-driven strategy, the use of success criteria

is a suggested technique with which program managers can meet this requirement. Success criteria are intermediate goals or targets on the path to meeting the desired capabilities. There are two uses of success criteria. First, they can be used to assess technical progress and maturity against CTPs. Second, they can be used as metrics to assess successful completion of a major phase of developmental testing, such as a major phase of ground testing or of flight testing, and determine readiness to enter the next phase of testing, whether developmental or operational. In the case of operational testing, these success criteria are tantamount to OT&E entrance criteria (required by DoD Instruction 5000.2) which are required for all operational tests. Technical parameters, such as levels of reliability growth or software maturity, increasing levels of weapons system accuracy, mission processing timelines, and the like, can be used as success criteria to assess technical progress. Alternatively, in the case of an event success criterion such as completion of the first set of missile test firings, the criteria can be a specified level of success, such as a percentage of successful missile firings from this group. Failure to meet this criterion might cause the program manager to decide on additional firings prior to transitioning to the next phase of testing. A program manager can use a combination of both types of success criteria and tailor them to best fit the program's T&E Strategy;

- Assess the safety of the system or item to ensure safe operation during OT&E, other troop-supported testing, operational usage, and to support success in meeting design safety criteria (required by DoD Instruction 5000.2). The intent is to ensure that developmental systems are sufficiently free of hazards to prevent injury to the typical users participating in OT&E and fielding;
- Provide data and analytic support to the decision process to certify the system ready for OT&E (required by DoD Instruction 5000.2). These data are provided in the DT&E report discussed below;
- Conduct information assurance testing on any system that collects, stores, transmits, and processes unclassified or classified information. The extent of IA testing depends upon the assigned Mission Assurance Category and Confidentiality Level. DoD Instruction 8500.2 mandates specific IA Control Measures that a system should implement as part of the development process. (required by DoD Instruction 5000.2);
- In the case of IT systems, including NSS, support the DoD Information Technology Security Certification and Accreditation Process and Joint Interoperability Certification process (required by DoD Instruction 5000.2)
- Discover, evaluate, and mitigate potentially adverse electromagnetic environmental effects (E3). (required by DoD Directive 3222.4)
- Support joint interoperability assessments required to certify system-of-systems interoperability; (required by DoD Directive 4630.5)
- In the case of financial management, enterprise resource planning, and mixed financial management systems, the developer shall conduct an independent

assessment of compliance factors established by the Office of the USD(C) (required by DoD Instruction 5000.2);

- Prior to full-rate production, demonstrate the maturity of the production process through Production Qualification Testing of LRIP assets. The focus of this testing is on the contractor's ability to produce a quality product, since the design testing should already have finished. Depending on when this testing is conducted, the results might be usable as another data source for IOT&E readiness determinations; and
- Demonstrate performance against threats and their countermeasures as identified in the DIA-validated System Threat Assessment. Any impact on technical performance by these threats should be identified early in technical testing, rather than in operational testing where their presence might have more serious repercussions (required by DoD Instruction 5000.2).

In addition to the mandatory items above, the following items are strongly recommended to ensure a robust T&E program:

- Involve testers and evaluators, from within the program and outside, early in T&E planning activities to tap their expertise from similar experiences and begin identifying resource requirements needed for T&E budgeting activities;
- Ensure the T&E Strategy is aligned with and supports the approved acquisition strategy, so that adequate, risk-reducing T&E information is provided to support decision events;
- Utilize ground test activities, where appropriate, to include hardware-in-the-loop simulation, prior to conducting full-up, system-level testing, such as flight-testing, in realistic environments;
- The required assessment of technical progress should also include reliability, desired capabilities, and satisfaction of Critical Operational Issues (COIs) to mitigate technical and manufacturing risks;
- Increase likelihood of OT&E success by testing in the most realistic environment possible;
- Assess system-of-systems Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) prior to OT&E to ensure that interoperability under loaded conditions will represent stressed OT&E scenarios.

9.3.2. T&E Working Integrated Product Team (T&E WIPT)

To develop a T&E Strategy, a program manager should rely on a T&E WIPT. The T&E WIPT is a sub-group that reports to the Integrating IPT. It should be established as early as possible during Concept Refinement, and it should be chaired by a concept development team leader or program office representative. In addition, it should include a representative from the Operational Test Agency (OTA). It can consist of other representatives of any agency that the program manager directs, as it is his/her support team that has the collective mission of facilitating the successful planning and execution of the program's T&E activities. Membership often includes representatives from the

program office, the combat developer, the independent Operational Test Activity, the intelligence community, the DoD Component T&E oversight agency, the Program Executive Office or its designated representative, and the contractor. For programs on the OSD T&E Oversight List, it is highly recommended that OSD T&E oversight agencies, (SE/AS and DOT&E), be included. Program managers should also consider forming lower level functional working groups, who report to the T&E WIPT, whose focus is on specific areas such as reliability scoring, M&S development and VV&A, threat support, etc. A charter should be developed early to, as a minimum, identify the responsibilities of the participating membership, and to describe the process by which the T&E WIPT will resolve issues. Two key products of this group are the Test and Evaluation Strategy and the Test and Evaluation Master Plan, both of which are discussed below. Working tools of the T&E WIPT include draft and final statements of desired capabilities, budget documentation, threat documentation, acquisition strategy and detailed DT, LFT and OT plans.

9.3.3. Combined DT&E and OT&E

Whenever feasible, DT&E and OT&E events should be combined, if that supports technical and operational test objectives to gain the optimum amount of testing benefit for reasonable cost and time. The user community should be involved early in test planning to ensure the statement of desired capabilities is interpreted correctly and tested realistically. Certain events can be organized to provide information useful to developmental and operational evaluators and lend themselves to the combined DT and OT approach. The concept is to conduct a single, combined test program that produces credible qualitative and quantitative information that can be used to address developmental and operational issues. Examples of this approach include combined DT and OT events, or piggybacking an operational assessment onto a developmental test. Likewise, developmental testing data requirements can be accommodated by an operational test. This approach can reduce the time and expense of conducting dedicated OT events that replicate DT events, or vice versa, yet still provide adequate technical risk reduction. The developmental and operational testers can develop a test management structure to share control of the combined events. Combined DT and OT events and test data requirements must be identified early to prevent unnecessary duplication of effort and to control costs. It is important that neither the DT&E nor OT&E objectives are compromised in designing combined events. For further explanation of this combined strategy, refer to the DAU Test and Evaluation Management Guide.

9.3.4. Modeling and Simulation in DT&E

Modeling and Simulation (M&S) is integral to and inseparable from T&E in support of acquisition. For T&E, M&S is an essential and proven tool. Each military department has extensive guidelines for use of M&S in acquisition and in T&E. These guidelines are intended to supplement other such resources.

The program manager should have an M&S WIPT that develops the program's M&S strategy. This M&S strategy, or "simulation support plan" will be the basis for program investments in M&S. M&S planned early in the program may retain its utility (if appropriately modified and updated) across the program's life. The planned M&S may

be applicable to not only the first increment of an evolutionary acquisition, but to later increments, as well. A program's test strategy should leverage the advantages of M&S.

An initial goal for the T&E manager is to assist in developing the program M&S strategy. One focus should be to plan for architectures providing M&S interoperability and reusability across the program's life cycle. For example: integrate program M&S with the overall T&E Strategy; plan to employ M&S tools in virtual evaluations of early designs; use M&S to demonstrate system integration risks; supplement live testing with M&S stressing the system; and use M&S to assist in planning the scope of live tests and in data analysis.

Another goal for the T&E manager is to develop a T&E Strategy identifying how to leverage program M&S to support T&E. This could include how M&S will predict system performance, identify technology and performance risk areas, and support determining system effectiveness and suitability. Some T&E Managers choose to develop a separate M&S support plan, which amplifies on the summary information contained in their TEMPs. The TEMP can then contain a pointer to this plan, thus reducing the size of the TEMP M&S discussion. There is no need to repeat the same information twice if an adequate plan exists.

A philosophy for interaction of T&E and M&S is to model-test-fix-model. Use M&S to provide predictions of system performance and effectiveness and, based on those predictions, use tests to provide empirical data to confirm system performance and to refine and validate M&S. This iterative process can be a cost-effective method for overcoming limitations and constraints upon T&E. M&S may enable a comprehensive evaluation, support adequate test realism, and enable economical, timely, and focused test.

With proper planning, simulation-based testing techniques can be applied to digital product descriptions (DPDs), system M&S, and hardware components, to predict system performance in support of early feasibility studies and design trade-off analyses. Test results provide data for validation and development of system M&S and DPDs. Virtual test beds and other M&S capabilities provide synthetic environments and stimuli for controllable, repeatable testing of components, software, and hardware throughout the acquisition cycle.

Computer-generated test scenarios and forces, as well as synthetic stimulation of the system, can support T&E by creating and enhancing realistic live test environments. Hardware-in-the-loop simulators enable users to interact with early system M&S. M&S can be used to identify and resolve issues of technical risk, which require more focused testing. M&S tools provide mechanisms for planning, rehearsing, optimizing, and executing complex tests. Integrated simulation and testing also provides a means for examining why results of a physical test might deviate from pre-test predictions. Evaluators use M&S to predict performance in areas that are impractical or impossible to test.

All M&S used in T&E must be accredited by the intended user (PM or OTA). Accreditation can only be achieved through a robust verification, validation, and accreditation (VV&A) process. Therefore, the intended use of M&S should be identified

early so that resources can be made available to support development and VV&A of these tools. DoD Instruction 5000.61 provides further guidance on VV&A.

The iterative use of M&S and T&E can support spiral development and evolutionary acquisition of a system. Tests help to confirm system performance and validate M&S (which may be then immersed into synthetic environments) and support decision-making. Integrating M&S with testing generates more understanding of the interaction of the system with its environment than either M&S or testing alone. For best efficiency and validity, system M&S used in system test should be the same as, or traceable to, M&S used for concept development, analysis of alternatives, system design, and production. Synthetic test environments may also be reused for training, operations planning and rehearsal, and subsequent concept developments.

9.3.5. System Readiness for IOT&E

The DoD Components develop and institutionalize processes to determine a system's performance and readiness to enter IOT&E. These processes should focus on precluding systems from entering IOT&E prematurely by ensuring that they have demonstrated technical maturity under the conditions expected in the IOT&E.

For programs on the OSD OT&E Oversight List, the DoD Component Acquisition Executive (CAE) is required to evaluate and determine materiel system readiness for IOT&E. The intent of this requirement is to ensure systems do not enter IOT&E before they are sufficiently mature to handle the rigors of the operational environment. Scarce resources, including the military participants, are wasted when an IOT&E is halted or terminated because of technical problems with the system under test, problems that should have been discovered during robust DT.

As part of this system readiness process, programs on the OSD T&E Oversight List are required to provide OSD a DT&E report and progress assessment (required by DoD Instruction 5000.2) that supports entry into IOT&E. That report can be a written document or a briefing to DOT&E and to the DD, DT&E, as the USD(AT&L) representative, that represents the DoD Component's position. The report should include the following: an analysis of the system's progress in achieving Critical Technical Parameters, to include reliability, if a requirement exists; satisfaction of approved IOT&E entrance criteria; a technical risk assessment; level of software maturity and status of software trouble reports; M&S results that project expected IOT&E results; and the predicted impacts of any shortcomings on the system's expected performance during IOT&E. Provide the report at least 20 days prior to the CAE's determination of system readiness. This will allow OSD time to formulate and provide its recommendation to the CAE. All appropriate developmental and operational test and evaluation organizations should be invited to the IOT&E readiness review.

9.4. Operational Test and Evaluation

9.4.1. OT&E Guidelines

DoD Instruction 5000.2 lists mandatory elements of OT&E planning and execution. Other considerations are included here:

The concept of early and integrated T&E should emphasize prototype testing during system development and demonstration and early OAs to identify technology risks and provide operational user impacts. OTAs should maximize their involvement in early, pre-acquisition activities. The goal of integrated T&E is to provide early operational insights into the developmental process. This early operational insight should reduce the scope of the integrated and dedicated OT&E thereby contributing to reduced acquisition cycle time and total ownership cost;

Appropriate use of accredited models and simulation to support DT&E, OT&E, and LFT&E should be coordinated through the T&E WIPT;

Planning should consider a combined DT&E, OT&E, and LFT&E approach. The combined approach should not compromise either developmental testing (DT) or operational testing (OT) objectives. Planning should provide for an adequate OT period and report generation, including the DOT&E Beyond LRIP Report prior to the decision milestone;

The DoD Component OTA is responsible for OT&E, including planning, gaining DOT&E plan approval, execution, and reporting.;

OT&E uses threat or threat representative forces, targets, and threat countermeasures, validated by DIA or the DoD Component intelligence agency, as appropriate, and approved by DOT&E during the test plan approval process. DOT&E oversees threat target, threat simulator, and threat simulation acquisitions and validation to meet developmental, operational, and live fire test and evaluation needs;

Test planning should consider modeling and simulation (M&S). Test planners (DT&E, LFT&E, OT&E) should collaborate early with the program manager's M&S Proponent on the planned use of M&S to support or supplement their test planning or analyze test results. Where feasible, consideration should be given to the use or development of M&S that encompasses the needs of each phase of T&E. Test planners must coordinate with the M&S proponent/developer/operator to establish acceptability criteria required to allow verification, validation, and accreditation (VV&A) of proposed M&S. It is the responsibility of the program manager's M&S Proponent to ensure V&V is conducted in a manner that supports accreditation of M&S for each test event/objective. Whenever possible, an OA should draw upon test results with the actual system, or subsystem, or key components thereof, or with operationally meaningful surrogates. When actual testing is not possible to support an OA, such assessments may utilize computer modeling and/or hardware in the loop, simulations (preferably with real operators in the loop), or an analysis of information contained in key program documents. The TEMP explains the extent of M&S supporting OT&E; if M&S is to be developed, resources must be identified and cost/benefit analysis presented;

Naval vessels, the major systems integral to ship construction, and military satellite programs typically have development and construction phases that extend over long periods of time and involve small procurement quantities. To facilitate evaluations and assessments of system performance (operational effectiveness and suitability), the program manager should ensure the independent OTA is involved in the monitoring of or participating in all relevant activity to make use of any/all relevant results to complete OAs. The OTA should determine the inclusion/exclusion of test data for use during OAs

and determine the requirement for any additional operational testing needed for effectiveness and suitability;

OTAs should participate in early DT&E and M&S to provide OT&E insights to the program manager, the Joint Capabilities Integration and Development System process participants, and acquisition decision makers;

OT&E will evaluate potentially adverse electromagnetic environmental effects (E3) and spectrum supportability situations. Operational testers should use all available data and shall review DD Form 1494, “Application for Equipment Frequency Allocation,” to determine which systems need field assessments; and

OT&E should take maximum advantage of training and exercise activities to increase the realism and scope of both the OT&E and the training, and to reduce testing costs.

9.4.2. Validation of Threat Representations (targets, threat simulators, or M&S)

To ensure test adequacy, operational testing should only incorporate validated, accredited threat representations unless coordinated with DOT&E.

The recommended validation guidelines are:

Threat representation validation supports the objective of ensuring that threat representations meet DT&E and OT&E credibility requirements. Validation of threat representations is defined as "the baseline comparison of the threat to the threat representation, annotation of technical differences, and impact of those differences on testing"

Validation of threat representations is typically conducted by the DoD Component responsible for the threat representation and culminates in a validation report which documents the results. DOT&E approves the DOD Component-validated reports;

Only current, DIA-approved threat data should be used in the validation report. Specifications pertaining to the threat representation should accurately portray its characteristics and may be obtained from a variety of sources including the developer and/or government-sponsored testing. For new developments, validation data requirements should be integrated into the acquisition process to reduce the need for redundant testing;

Incorporation of an IPPD process for new threat representation developments is recommended. The objective of the IPT is to involve DOT&E and its Threat Systems Office (TSO) early and continuously throughout the validation process. DoD Component organizations responsible for conducting threat representation validation should notify DOT&E of their intent to use an IPPD process and request DOT&E/TSO representation at meetings and reviews, as appropriate. The DOT&E representative will be empowered to provide formal concurrence or non-concurrence with these validation efforts as they are accomplished. After the IPPD process, DOT&E will issue an approval memorandum, concurring with the threat representation assessment;

When a WIPT is not used, draft threat representation validation reports should be forwarded to the Threat Systems Office for review. TSO will provide recommendations

for corrections, when necessary. Final reports are then submitted to the TSO for DOT&E approval;

DOT&E approval confirms that an adequate comparison to the threat has been completed. It does not imply acceptance of the threat test asset for use in any specific test. It is the responsibility of the operational test agency to accredit the test resource for a specific test and for DOT&E to determine if the threat test resource is adequate; and

These guidelines do not address the threat representation verification or accreditation processes. Verification determines compliance with design criteria and requires different methods and objectives. Accreditation, an operational test agency responsibility, determines the suitability of the threat representation in meeting the stated test objectives. The data accumulated during validation should be a primary source of information to support the accreditation process.

9.4.3. Evaluation of Test Adequacy

OT&E adequacy encompasses both test planning and test execution. Considerations include the following:

- Realistic combat-like conditions
  - Equipment and personnel under realistic stress and OPTEMPO
  - Threat representative forces
  - End-to-end mission testing
  - Realistic combat tactics for friendly and enemy
  - Operationally realistic environment, targets, countermeasures
  - Interfacing systems
- Production representative system for IOT&E
  - Articles off production line preferred
  - Production representative materials and process
  - Representative hardware and software
  - Representative logistics, maintenance, manuals
- Adequate resources
  - Sample size
  - Size of test unit
  - Threat portrayal
- Representative typical users
  - Properly trained personnel, crews, unit
  - Supported by typical support personnel and unit
  - Missions given to units (friendly and hostile)

9.4.4. Evaluation of Operational Effectiveness

Operational effectiveness is the overall degree of mission accomplishment of a system when used by representative personnel in the environment planned or expected for operational employment of the system considering organization, doctrine, tactics, survivability, vulnerability, and threat.

The evaluation of operational effectiveness is linked to mission accomplishment. The early planning for the evaluation should consider any special test requirements, such as the need for large test areas or ranges or supporting forces, requirements for threat systems or simulators, new instrumentation, or other unique support requirements.

For weapon systems, integrate LFT&E of system lethality into the evaluation of weapon system effectiveness. For example, operational testing could identify likely shot lines, hit points, burst points, or miss distances that might provide a context for LFT&E lethality assessments. Fuse performance, as determined under DT&E or otherwise, can provide a context for both OT&E and LFT&E assessments.

9.4.5. Evaluation of Operational Suitability

Operational suitability is the degree to which a system can be satisfactorily placed in field use, with consideration given to reliability, availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistics supportability, documentation, training requirements, and natural environmental effects and impacts.

Early planning for the suitability evaluation should include any special needs for number of operating hours, environmental testing, maintenance demonstrations, testing profiles, usability of DT data, or other unique test requirements.

Operational suitability should be evaluated in a mission context in order to provide meaningful results. For example, maintaining a required OPTEMPO over an extended period while conducting realistic missions gives insight into the interactions of various suitability factors, such as the ability to maintain stealth features during sustained operations.

9.4.6. Evaluation of Survivability

Survivability includes the elements of susceptibility, vulnerability, and recoverability. As such, survivability is an important contributor to operational effectiveness and suitability. A survivability assessment should be conducted for all systems under OT&E oversight that may be exposed to threat weapons in a combat environment, whether or not the program is designated for LFT&E oversight. (For example, unmanned vehicles are not required to undergo survivability LFT&E under 10 USC 2366, but should be assessed for survivability.) The assessment may identify issues to be addressed by testing.

The DT&E, OT&E, and LFT&E strategies should be integrated so that the full spectrum of system survivability is assessed in a consistent manner. The Critical Operational Issues should include the issues to be addressed in the OT&E evaluation of survivability. Personnel survivability must be addressed for systems under LFT&E oversight (10 USC

2366) and should be integrated into the overall system evaluation of survivability conducted under OT&E.

Generally, vulnerability is addressed through LFT&E and susceptibility through OT&E, but there are areas of overlap. Realistic hit distributions are needed for the evaluation of LFT&E results. The OT&E evaluation of susceptibility might identify realistic hit distributions of likely threats, hit/burst points, and representative shot lines that might provide a context for LFT&E vulnerability assessments. Other LFT&E insights available from DT&E and OT&E testing of susceptibility might include information on signatures, employment of countermeasures, and tactics used for evasion of threat weapons. Similarly, LFT&E tests such as Full Ship Shock trials might provide OT&E evaluators with demonstrations of operability and suitability in a combat environment.

Recoverability addresses the consequences of system damage. Typically, recoverability is primarily addressed by LFT&E. However, in general, tests relating to recoverability from combat damage or from peacetime accidents, battle damage assessment and repair, crashworthiness, crew escape, and rescue capabilities are of interest to both LFT&E and OT&E.

Real Time Casualty Assessment (RTCA) conducted during IOT&E should be coordinated with LFT&E to ensure that assumptions supporting the RTCA are consistent with LFT&E results.

9.5. Live Fire Test and Evaluation

9.5.1. Objective

The objective of LFT&E is to provide a timely and reasonable assessment of the vulnerability/lethality of a system as it progresses through its development and prior to full-rate production. In particular, LFT&E should accomplish the following:

- Provide information to decision-makers on potential user casualties, vulnerabilities, and lethality, taking into equal consideration susceptibility to attack and combat performance of the system;
- Ensure that knowledge of user casualties and system vulnerabilities or lethality is based on testing of the system under realistic combat conditions;
- Allow any design deficiency identified by the testing and evaluation to be corrected in design or employment before proceeding beyond low-rate initial production; and
- Assess recoverability from battle damage and battle damage repair capabilities and issues.

The LFT&E Strategy for a given system should be structured and scheduled so that any design changes resulting from the testing and analysis, described in the LFT&E Strategy, may be incorporated before proceeding beyond low-rate initial production.

9.5.2. Covered Systems

"Covered syste" is the DoD term that is intended to include all categories of systems or programs requiring LFT&E. A "covered system" means a system that DOT&E, acting for the Secretary of Defense, has determined to be a major system within the meaning of that term in 10 U.S.C. 2302(5) that is:

- user-occupied and designed to provide some degree of protection to its occupants in combat; or
- a conventional munitions program or missile program; or
- a conventional munitions program for which more than 1,000,000 rounds are planned to be acquired (regardless of whether or not it is a major system); or
- a modification to a covered system that is likely to affect significantly the survivability or lethality of such a system.

9.5.3. Early LFT&E

DOT&E approves the adequacy of the LFT&E Strategy before the program begins LFT&E. The program should be driven by LFT&E issues identified in the strategy, and be fully integrated with planned DT&E and OT&E. LFT&E typically includes testing at the component, subassembly, and subsystem level, and may also draw upon design analyses, M&S, combat data, and related sources such as analyses of safety and mishap data. This is standard practice, regardless of whether the LFT&E program culminates with full-up, system-level (FUSL) testing, or whether a waiver is obtained from FUSL testing. One of the purposes of conducting LFT&E early in the program life cycle is to allow time to correct any design deficiency demonstrated by the test and evaluation. Where appropriate, the program manager may correct the design or recommend adjusting the employment of the covered system before proceeding beyond LRIP.

9.5.4. Full-Up, System-Level Testing (FUSL) and Waiver Process

The term, “full-up, system-level testing,” is the testing that fully satisfies the statutory requirement for “realistic survivability testing” or “realistic lethality testing” as defined in 10 USC 2366. The criteria for FUSL testing differ somewhat depending on whether the testing is for survivability or lethality. The following is a description of FUSL testing:

Vulnerability testing conducted, using munitions likely to be encountered in combat, on a complete system loaded or equipped with all the dangerous materials that normally would be on board in combat (including flammables and explosives), and with all critical subsystems operating that could make a difference in determining the test outcome; or

Lethality testing of a production-representative munition or missile, for which the target is representative of the class of systems that includes the threat, and the target and test conditions are sufficiently realistic to demonstrate the lethal effects the weapon is designed to produce.

The statute requires an LFT&E program to include FUSL testing unless a waiver is granted in accordance with procedures defined by the statute. A waiver package must be sent to the Congressional defense committees prior to Milestone B; or, in the case of a system or program initiated at Milestone B, as soon as practicable after Milestone B; or if

initiated at Milestone C, as soon as practicable after Milestone C. Typically, this should occur at the time of TEMP approval.

The waiver package includes certification by the USD(AT&L) or the DoD Component Acquisition Executive that FUSL testing would be unreasonably expensive and impractical. It also includes a DOT&E-approved alternative plan for conducting LFT&E in the absence of FUSL testing. Typically, the alternative plan is similar or identical to the LFT&E Strategy contained in the TEMP. This alternative plan should include LFT&E of components, subassemblies, or subsystems; and, as appropriate, additional design analyses, M&S, and combat data analyses.

Programs that have received a waiver from FUSL testing are conducted as LFT&E programs (with exception of the statutory requirement for FUSL testing). In particular, the TEMP contains an LFT&E Strategy approved by DOT&E, and DOT&E, as delegated by the Secretary of Defense, submits an independent assessment report on the completed LFT&E to the Congressional committees as required by statute.

9.5.5. Personnel Survivability

LFT&E has a statutory requirement to emphasize personnel survivability for covered systems occupied by U.S. personnel (10 USC 2366). In general, personnel survivability should be addressed through dedicated measures of evaluation, such as "expected casualties" The ability of personnel to survive should be addressed even in cases where the platform cannot survive. If the system or program has been designated by DOT&E for survivability LFT&E oversight, the program manager should integrate the T&E to address crew survivability issues into the LFT&E program supporting the Secretary of Defense LFT&E Report to Congress.

9.6. T&E Planning Documentation

The two top-level T&E planning documents are the Test and Evaluation Strategy and the Test and Evaluation Master Plan.

9.6.1. Test and Evaluation Strategy (TES)

9.6.1.1. Description

The TES is an early T&E planning document that describes the T&E activities starting with Technology Development and continuing through System Development and Demonstration into Production and Deployment. Over time, the scope of this document will expand, the TES will evolve into the TEMP due at Milestone B. The TES describes, in as much detail as possible, the risk reduction efforts across the range of activities (e.g., M&S, DT&E, OT&E, etc.) that will ultimately produce a valid evaluation of operational effectiveness, suitability, and survivability before full-rate production and deployment. It is a living document and should be updated as determined by the T&E WIPT during the Technology Development Phase. Its development will require early involvement of testers, evaluators, and others as a program conducts pre-system acquisition activities. These personnel will provide the necessary expertise to ensure nothing is overlooked in

laying out a complete strategy. The TES should be consistent with and complementary to the Systems Engineering Plan.

The TES begins by focusing on Technology Development activities, and describes how the component technologies being developed will be demonstrated in a relevant environment (i.e., an environment of stressors at least as challenging as that envisioned during combat) to support the program's transition into the System Development and Demonstration Phase. It contains hardware and software maturity success criteria used to assess key technology maturity for entry into System Development and Demonstration. The TES is the tool used to begin developing the entire program T&E Strategy, and includes the initial T&E concepts for Technology Development, System Development and Demonstration and beyond. For programs following an evolutionary acquisition strategy with more than one developmental increment, the TES should describe how T&E and M&S would be applied to confirm that each increment provides its required operational effectiveness, suitability, and survivability, as would be required of a program containing only one increment. Its development establishes an early consensus among T&E WIPT member organizations on the scope of how the program will be tested and evaluated, with particular consideration given to needed resources, in order to support PPBE process activities.

9.6.1.2. Format

There is no prescribed format for the TES, but it should include the following items, to the extent they are known:

- Introduction and objectives of the system-specific technical and operational evaluations that will support future decision events;
- System description, mission, concept of operations, and major performance capabilities from the Initial Capabilities Document. Identify new technology and the plan to identify associated risk;
- Acquisition strategy concept - For programs following the preferred evolutionary acquisition strategy, the TES should describe how T&E and M&S would be applied to each increment. It should show how each increment would ultimately provide a demonstrated level of operational effectiveness, suitability, and survivability, and meet user needs with a measurable increase in mission capability;
- Time-phased threats to mission accomplishment;
- Anticipated concept of operations, including supportability concept;
- Technical risk reduction testing, including any new or critical technologies identified in the Technology Development Strategy;
- Anticipated component and sub-system developmental testing that begins after MS A;
- Test and evaluation strategy for System Development and Demonstration;
- Critical operational and live fire (if appropriate) issues;

- Scope and structure of the operational and live fire evaluations;
- Likely sources of required data;
- Major T&E design considerations;
- Hardware and software maturity success criteria;
- T&E schedule;
- Anticipated M&S used for future system evaluations; and
- T&E funding estimates in enough detail to permit programming and budgeting.

9.6.1.3. TES Approval Process

- For all programs on OSD T&E oversight, the program manager or leader of the concept development team, with the T&E WIPT providing support, must submit the DoD Component-approved TES to OSD for staffing and approval before Milestone A. Early involvement of testers will ensure a better product and will expedite the approval process, as issues will be addressed and resolved early through the IPPD process.
- It should be submitted 45 days prior to MS A so that an OSD-approved document is available to support the decision.
- The TES for an OSD T&E oversight program is submitted by the DoD Component TES approval authority to the DD, DT&E in the Office of the Director of Defense Systems. The DOT&E and the cognizant OIPT leader approve the TES for all programs on the OSD T&E Oversight List.
- OIPT leaders include the Director, Defense Systems and the Deputy to the ASD (Networks and Information Integration) for C3ISR and IT Acquisition. For programs not on the OSD T&E Oversight List, the CAE, or designated representative, approves the TES.

9.6.2.. Test and Evaluation Master Plan (TEMP)

9.6.2.1. Description

All programs on the OSD T&E Oversight List are required to submit for OSD approval a master plan that describes the total T&E planning from component development through operational T&E into production and acceptance. The program manager, with T&E WIPT providing support, is responsible for producing the TEMP. It is an important document in that it contains the required type and amount of test and evaluation events, along with their resource requirements. The TEMP is considered a contract among the program manager, OSD, and the T&E activities. The program manager must follow the approved TEMP to budget for T&E resources and schedules, which is why it is imperative that all T&E stakeholders participate early in the T&E Strategy development and make timely updates when events or resource requirements change. Stakeholders should include representatives from USD(AT&L) (e.g., SE/AS) and DOT&E, as those offices ultimately will approve the TEMP. Their representatives can advise on what

would constitute acceptable DT, OT, and, if appropriate, LF risk reduction strategies, and can ensure programs are satisfying statutory and regulatory T&E requirements.

While the program manager is responsible for developing the TEMP, the T&E WIPT should make every effort to complete the TEMP in a timely manner and resolve any outstanding issues and reach consensus. Each WIPT member should make every attempt to ensure its organization's issues are surfaced during WIPT meetings to avoid surprises during staffing. If the T&E WIPT cannot resolve all the issues, the program manager should not allow the issues to linger and let the T&E WIPT continue to debate. Instead, the program manager should raise the issues for resolution via the IPPD process.

The TEMP focuses on the overall structure, major elements, and objectives of the T&E program and must be consistent with the acquisition strategy, approved Capability Development Document or Capability Production Document, System Threat Assessment, and Information Support Plan. The TEMP should be consistent with and complementary to the Systems Engineering Plan. For a program using an evolutionary acquisition strategy, the TEMP must also be consistent with the time-phased statement of desired capabilities in the Capability Development Document or Capability Production Document. It provides a road map for integrated simulation, test, and evaluation plans, schedules, and resource requirements necessary to accomplish the T&E program objectives. The TEMP must also be consistent with DOT&E's intended schedule for complying with the statutory reporting requirements for OT&E and/or LFT&E, whether through the phased submittal of dedicated reports or of the Beyond-LRIP or LFT&E reports, or through DOT&E's Annual Report to the Congress. After MS B, no contractor or government testing should be conducted that is not identified in an approved TEMP, otherwise the program manager runs the risk of expending scarce resources on testing that might not be considered adequate by OSD.

9.6.2.2. Format

While there is no mandatory format for a TEMP, this Guidebook contains a suggested format that includes all required information. To provide a clear understanding of the program's overall T&E Strategy, and to ensure approval by OSD, it should contain the following information:

- A summary of the program, system description, and acquisition strategy;
- A listing of the Measures of Effectiveness and Suitability and the corresponding Critical Technical Parameters, along with their thresholds;
- A description of the T&E WIPT management structure, to include sub-level working groups, e.g., reliability, live fire, M&S. If a government-contractor combined test organization is planned, describe its purpose and composition, along with how it interfaces with the T&E WIPT. Distinguish between who is performing test management functions versus test execution or evaluation functions;
- An integrated T&E master schedule that describes the "big picture" and identifies the major testing activities and phases relative to decision points (e.g., milestone decisions and Operational Test Readiness Reviews) and developmental phases. It

must reflect the major phases of contractor and government DT&E, LFT&E, and OT&E events; preliminary and critical design reviews; and the major T&E reporting products, e.g., the DT&E report that supports IOT&E, IOT&E certification, interoperability certification, and Beyond LRIP Report;

- An expanded, detailed schedule that identifies the specific T&E events taking place during SDD (in a MS B TEMP or SDD update) or Production and Deployment (in a MS C TEMP update). For example, the detailed schedule would show specific types of testing such as flight tests, reliability testing periods, or natural environments testing.
- Plans to test and evaluate the system against threats and their countermeasures as identified in the System Threat Assessment and other supporting threat documentation;
- Descriptions of the T&E events for DT&E, OT&E, and LFT&E, including the number of and use of ground test assets and prototypes, and production test and evaluation, including the test purpose, scenario, sample sizes, test conditions, and limitations;
- Descriptions of assessments of system components (hardware, software, and human interfaces) critical to achieving and demonstrating contract technical performance and operational effectiveness, suitability, and survivability;
- System-level and system-of-systems-level test planning;
- Required success criteria (i.e., levels of Critical Technical Parameter maturity) with which to assess technical progress within a program phase;
- Methodologies and plan to be used for verifying, validating, and accrediting M&S, where appropriate, to aid in the system's design, provide insights into system performance, produce pretest predictions and modification of M&S based on test results, and to optimize the amount, duration, and cost of live testing. Explain the extent of M&S supporting DT&E, OT&E, and LFT&E;
- Plans for developing an interoperability certification strategy and test plan (i.e. Interoperability Test Plan and/or Interoperability Certification Evaluation Plan) and demonstrating interoperability with other systems, including meeting the interoperability KPP, and for obtaining interoperability certification by the full-rate production decision review;
- A matrix that identifies all tests within the LFT&E strategy, their schedules, the issues they will address, and which planning documents the DoD Components will submit to DOT&E for approval and which will be submitted for information and review only;
- A capabilities crosswalk matrix depicting the flow-down of desired capabilities from the Initial Capabilities Document to Capability Development Document or CPD, then to the Measures of Effectiveness, Suitability, and Survivability, and finally the Critical Technical Parameters to ensure all desired capabilities will be evaluated;

- A reliability growth plan that describes the testing and anticipated reliability growth of the system throughout its development;
- OT&E entrance criteria for all OT events;
- T&E implications of information assurance;
- Resource requirements, including T&E budget and required funding, test assets, M&S support, facilities, test participants, instrumentation, data reduction capability, expendables, with any shortfalls highlighted. Required threat resources and test targets must also be included. This section of the TEMP is critical to the overall success of the program. It must be as complete and as accurate as possible in reflecting the T&E resource requirements and budget required for T&E. Program T&E problems can often be traced to poor T&E resource requirement definition at the beginning of a program or failure to reprogram T&E resources as program schedules change. When program schedule changes occur, it is imperative that the TEMP is updated and that T&E resources are reprogrammed. Failure to consider T&E resource implications before allowing schedule changes, and failure to reprogram the required T&E resources are often the cause of problems between the developmental and T&E communities.

9.6.2.3. Approval Process

- The TEMP for an OSD T&E oversight program is submitted by the DoD Component TEMP approval authority to the DD, DT&E. The DOT&E and the cognizant OIPT leader approve the TEMP for all programs on the OSD T&E Oversight List. For other programs, the CAE, or designated representative, approves the TEMP.
- For OSD T&E oversight programs, the DD, DT&E staffs the document through appropriate OSD organizations for coordination, formally concurs on the adequacy of the TEMP, and then forwards it to the cognizant OIPT leader and DOT&E for approval. For programs not on OSD T&E oversight, the document is submitted to the CAE for approval.
- A TEMP must be submitted not later than 45 days prior to the Milestone decision point or subsequent program initiation if a PM must have an OSD-approved document by the decision date. For programs newly added to the OSD T&E Oversight List, the TEMP must be submitted within 120 days of such written designation.

9.6.2.4. TEMP Updates

TEMPs are required to be updated at Milestone C and the Full Rate Production Decision Review, but should also be updated when the program baseline has been breached, when the associated Joint Capabilities Integration and Development System document or ISP has been significantly modified, or on other occasions when the program is significantly changed or restructured. Evolutionary acquisition programs may require additional updates to ensure that the TEMP reflects the currently defined program. When a program baseline breach occurs, the TEMP should be updated within 120 days of the date of the

program manager's Program Deviation Report to ensure it reflects the restructured program. When a program changes significantly, the TEMP due date will be negotiated between the program manager and the component TEMP approval authority. In the case of programs under OSD T&E oversight, the negotiations will take place between the program manager, DoD Component TEMP approval authority, SE/AS, and DOT&E. In either case, the goal should be to update the TEMP within 120 days.

9.6.2.5. Circumstances When a TEMP is No Longer Required

When a program's development is completed and COIs are satisfactorily resolved, including the verification of deficiency corrections, TEMP updates are no longer required. The following attributes are examples for which an updated TEMP submission may no longer be required:

- Fully deployed system with no operationally significant product improvements or increment modification efforts;
- Full production ongoing and fielding initiated with no significant deficiencies observed in production qualification test results;
- Partially fielded system in early production phase having successfully accomplished all developmental and operational test objectives;
- Programs for which planned test and evaluation is only a part of routine aging and surveillance testing, service life monitoring, or tactics development;
- Programs for which no further operational testing or live fire testing is required by any DoD Component;
- Program for which future testing (e.g., product improvements or incremental upgrades) has been incorporated in a separate TEMP (e.g., an upgrade TEMP).

9.6.2.6. Requesting Cancellation of TEMP Requirement

Written requests for cancellation of a TEMP requirement for a program on OSD T&E oversight must be forwarded through the DoD Component TEMP approval authority to the OIPT leader (through SE/AS). Justification, such as applicability of any the above circumstances, must be included in the request. The OIPT leader will jointly review the request with DOT&E and notify the DoD Component TEMP approval authority of the result.

9.7. T&E Reports

9.7.1. DoD Component Reporting of Test Results

Programs designated for OSD T&E oversight are required by DoD Instruction 5000.2 to provide formal, detailed, reports of results, conclusions, and recommendations from DT&E, OT&E, and LFT&E to DOT&E and USD(AT&L) (or ASD(NII), as appropriate). For those reports supporting a decision point, the report should generally be submitted 45 days before the decision point.

All developmental and operational T&E agencies shall identify test and evaluation limitations. Their assessment should include the effect of these limitations on system performance, and on their ability to assess technical performance for DT&E or operational capabilities for OT&E.

9.7.2. LFT&E Report

DOT&E monitors and reviews the LFT&E of each covered system. At the conclusion of LFT&E, the Director prepares an independent assessment report that:

- Describes the results of the survivability or lethality LFT&E, and
- Assesses whether the LFT&E was adequate to provide information to decision-makers on potential user casualties and system vulnerability or lethality when the system is employed in combat, and to ensure that knowledge of user casualties and system vulnerabilities or lethality is based on realistic testing, consideration of the validated statement of desired operational capabilities, the expected threat, and susceptibility to attack.

DOT&E prepares the OSD LFT&E Report within 45 days after receiving the DoD Component LFT&E Report, which is required by DoD Instruction 5000.2. The Secretary of Defense (or DOT&E if so delegated) submits the OSD LFT&E report to Congress before a covered system proceeds beyond LRIP (10 USC 2366). If the system is designated for both OT&E and LFT&E oversight, DOT&E may choose to combine the LFT&E and Beyond LRIP reports under single cover, so as to better integrate the reporting of LFT&E and OT&E.

9.7.3. Beyond-Low Rate Initial Production (LRIP) Report

To meet the statutory requirements of 10 USC 2399, DOT&E analyzes the results of IOT&E conducted for each MDAP and DOT&E-designated program. At the conclusion of IOT&E, the Director prepares a report stating the opinion of the Director as to:

- Whether the T&E performed were adequate; and
- Whether the results of such T&E confirm that the items or components actually tested are effective and suitable for combat.

The Director submits Beyond-LRIP reports to the Secretary of Defense, USD(AT&L), and the congressional defense committees. Each such report is submitted to those committees in precisely the same form and with precisely the same content as the report originally was submitted to the Secretary and USD(AT&L) and shall be accompanied by such comments as the Secretary may wish to make on the report. A final decision within the Department of Defense to proceed with an MDAP or DOT&E-designated program beyond LRIP may not be made until the Director has submitted to the Secretary of Defense the Beyond-LRIP Report with respect to that program and the congressional defense committees have received that report (10 U.S.C. 2399).

If the report indicates that either OT&E was inadequate or that the system as tested was ineffective or unsuitable, DOT&E will continue to report his/her assessment of test adequacy and system operational effectiveness and suitability, based on FOT&E, in the DOT&E Annual Report.

In evolutionary acquisition programs that conduct a separate IOT&E for successive development configurations or increments, DOT&E may submit separate BLRIP reports, or if the scope of the configuration change is minimal, may use the DOT&E annual report for the purpose of notifying Congress and the Secretary.

9.7.4. DOT&E Annual Report

DOT&E prepares an annual OT&E and LFT&E report, in both classified and unclassified form, summarizing all OT&E and LFT&E activities, and addressing the adequacy of test resources within the Department of Defense during the previous fiscal year (10 U.S.C. 139). The report includes the status of information assurance, E3, and interoperability for each program (Pub.L. 107-314, Sec. 235). The report also includes an assessment of the waivers of and deviations from requirements in test and evaluation master plans and other testing requirements that occurred during the fiscal year, any concerns raised by the waivers or deviations, and the actions that have been taken or are planned to be taken to address the concerns. DOT&E submits the reports concurrently to the Secretary of Defense, USD(AT&L), and Congress, within 10 days of the President's Budget to Congress.

9.7.5. Electronic Warfare (EW) T&E Report

House Report 103-357 (1993) requires the Secretary of Defense to develop a DoD T&E Process for EW Systems and to report annually on the progress toward meeting this process. DoD memorandum, "Designation of Programs for OSD Test and Evaluation (T&E) Oversight" promulgates the reporting procedure, the list of EW programs required to report, and report format. Designated programs shall submit a one-page status report, through DoD Component channels, to the Deputy Director, SE/AS, Office of the Director, Defense Systems, Office of the USD(AT&L), by November 15th of each year.

9.8. Best Practices

9.8.1. DT&E Best Practices

In the past, some programs have succeeded with their DT&E activities and fared better in Operational Test, while others have struggled. The successful ones share common characteristics or lessons learned. These “best practices” are offered for Program Managers to increase the likelihood of a successful T&E program.

9.8.1.1. Recognize the Value of T&E

T&E is a key part of the system engineering process. It is the validation step in the feedback loop for system design. Use T&E to understand risk and help determine technical issue areas. Review the T&E progress (planning, testing, metrics) often. Look for trends in problems and make appropriate adjustments in overall program priorities. Positive test results will give you confidence that your early designs are valid. Failures in test, when discovered and acted on early in development will result in a better product at less cost - advantages you would not experience if you did not conduct the T&E. Studies have revealed that roughly 75% of life cycle costs of a program are fixed as a result of the initial design process. Obviously, the longer you wait to discover deficiencies, the more

it will cost to implement changes. Spending the time and money early in a program for a rigorous test program will save time and money later.

9.8.1.2. Pick a Strong T&E Manager Early

This individual must be a leader - good at group dynamics, resolving conflict, and forging consensus. T&E experience is a plus, but the other characteristics are key. This individual should be named early in program office organizational staffing, and charged to put in place a rigorous test strategy to carry across the life of the program. Empower this individual to run the T&E program and provide direct access to the Program Manager.

9.8.1.3. Learn and Communicate

Learn the necessary procedures and strategy to develop a sound test strategy. Have the T&E manager become an expert on the T&E aspects of DoD Instruction 5000.2 and this Guidebook. Extended TEMP approval cycles can easily be avoided by having the T&E manager, and preferably others in the T&E organization, knowledgeable of what is required and expected. If there is a question on any DoD Instruction 5000.2 T&E requirement, T&E managers should contact the SE/AS office, or DOT&E as appropriate, for clarification. Consult with the OSD SE/AS office staff early; ask for advice on special problems, selecting metrics, etc. Early discussions will go a long way to setting the right course to facilitate a good test program.

9.8.1.4. Establish and Use a T&E WIPT

Encourage the T&E manager to create and use the collaborative power of the IPPD process. Assemble the user representative, developmental and operational testers, evaluators, and various special experts (information assurance, for example) early to help create the test strategy. Empower the T&E leader to work the WIPT and bring the WIPT group together often-not only to support milestone required documentation, but also to review progress and results.

9.8.1.5. Embed T&E in the Acquisition Strategy, and Vice Versa

The T&E Strategy must support the acquisition strategy. Assure the T&E Master Plan is framed around the acquisition strategy, but also allow T&E to support the acquisition strategy. An example is schedule: allow sufficient schedule for finding problems in testing, fixing them, and retesting.

9.8.1.6. Make "Openness" Your Policy

Facilitate open communications. The IPT process will facilitate this practice. For example: open test planning to a wide cross section of the T&E community; invite the user and the operational tester to witness DT activity; share data and findings with the user and the evaluators; bring the user into the prioritization process for addressing problems; ask for advice from other programs and the OSD Acquisition staff in resolving T&E issues.

9.8.1.7. Develop a Good T&E Strategy

The documentation involved is the TES and the TEMP. Together they represent the test and evaluation program strategy. Ensure the strategy contains a realistic schedule, rigorous and robust technical and operational testing, and is adequately resourced. Put them together early, but also carefully and in sufficient detail. Assure the test program responds to desired system capabilities -metrics should measure progress toward achieving the desired capabilities. Consider incremental success measures to assess progress across the development phase. Bring the user into the planning, to assure the test metrics properly reflect the user's statement of desired capabilities. Align DT & OT. Results of DT should link directly to confidence in entering OT. Introduce operational architectures, operators, and stress into DT parameters when prudent. Track reliability across the entire test program. Look in DT for reliability indicators to exceed required levels, because the stress and environment is usually less severe in DT. Do not assume each test will be successful. Follow the paradigm of: test-fix-retest to verify fixes. Allow schedule time to fix problems and retest.

9.8.1.8. Stick with the Plan

When technical problems arise in DT&E that consume planned test schedule time, program managers should consider restructuring a program schedule to add additional time to accomplish DT&E events. Do not drop testing to save time. Schedule additions when technical problems first arise are less problematic than having to add schedule time late in a program. Avoid the tendency to sacrifice test events to pay for Program budget cuts, or to pay for schedule pressure resulting from slow development progress. Such action invariably will result in higher overall program costs, because discovery of problems will be delayed.

9.8.1.9. Exploit Modeling and Simulation (M&S)

M&S technology is here to stay. It is a fundamental part of all product design and development. It is also a fundamental part of T&E. Seek synergy between system design/development applications of M&S, and T&E applications. Look for opportunities for M&S reuse across the program life cycle. Employ the paradigm of Guidebook Chapter. Planning and investment in M&S should be done early in the program, including M&S for T&E.

9.8.1.10. Employ Event-Driven T&E Strategies

Programs face the dilemma of choosing between a schedule-driven DT&E program, due to funding considerations and demanding IOC dates, and an event-driven program designed to reduce technical risk. The temptation is to focus on the perceived short term benefits of schedule-driven strategies, but in the long run, programs with the discipline to develop and follow event-driven strategies tend to be more successful. This is because perceived short-term benefits are often overcome by the technical risks that programs take. However, the more successful programs tend to maintain an event-driven strategy and proceed from one T&E event to the next only when testing objectives have been accomplished and success criteria have been satisfied. One planned event is successfully completed prior to advancing to the next.

9.8.1.11. Incorporate Operational Realism in DT&E

DT planning should consider operational realism when practical. Introduce operational environments, uniformed operators, and even typical scenario stresses early to gain understanding of potential performance and human factor issues. Look for opportunities to combine DT events with operational assessments and tests. Early user involvement in DT&E has demonstrated exceptional value by providing user insights early into the design process. Operational realism in DT&E will also build confidence in preparing for IOT&E.

9.8.1.12. Work with the OSD SE/AS Office

SE/AS is responsible for monitoring program progress and keeping senior OSD AT&L leadership informed. Programs on OSD SE/AS oversight should establish a rapport with the OSD SE/AS office early on to enlist their help in planning a robust T&E Strategy and to help work through the predictable technical and schedule problems that arise with all programs. The SE/AS office should be a member of the program's T&E WIPT, and they should be participants in the program's developmental and operational test readiness review process. They, and their counterparts in the Defense Systems warfare offices, should be kept apprised of technical problems as they arise so that they can aid in the resolution. Their expertise from supporting programs of all DoD Components can provide lessons learned on similar problems and suggestions on remedial actions. Timely information flow is very important; keep SE/AS apprised of all significant test event results, both successes and failures.

9.8.1.13. Apply Appropriate Commercial Practices

The OSD SE/AS office has published a study report on commercial best practices in T&E. Consider these T&E best practices of commercial industry, and apply them as appropriate. Most of the commercial best practices are logical, and application to defense programs is readily understandable. A sample listing of these best practices follows:

- Recognize that testing is a way to identify and solve problems early in the process in order to control time, cost and schedule late in the process;
- Stabilize corporate leadership and test staff and commit to T&E as a key enabler. Military billet rotation demands that the TES and TEMP be current and document agreements between the OTA, program manager and Milestone Decision Authority;
- Develop consistent processes to ensure consistent products;
- Ensure T&E is consistently part of the decision, planning, and execution process;
- Early commitment by all stakeholders on required T&E resources;
- Certification of T&E processes and organizations (~ISO 9000);
- Increase T&E to assure product quality rather than reduce it to save T&E cost;
- Use metrics and quality control processes to understand how well test process is operating;

- Automate data collection and archiving;
- Use measurements and metrics;
- Continue to increase the use of modeling and simulation to expand the evaluation context based on verified test data;
- Correlate faults and solutions in a closed loop process to ensure problems are resolved;
- Use Physics of Failure as a tool to predict and analyze system performance and shortfalls; and
- Establish internal web based sites for exchange of ideas, benchmarks, data, applications, and processes.

9.8.1.14. Engage Specialists Early

Certain specialty areas, such as information system security, information assurance, interoperability, human systems integration, and software reliability, require early attention. Invite consultation with technical experts (DISA, JITC, OSD SE/AS, etc) to help plan the most efficient test program to build confidence in system maturity.

9.8.1.15. Leverage Other System T&E Planning to Benefit Your Program

Seek out other systems that may compete for similar test resources and combine test activities where practical. Extend this thinking to other areas, such as training. For example, by pursuing built-in test equipment, effective testing can be accomplished in coordination with training.

9.8.1.16. Learn from Others

Contact similar programs, including those of other DoD Components, to learn the lessons of their experience. Take advantage of their successes and avoid repeating their failures.

9.8.1.17. Be Ready for IOT&E

Program managers should not allow their system to enter IOT&E without first being confident that they will succeed.

9.8.2. OT&E Best Practices

- Provide for an integrated DT/OT/LFT&E evaluation, using a phased approach that identifies key decision points and that generates timely and objective information for decision makers on the system's demonstrated capabilities to date (i.e., learn something each year).
- In planning for the operational evaluation, focus on the mission(s) that will be accomplished by a unit or crew equipped with this system. Identify the operational capabilities that will be critical to mission accomplishment. (This starts a "top-down" methodology leading to COIs, MOEs, critical LFT&E issues, and other evaluation issues, measures of performance, and data requirements. These are ultimately to be "rolled back up" to assess the degree of mission

accomplishment. The resulting OT&E concept will link mission accomplishment to the key operational capabilities that are identified in the Joint Capabilities Integration and Development System documents as the basis for accepting the system.)

- During planning, consider how the system will be employed to accomplish the mission(s) previously described. Describe the steps of a complete mission cycle, from mission tasking through successful execution and return. Consider organizational structure; tactics, techniques, and procedures (TTP); training; and any required supporting systems. This provides a "system-of-system" perspective that gives insight into any important interoperability requirements. Determining the appropriate external systems, measures, operational context, and mix of live virtual and constructive resources will depend on the particular system and situation.
- For programs using evolutionary acquisition, the ultimate functionality may or may not be defined at the beginning of the program. Each increment, however, must provide a militarily useful and supportable operational capability, with thresholds and objectives set by the user. The T&E Strategy should provide for an evaluation of the ability of each increment to meet the user's thresholds and evaluate the potential for growth. Comparisons of the capabilities of the legacy system or baseline and the planned increment may assist in evolutionary acquisition by answering the question of whether the new increment provides enough of an improvement in mission capability to warrant fielding to the force.
- For software-intensive systems, follow the DOT&E Guidelines for Conducting Operational Test and Evaluation (OT&E) for Software-Intensive System Increments.
- During planning, the study of the mission, desired performance capabilities, employment concept, and studies such as AOAs, lead to a set of critical operational issues (COIs) and critical LFT&E issues whose satisfactory resolution is vital to the system's operational effectiveness, suitability, and survivability evaluation. The COIs should be few in number, operational in nature, observable, and testable. They should address mission accomplishment and survivability at a level (e.g., ship, flight, unit) appropriate to the evaluation required. The COIs should include measurable improvements to the baseline or current mission capability.
- Whenever applicable, provide a measurable means for comparisons to a baseline system. Baseline comparisons can reduce risk to the program by demonstrating possible improvement in overall mission capability even if certain technical performance requirements are not met. Use of a baseline may reduce risks to test adequacy by compensating for unexpected problems with test environment, training of the test unit, or data collection. Finally, comparisons to the baseline system can demonstrate the degree to which the original deficiencies (in terms of mission accomplishment) have been corrected.
- Identify proposed sources of data for the MOEs and MOPs associated with each COI, LFT&E issue, and secondary evaluation issue. In addition to the IOT&E,

consider other operational events, as well as live fire tests, key developmental test events, modeling and simulation, dedicated side tests, excursions, and "piggy-backin" on training or other planned testing opportunities. Look for opportunities to integrate LFT&E and OT&E.

- Realistically stress systems during developmental testing. Do not let IOT&E be the first time that the system is exposed to operationally realistic environments.
- Test in extreme environments - chambers are necessary but not sufficient to understand system capabilities and limitations.
- Involve the Operational Test Agencies, intelligence agencies, and OSD (for OSD oversight programs) early in the program design stages.

9.8.3. LFT&E Best Practices

9.8.3.1. Pretest Predictions

Pretest predictions are standard practice for every live fire test event. The predictions may be based on computer models, engineering principles, or engineering judgment, and should address a level of detail comparable to the test damage assessment methodology. The DOT&E-approved LFT&E Strategy should address both the nature of the pretest predictions and the schedule of pretest prediction deliverables. The deliverables and supporting documentation should identify basic assumptions, model inputs, and known limitations. If the live fire evaluation plan incorporates the use of vulnerability or lethality models, the pretest predictions should exercise those models, and support the verification, validation, and accreditation of those models. Adequate time and resources should be planned to support pre-test predictions and post-test reconciliation of models and test results.

9.8.3.2. Evaluation Measures

Although the evaluation of live fire test results will address kill given a hit (i.e., vulnerability or lethality), the outcome of LFT&E is not necessarily expressed in terms of probabilities. Rather, live fire testing typically addresses vulnerability or lethality primarily by examining basic damage and kill mechanisms and their interactions with the target system. Further, the evaluation of vulnerability test results should address, where possible, the susceptibility and recoverability of the system and be integrated with results of OT&E.

9.9. Special Topics

9.9.1. Interoperability

For IT systems, including NSS, with interoperability requirements, the Joint Interoperability Test Command (JITC) is required to provide system Net-Ready certification memoranda to the Director, Joint Staff J-6, throughout the system Life-cycle and regardless of Acquisition Category. Based on net readiness evaluations and other pertinent factors, the Joint Staff J-6 shall issue Net-Ready system certification

memoranda to the respective DoD Components and developmental and operational test organizations in support of the full-rate production decision review.

Net readiness applies to C4ISR systems and to any weapon or system that shares data. In general, every system is required to have a Net-Ready KPP and be certified for net readiness. Net-Ready certification is required for a FRP decision, and acceptable net readiness must be demonstrated prior to a Milestone C LRIP decision and IOT&E. In addition, systems will be tested and evaluated periodically over their life cycle for net readiness.

As with most other aspects of a system, net readiness is an early consideration for design and test. The strategy for testing net readiness should be included in the TEMP. An important aspect is to develop a strategy for testing each system in the context of the system-of-systems, or family-of-systems architecture within which it is required to operate.

The Department's test organization for net readiness is the Joint Interoperability Test Command. JITC is the agency that will facilitate a system's Net-Ready certification. The philosophy employed by JITC is to leverage other planned test events to generate necessary data for Net-Ready certification. A special test will be necessary only if other events do not provide the appropriate data. It is important that JITC be included as a member of the T&E WIPT, and participates in the TEMP development.

If the program manager cannot provide the documentation necessary to evaluate and test net readiness, or if a net-readiness certification has not been completed and there is an urgent operational requirement to field a given system or capability, then the program manager must obtain an Interim Certificate to Operate (ICTO) from the Military Communications-Electronics Board (MCEB). An ICTO provides the authority to deploy or operate Information Technology and National Security Systems for a limited time (up to 1 year), with a limited number of platforms, to support developmental efforts, demonstrations, exercises, or operational use. The MCEB Interoperability Test Panel makes the decision to grant an ICTO based on the sponsoring DoD Component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed. The ICTO applies only to JITC interoperability test certification. The Interoperability Test Panel views the ICTO as an infrequent exception to normal procedure and establishes the ICTO's authorized duration based upon the program's action plan to meet certification requirements. During the ICTO authorized period, program managers should take all necessary steps to finalize actions needed to obtain Net-Ready Certification, and they may be required to brief the MCEB Interoperability Test Panel on progress towards that goal.

9.9.2. Information Assurance (IA) T&E Considerations

The test and evaluation of information assurance requirements is an integral part of the overall T&E process. DoD Instruction 5000.2 directs that IA testing be conducted during both DT&E and OT&E. The key aspects of IA include availability, integrity, confidentiality, authentication, and non-repudiation. Key considerations for the planning, coordination and execution of IA testing include the following:

9.9.2.1. Sources of IA Requirements

To ensure that IA testing adequately addresses all system IA requirements, all sources of IA requirements must be considered. These sources include the applicable capabilities documents (e.g., Initial Capabilities Document, Capability Development Document, Capability Production Document, the former ORD, etc.), the applicable IA Baseline Controls are described in DoD Instruction 8500.2 as IA Control Measures. Additional requirements may be derived from the risk management process.

9.9.2.2. Integration of Certification and Accreditation Activities

It is important to consider the impact of the DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP) on the overall test and evaluation schedule. An Interim Authority to Operate (IATO) or Authority to Operate (ATO) is required prior to conducting operational test. These authorities are granted only after the bulk of C&A activities are concluded, and the Designated Approving Authority (DAA) is satisfied with the residual risk to the system. Significant C&A activities and events should be visible on the integrated test schedule to ensure appropriate coordination of events. See paragraph 7.4.4. for additional information.

9.9.2.3. IA Considerations for the TEMP

IA has become increasingly important to joint operations and effective defense system performance. The success of net-centric warfare will depend to a great extent upon information assurance. It is important to address IA in the TEMP. IA roles and responsibilities, test strategies and summaries, and special resources should all be addressed. For example: identify the DAA, and include IATO/ATO as entrance criteria for appropriate test events. OTAs should evaluate protection mechanisms (IA Controls) and the ability to detect system or information attack and subsequently respond and restore systems and information.

9.9.3. Electromagnetic Environmental Effects Testing

Electromagnetic Environmental Effects (E3) can adversely affect the operational effectiveness of military forces, equipment, systems, and platforms. Additionally, today's complex military operational environment is characterized by an increasingly congested electromagnetic spectrum coupled with a reduction of spectrum allocated for exclusive military use. The mix of DoD-developed and commercial-off-the-shelf electronic equipment increases the importance of effectively managing E3 and spectrum usage in the battle space. It is the responsibility of the program manager to ensure, and the responsibility of the Developmental and Operational Test Agencies to validate, the readiness of systems to be fielded into this environment. Historically, failure to verify equipment/platform electromagnetic compatibility in the item's intended operational electromagnetic environment have caused costly program delays and reduced operational effectiveness.

A series of evaluations should be conducted to demonstrate that an item's engineering design is complete and sound, that E3 have been effectively controlled and that E3 limitations and vulnerabilities have been identified and documented. These evaluations

and the associated test requirements vary depending on the item under consideration and the operational EME associated with its intended use. General test requirements and guidelines for electromagnetic compatibility are contained in MIL-STD-461. E3 requirements for systems can be found in MIL-STD-464 and MIL-HDBK-237. These evaluations should be initiated at the earliest practical point in the item's Life-cycle so that deficiencies can be identified early and corrected. Program managers are encouraged to contact their DoD Component E3 representatives to establish an E3 control and evaluation plan for their acquisition program.

9.9.3.1. Hazards of Electromagnetic Radiation to Ordnance (HERO)

In DoD terminology, the hazards that result from adverse interactions between radio frequency (RF) emitters and electrically initiated devices or initiating systems contained within ordnance systems (e.g., fuses) are referred to as HERO. Where applicable, HERO tests should be conducted to determine if exposure of electrically initiated ordnance to specified EME levels will adversely affect the ordnance. The general approach for HERO testing is to expose inert, instrumented ordnance to a controlled test EME and to monitor each EID contained within the ordnance for a possible response. For most EIDs, the response is quantified in terms of the magnitude of RF current induced into the heating element, or bridge wire, of the device. A common objective in all HERO testing is to determine the maximum or worst case response at various test frequencies for various ordnance physical configurations. HERO testing should emphasize exposure of the ordnance to the EME levels that are associated with each operational phase of an ordnance item to include assembly/disassembly, staged, handling and loading, platform loaded, immediate post launch, transportation and storage. Detailed guidance on HERO testing can be found in MIL-HDBK-240, "HERO Test Guide"

9.9.3.2. Hazards of Electromagnetic Radiation to Personnel (HERP)

A potential hazard can exist when personnel are exposed to an electromagnetic field of sufficient intensity to heat the human body. The potential for electromagnetic radiation to produce harmful biological effects in humans is referred to as HERP. Radar and electronic warfare systems present the greatest potential for personnel hazard due to their high transmitter output powers and antenna characteristics. Where applicable, HERP tests should be conducted to establish safety tolerance levels for exposure to EMR as defined in DoD Instruction 6055.11.

9.9.3.3. Hazards of Electromagnetic Radiation to Fuels (HERF)

An electromagnetic field of sufficient intensity can create sparks with sufficient energy to ignite volatile combustibles, such as fuel. The potential for electromagnetic radiation to cause ignition or detonation of volatile combustibles, such as fuels, is referred to as HERF. The existence and extent of a fuel hazard are determined by comparing the actual RF power density to an established safety criterion. When applicable, HERF tests should be conducted to establish safe operating distances as defined in T.O. 31Z-10-4 and OP 3565.

9.9.4. Support for Joint Munitions Effectiveness Manuals (JMEMs)

Each DoD Component should provide weapons effectiveness data for weapons in the acquisition process to DOT&E for use in the Joint Munitions Effectiveness Manuals. The DoD Component should provide the data prior to the weapon achieving initial operational capability, and should prepare the data in coordination with the Joint Technical Coordinating Group for Munitions Effectiveness.

9.9.5. Spectrum Management Support

To evaluate spectrum availability, spectrum-related operational restrictions, frequency availability, host nation approvals, electromagnetic compatibility, and other such issues should be considered. An SM OT assessment is essentially a review of the spectrum management process for the system/equipment in question. DT&E and the early phases of OT&E, if appropriate, should determine if spectrum management issues are resolved, prior to Developmental Performance Verification Testing. All systems/equipment that have spectrum requirements normally undergo Developmental Performance Verification Testing. The CAE should review unresolved spectrum management issues when evaluating system readiness for IOT&E. The DOT&E E3 and SM Assessment Guide for Operational Testing dated 13 June 2001, provides additional information.

9.10. Test and Evaluation Master Plan Recommended Format

The recommended TEMP format for all Acquisition Category I programs, for IT (including NSS), programs regardless of Acquisition Category, and for other OSD T&E Oversight programs begins on the next page. While this format is not mandatory, the following pages reflect staff expectations. The inclusion of all information shown is required for programs under OSD T&E oversight.

TEST AND EVALUATION MASTER PLAN
FOR
PROGRAM TITLE/SYSTEM NAME
Program Elements
Xxxxx

****

SUBMITTED BY

_____ _____
Program Manager DATE

CONCURRENCE

_____ _____
Program Executive Officer DATE
or Developing Agency (if not under the Program Executive Officer structure)

_____ _____
Operational Test Agency DATE

_____ _____
User's Representative DATE

DOD COMPONENT APPROVAL

_____ _____
DoD Component Test and Evaluation Director DATE

_____ _____
DoD Component Acquisition Executive (Acquisition Category I) DATE
Milestone Decision Authority (for less-than-Acquisition Category I)

****

OSD APPROVAL

_____ _____ / _____ _____
Cognizant OIPT Leader / Date Date
Director, Operational Test and Evaluation

1. PART I-SYSTEM INTRODUCTION

a. Mission Description. Reference the capabilities document and ISP. Briefly summarize the mission need described therein. Describe the mission in terms of objectives and general capabilities. Include a description of the operational and logistical environment envisioned for the system.

b. System Description. Briefly describe the system design, to include the following items:

(1) Key features and subsystems, both hardware and software (such as architecture, interfaces, security levels, reserves) for each increment configuration, allowing the system to perform its required operational mission.

(2) Interfaces with existing or planned systems that are required for mission accomplishment. Address relative maturity and integration and modifications needed for commercial items. Include interoperability with existing and/or planned systems of other DoD Components or Allies. Provide a diagram of the system Operational View (OV-1).

(3) Critical system characteristics or unique support concepts resulting in special test and analysis requirements (e.g., post deployment software support, resistance to chemical, biological, nuclear, and radiological effects; resistance to countermeasures; resistance to reverse engineering/exploitation efforts (Anti-Tamper); development of new threat simulation, simulators, or targets).

c. System Threat Assessment. Reference the System Threat Assessment and briefly summarize the threat environment described therein.

d. Measures of Effectiveness and Suitability. List (see example matrix below) the performance (operational effectiveness and suitability) capabilities identified as required in the approved Joint Capabilities Integration and Development System document. The critical operational effectiveness and suitability parameters and constraints must crosswalk to those used in the Analysis of Alternatives, and include manpower, personnel, training, software, computer resources, transportation (lift), compatibility, interoperability and integration, Information Assurance (IA), Electromagnetic Environmental Effects and Spectrum Supportability, etc. Focus on operational capabilities, not design specifications such as weight, size, etc. Limit the list to critical measures that apply to capabilities essential to mission accomplishment. Include and clearly identify all key performance parameters (KPPs). For each listed parameter, provide the threshold and the objective values from the requirement document and reference paragraph. If the Operational Test Agency (OTA) or the DOT&E determines that the required capabilities and characteristics contained in the capabilities document provide insufficient measures for an adequate OT&E, the OTA or DOT&E shall propose additional measures through the IPPD process. Upon receipt of such a proposal, the capabilities approval authority shall establish the level of required performance.

Measures of Effectiveness and Suitability

Operational Capability	Parameter	Capability Threshold	Capability Objective	Capability Reference
Mobility	Land Speed** Miles per hour on secondary roads	xx miles per hour	xx miles per hour	Paragraph xxx
Firepower	Accuracy Main Gun Probability of hit/stationary platform/ stationary target	xxx probability of hit @ xxx range	xxx probability of hit @ xxx range	Paragraph xxx
Supportability	Reliability Mean Time Between Operational Failure	xxx hours	xxx hours	Paragraph xxx

** Key Performance Parameter

e. Critical Technical Parameters

(1) List in a matrix format (see example below) the critical technical parameters of the system (including software maturity and performance measures) that will be evaluated (or reconfirmed if previously evaluated) during the remaining phases of developmental testing. Critical technical parameters are measurable critical system characteristics that, when achieved, allow the attainment of desired operational performance capabilities. They are not user requirements. Rather, they are technical measures derived from desired user capabilities. Failure to achieve a critical technical parameter should be considered a reliable indicator that the system is behind in the planned development schedule or will likely not achieve an operational requirement. Limit the list of critical technical parameters to those that support critical operational issues. The system specification is usually a good reference for the identification of critical technical parameters.

(2) Next to each technical parameter, list a threshold for each stage of development. Developmental test events are opportunities to measure the performance of the system as it matures. For most technical parameters, the listed thresholds should reflect growth as the system progresses toward achieving the desired capabilities. Also, list the decision supported after each event to highlight technical performance required before entering the next acquisition or operational test phase.

(3) Ensure technical parameters are included for technical interoperability.

Critical Technical Parameters

Supported Operational Capability (Include ICD/CDD/ CPD reference)	Technical Parameter	Developmental Stage Event	Threshold Value	Decision Supported
In most cases a measure of effectiveness or suitability from paragraph 1d.	Technical measure(s) derived to support operational desired capabilities .	Developmental stage events (Described in TEMP Part III) designed to measure system performance against technical parameters.	Minimum value required at each developmental event. Most parameters will show growth as the system progress through testing. Final value should reflect level of performance necessary to satisfy the desired capabilities .	May be any decision marking the entrance into a new acquisition phase or may be a readiness for operational test decision.
Example: Main Gun Probability of Hit, 94 % at 1,500 meters (CDD. para. xxx.x)	Example: Auxiliary sight Bore sight accuracy	Example: System Demo Test-Accuracy Test Prod Readiness Test-Accuracy Prod Qual Test	Example: +/- 5 mils +/- 3 mils +/- 1 mil	Example: Milestone B MS C (Low-Rate Initial Production Decision) FRP DR

2. PART II-INTEGRATED TEST PROGRAM SUMMARY

a. Integrated Test Program Schedule

(1) Display on a chart (see Figure 1) the integrated time sequencing of the major test and evaluation phases and events, related activities, and planned cumulative funding expenditures by appropriation. Display on a second chart the specific T&E details for the current and next phase.

(2) Include event dates such as major decision points as defined in DoD Instruction 5000.2, e.g., operational assessments, preliminary and critical design reviews, test article availability; software version releases; appropriate phases of developmental test and evaluation; live fire test and evaluation, JITC interoperability testing and certification date to support FRP Decision Review, and operational test and evaluation; low rate initial production deliveries; Initial Operational Capability; Full Operational Capability; and statutorily required reports, such as the Live-Fire T&E Report and Beyond-LRIP Report.

(3) Provide a single schedule for multi-DoD Component or Joint and Capstone TEMPs showing all DoD Component system event dates.

(4) Provide the date (fiscal quarter) when the decision to proceed beyond low-rate initial production is planned. (LRIP quantities required for initial operational test must be identified for approval by the DOT&E prior to entry into System Development and Demonstration Phase for Acquisition Category I programs and other programs designated for DOT&E oversight).

b. Management

(1) Discuss the test and evaluation responsibility of all participating organizations (developers, testers, evaluators, users).

(2) Identify the T&E WIPT structure, to include the sub-T&E WIPTs, such as a Modeling & Simulation or Reliability, with their participating organizations. A more detailed discussion can be contained in a separate T&E charter; however, sufficient detail is needed here for those persons not having convenient access to the charter.

(3) Provide the proposed or approved performance Exit Criteria to be assessed at the next major decision point. For a TEMP update, generated by a program breach or significant change, provide the Acquisition Decision Memorandum-approved Exit Criteria from the current phase's beginning milestone decision, or any revised ones generated by the breach or significant change.

3. PART III-DEVELOPMENTAL TEST AND EVALUATION OUTLINE

a. Developmental Test and Evaluation Overview. Explain how developmental test and evaluation will verify the status of engineering and manufacturing development progress; verify that design risks have been minimized; verify that anti-tamper provisions have been implemented; and substantiate achievement of contract technical performance requirements. Explain how DT&E will be used to certify readiness for dedicated operational test. Specifically, identify:

(1) Any technology/subsystem that has not demonstrated its ability to contribute to system performance and ultimately achieve the desired mission capabilities.

(2) The degree to which system hardware and software design has stabilized so as to reduce manufacturing and production decision uncertainties.

b. Future Developmental Test and Evaluation. Discuss all remaining developmental test and evaluation that is planned, beginning with the date of the current TEMP revision and extending through completion of production. Emphasize the next phase of testing. For each phase, include:

(1) *Configuration Description* . Summarize the functional capabilities of the system's developmental configuration and how they differ from the production model.

(2) *Developmental Test and Evaluation Objectives* . State the test objectives for this phase in terms of the critical technical parameters to be confirmed, to include anti-tamper characteristics. Provide a table of success criteria corresponding to the Critical Technical Parameters to be confirmed, or for each major phase of DT&E, or combination of both. Identify any specific technical parameters that the milestone decision authority has designated as exit criteria and/or directed to be demonstrated in a given phase of testing.

(3) *Developmental Test and Evaluation Events, Scope of Testing, Basic Scenarios, and Integrated Test Opportunities* . Summarize the test events, test scenarios and the test design concept. Quantify the testing (e.g., number of test hours, test events, test firings). List the specific threat systems, surrogates, countermeasures, component, or subsystem testing, and test beds that are critical to determine whether or not developmental test objectives are achieved. As appropriate, particularly if an agency separate from the test agency will be doing a significant part of the evaluation, describe the methods of evaluation. List all models and simulations to be used to help evaluate the system's performance, explain the rationale for their credible use and provide their source of verification, validation and accreditation (VV&A). Describe how performance in natural environmental conditions representative of the intended area of operations (e.g., temperature, pressure, humidity, fog, precipitation, clouds, electromagnetic environment, blowing dust and sand, icing, wind conditions, steep terrain, wet soil conditions, high sea state, storm surge and tides, etc.) and interoperability with other weapon and support systems, as applicable, to include insensitive munitions, will be tested. Describe the developmental test and evaluation plans and procedures that will support the JITC/DISA interoperability certification recommendation to the Director, Joint Staff (J-6) in time to support the FRP Decision Review. Describe test phases and events that will provide opportunities to integrate testing with contractors and operational testers.

(4) *Limitations* . Discuss the test limitations that may significantly affect the evaluator's ability to draw conclusions, the impact of these limitations, and resolution approaches.

4. PART IV-OPERATIONAL TEST AND EVALUATION OUTLINE

a. Operational Test and Evaluation Overview

(1) The primary purpose of operational test and evaluation is to determine whether systems are operationally effective and suitable for the intended use by representative users in a realistic environment before production or deployment.

(2) Show how program schedule, test management structure, and required resources are related to needed mission capabilities documented in the approved capabilities document, and derived requirements from the ISP; critical operational issues; test objectives; and

major decision points. Testing shall evaluate the system (operated by typical users) in an environment as operationally realistic as possible, including threat representative hostile forces and the expected range of natural environmental conditions.

b. Critical Operational Issues

(1) List in this section the critical operational issues. Critical operational issues are the operational effectiveness and operational suitability issues (not parameters, objectives, or thresholds) that must be examined in operational test and evaluation to evaluate/assess the system's capability to perform its mission.

(2) A critical operational issue is typically phrased as a question that must be answered in order to properly evaluate operational effectiveness (e.g., "Will the system detect the threat in a combat environment at adequate range to allow successful engagement?") and operational suitability (e.g., "Will the system be safe to operate in a combat environment?").

(3) Some critical operational issues will have critical technical parameters and thresholds. Individual attainment of these attributes does not guarantee that the critical operational issue will be favorably resolved. The judgment of the operational test agency is used by the DoD Component to determine if the critical operational issue is favorably resolved.

(4) State the measures of effectiveness (MOEs) and measures of performance (MOPs). Define the evaluation criteria and data requirements for each MOE/MOP.

(5) If every critical operational issue is resolved favorably, the system should be operationally effective and operationally suitable when employed in its intended environment by typical users.

c. Future Operational Test and Evaluation. For each remaining phase of operational test and evaluation, separately address the following:

(1) *Configuration Description* . Identify the system to be tested during each phase, and describe any differences between the tested system and the system that will be fielded including, where applicable, software maturity performance and criticality to mission performance, and the extent of integration with other systems with which it must be interoperable or compatible. Characterize the system (e.g., prototype, engineering development model, production representative or production configuration).

(2) *Operational Test and Evaluation Objectives* . State the test objectives including the objectives and thresholds and critical operational issues to be addressed by each phase of operational test and evaluation and the decision points supported. Provide a table of OT&E Entrance Criteria for each phase of OT&E/OA. Operational test and evaluation that supports the beyond low-rate initial production decision shall have test objectives, to include anti-tamper characteristics that interface with operators and maintainers, that resolve all unresolved effectiveness and suitability COIs.

(3) *Operational Test and Evaluation Events, Scope of Testing, Scenarios, and Integrated Test Opportunities* . Summarize the scenarios and identify the events to be conducted, type of resources to be used, the threat simulators and the simulation(s) to be employed, the type of representative personnel who will operate and maintain the system, the status of the logistic support, the operational and maintenance documentation that will be used,

the environment under which the system is to be employed and supported during testing, the plans for interoperability and compatibility testing with other United States/Allied weapon, the anti-tamper characteristics to be assessed in an operational environment and support systems as applicable, etc. Identify planned sources of information (e.g., developmental testing, testing of related systems, modeling, simulation, etc.) that may be used by the operational test agency to supplement this phase of operational test and evaluation. Whenever models and simulations are to be used: identify the planned models and simulations; explain how they are proposed to be used; and provide the source and methodology of the verification, validation, and accreditation underlying their credible application for the proposed use. If operational test and evaluation cannot be conducted or completed in this phase of testing and the outcome will be an operational assessment instead of an evaluation, so state and clearly explain the reason(s). Describe the operational test and evaluation plans and procedures that will support the JITC/DISA interoperability certification recommendation to the Director, Joint Staff (J-6) in time to support the FRP Decision Review. Describe test phases and events that will provide opportunities to integrate testing with contractors and developmental testers.

(4) *Limitations* . Discuss the test and evaluation limitations including threat realism, resource availability, limited operational (military, climatic, CBNR, etc.) environments, limited support environment, maturity of tested system, safety, etc., that may impact the resolution of affected critical operational issues. Indicate the impact of the test and evaluation limitations on the ability to resolve critical operational issues and the ability to formulate conclusions regarding operational effectiveness and operational suitability. Indicate the critical operational issues affected in parenthesis after each limitation.

d. Live Fire Test and Evaluation.* Include a description of the overall live fire test and evaluation strategy for the item; critical live fire test and evaluation issues; required levels of system protection and tolerance to terminal effects of threat weapons and lethality; the management of the live fire test and evaluation program; live fire test and evaluation schedule; related prior and future live fire test and evaluation efforts; the evaluation approach and shot selection process; the strategy matrix that identifies planning document approval levels; and major test and evaluation limitations for the conduct of live fire test and evaluation. Discuss, if appropriate, procedures intended for obtaining a waiver from full-up, system-level live fire testing (realistic survivability/lethality testing as defined in 10 U.S.C. 2366) before entry into the System Development and Demonstration Phase at Milestone B, or, in the case of a system or program initiated at Milestone B, as soon as practicable after Milestone B, or if initiated at Milestone C, as soon as practicable after Milestone C. Identify LFT&E resource requirements (including test articles and instrumentation) in the Test and Evaluation Resource Summary.

* Not applicable to AIS programs.

5. PART V-TEST AND EVALUATION RESOURCE SUMMARY

a. Provide a summary (preferably in a table or matrix format) of all key test and evaluation resources, both government and contractor, that will be used during the course of the acquisition program. Specifically, identify the following test resources:

(1) *Test Articles* . Identify the actual number of and timing requirements for all test articles, including key support equipment and technical information required for testing in each phase of DT&E, LFT&E, and OT&E. If key subsystems (components, assemblies, subassemblies or software modules) are to be tested individually, before being tested in the final system configuration, identify each subsystem in the TEMP and the quantity required. Specifically identify when prototype, engineering development, or production models will be used.

(2) *Test Sites and Instrumentation* . Identify the specific test ranges/facilities to be used for each type of testing. Compare the requirements for test ranges/facilities dictated by the scope and content of planned testing with existing and programmed test range/facility capability, and highlight any major shortfalls, such as inability to test under representative natural environmental conditions. Identify instrumentation that must be acquired specifically to conduct the planned test program. Describe how environmental compliance requirements will be met.

(3) *Test Support Equipment* . Identify test support equipment that must be acquired specifically to conduct the test program.

(4) *Threat Representation* . Identify the type, number, availability, and fidelity requirements for all representations of the threat to be used in testing. Compare the requirements for threat representations with available and projected assets and their capabilities. Highlight any major shortfalls. Subject each representation of the threat (target, simulator, model, simulation or virtual simulation) to validation procedures to establish and document a baseline comparison with its associated threat and to determine the extent of the operational and technical performance differences between the two throughout the life cycle of the threat representation.

(5) *Test Targets and Expendables* . Identify the type, number, and availability requirements for all targets, weapons, flares, chaff, sonobuoys, smoke generators, acoustic countermeasures, etc., that will be required for each phase of testing. Identify any major shortfalls. Subject each threat target to validation procedures, tailored to characteristics of interest, in order to establish and document a baseline comparison with its associated threat and to ascertain the extent of operational and technical performance differences throughout the threat target's life cycle.

(6) *Operational Force Test Support* . For each test and evaluation phase, identify the type and timing of aircraft flying hours, ship steaming days, and on-orbit satellite contacts/coverage, and other critical operating force support required.

(7) *Simulations, Models and Testbeds* . For each test and evaluation phase, identify the models and simulations to be used, including computer-driven simulation models and hardware/software-in-the-loop test beds. However, provide the discussion of how these models and simulations will be used in Parts III and IV. Identify the resources required to accredit their usage. Identify the M&S Proponent, the V&V Agent, and the Accreditation Agent for intended user.

(8) *Special Requirements* . Discuss requirements for any significant non-instrumentation capabilities and resources such as: special data processing/data bases, unique

mapping/charting/geodesy products, extreme physical environmental conditions or restricted/special use air/sea/landscapes.

(9) *Test and Evaluation Funding Requirements* . Estimate, by Fiscal Year and appropriation line number (program element), the funding required to pay direct costs of planned testing. State, by fiscal year, the funding currently appearing in those lines (program elements).

(10) *Manpower/Personnel Training* . Identify manpower/personnel and training requirements and limitations that affect test and evaluation execution.

b. Project the time-phased test and test support resources necessary to accomplish development, integration and demonstration testing and early operational assessment. Estimate, to the degree known, the key resources necessary to accomplish developmental test and evaluation, operational assessment, live fire test and evaluation, and operational test and evaluation. These include test and training ranges of the Major Range and Test Facility Base (MRTFB), test equipment and facilities of the MRTFB, capabilities designated by industry and academia, unique instrumentation, threat simulators, targets, and modeling and simulation. As system acquisition progresses, the preliminary test resource requirements should be reassessed and refined, and subsequent TEMP updates should reflect any changed system concepts, resource requirements, or updated threat assessment.

6. Annex A-BIBLIOGRAPHY

a. Cite in this section all documents referred to in the TEMP.

b. Cite all reports documenting technical, live fire, and operational testing and evaluation.

7. Annex B-ACRONYMS

List and define acronyms used in the TEMP.

8. Annex C-POINTS OF CONTACT

Provide a list of points of contact as illustrated by Figure 2.

9. ATTACHMENTS

Provide as appropriate.

FIGURE 9.10.1. - Integrated Test Program Schedule

FIGURE 1 - INTEGRATED TEST PROGRAM SCHEDULE

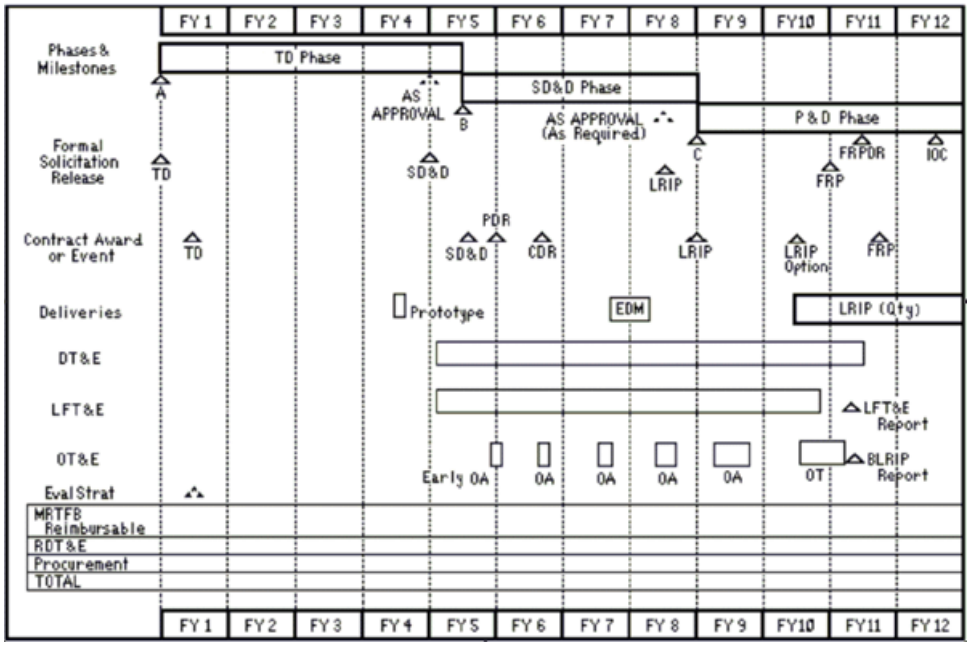

FIGURE 2 - PROGRAM POINTS OF CONTACT

NAME ORGANIZATION TELEPHONE (COMM/DSN) E-MAIL ADDRESS

DoD Component Secretary/Agency Director/Monitor/Coordinator

User Representative

Program Manager

Developmental Test Director/Coordinator

Operational Test Director/Coordinator

DoD Component T&E Action Officer

OUSD(AT&L)/DT Action Officer

OSD/DOT&E Action Officer

CHAPTER 10

Decisions, Assessments, and Periodic Reporting

10.0. Overview

10.0.1. Purpose

This Chapter discusses major program decisions, assessments, and periodic reporting. Generically, it prepares the Program Manager and Milestone Decision Authority to execute their respective oversight responsibilities.

10.0.2. Contents

The chapter starts with overviews of the major decision points and executive reviews associated with a program. It also discusses Integrated Product Teams (IPTs). Other topics include Exit Criteria, Independent Assessments, Information Sharing and DoD Oversight, Management Control, Program Plans, and Periodic Reports. The chapter closes with an overview of the Consolidated Acquisition Reporting System.

10.1. Decision Points

There are two types of decision points: milestone decisions and decision reviews. Each decision point results in a decision to initiate, continue, advance, or terminate a project or program work effort or phase. The review associated with each decision point typically addresses program progress and risk, affordability, program trade-offs, acquisition strategy updates, and the development of exit criteria for the next phase or effort. The type and number of decision points should be tailored to program needs. The Milestone Decision Authority approves the program structure, including the type and number of decision points, as part of the acquisition strategy.

Milestone decision points initiate programs and authorize entry into the major acquisition process phases: Technology Development, System Development and Demonstration, and Production and Deployment. The statutory and regulatory information requirements specified in DoD Instruction 5000.2 support milestone decisions.

Decision reviews assess progress and authorize (or halt) further program activity. The Concept Decision authorizes Concept Refinement; the Design Readiness Reviewassesses program progress within the System Development and Demonstration phase; and the Full-Rate Production Decision Review (or Deployment Decision Review for Automated Information Systems or software-intensive systems with no developmental hardware) occurs during the Production and Deployment phase.

The information required to support both milestone decision points and decision reviews should be tailored to support the review, but must be consistent with (and not exceed) the requirements specified in DoD Instruction 5000.2.

10.2. Executive Reviews

The following paragraphs address DoD assessment reviews associated with major decision points.

10.2.1. Defense Acquisition Board Review

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) is the Defense Acquisition Executive (DAE), and conducts Defense Acquisition Board reviews for Acquisition Category ID programs at major program milestones (and at the Full-Rate Production Decision Review if not delegated) and at other times, as necessary. Whenever possible, these reviews should take place in the context of the existing Integrated Product Team and acquisition milestone decision review processes. An Acquisition Decision Memorandum documents the decision(s) resulting from the review.

10.2.2. Information Technology Acquisition Board Reviews

Information Technology Acquisition Board Reviews provide the forum for approving Acquisition Category IAM milestones; deciding critical Acquisition Category IAM issues when they cannot be resolved at the Overarching Integrated Product Team level; and for enabling the execution of the DoD Chief Information Officer's acquisition-related responsibilities for Information Technology, including National Security Systems, under Title 10 and the Clinger-Cohen Act. Whenever possible, these reviews should take place in the context of the existing Integrated Product Team and acquisition milestone review process. An Acquisition Decision Memorandum documents the decision(s) resulting from the review.

Information Technology Acquisition Board Reviews should focus on key principles such as:

- Support of mission needs as described in the Strategic Planning Guidance and the Joint Programming Guidance, Joint Vision 2020, the DoD Information Management Strategic Plan, the operational view of the approved Global Information Grid (GIG) Integrated Architecture, and the approved GIG Capstone Requirements Document.
- Compliance with GIG-related policies and the approved GIG Integrated Architecture.
- Net-centric readiness plans and status implications of program and budget decisions/alternatives.

Information Technology Acquisition Board members are the following department officials: the Deputy DoD Chief Information Officer; Information Technology Overarching Integrated Product Team Leader; Cognizant Program Executive Officer(s) and Program Manager(s); Cognizant OSD Principal Staff Assistant(s); the Under Secretary of Defense (Comptroller) (Director, Program Budget and Deputy Chief Financial Officer, the Under Secretary of Defense (Personnel & Readiness);the Director, Operational Test & Evaluation; the Director, Program Analysis and Evaluation; the Director, Force Structure (J8); the Component Acquisition Executives of the Army, Navy, and Air Force; DoD General Counsel; the Deputy Director, Developmental Test & Evaluation; the Director, Defense Procurement and Acquisition Policy; and DoD Component User Representatives,

Information Technology Acquisition Board advisors include the Under Secretary of Defense (Policy); the Under Secretary of Defense (Intelligence); the Domain Owner; Component CIOs; the Director, Defense Intelligence Agency; the Director, Cost Analysis Improvement Group; the Director, Defense Procurement and Acquisition Policy; Representatives of the Joint Staff; the Deputy Under Secretary of Defense (Logistics and Material Readiness); the Deputy Under Secretary of Defense (Installations and Environment); the Deputy Under Secretary of Defense (Industrial Policy); the Director, International Cooperation; and the Director, Acquisition Resources and Analysis.

The DoD Chief Information Officer may ask other Department officials to participate in reviews, as required.

10.2.3. Joint Requirements Oversight Council (JROC)

The JROC reviews programs designated as JROC interest and supports the acquisition review process. In accordance with the CJCS Instruction 3170.01, the Joint Staff reviews all Joint Capabilities Integration and Development System documents and assigns a Joint Potential Designator. The JROC charters Functional Capabilities Boards. The boards are chaired by a JROC-designated chair and, for appropriate topics, co-chaired by a representative of the Milestone Decision Authority. Functional Capabilities Boards are the lead coordinating bodies to ensure that the joint force is best served throughout the Joint Capabilities Integration and Development System and acquisition processes. The Joint Capabilities Integration and Development System process encourages early and continuous collaboration with the acquisition community to ensure that new capabilities are conceived and developed in the joint warfighting context. The JROC, at its discretion, may review any Joint Capabilities Integration and Development System issues which may have joint interest or impact. The JROC will also review programs at the request of, and make recommendations as appropriate to, the Secretary of Defense, Deputy Secretary of Defense, Under Secretary of Defense (Acquisition, Technology, and Logistics), Assistant Secretary of Defense (Networks and Information Integration), and the Under Secretary of the Air Force (as DoD Space Milestone Decision Authority). The JROC also validates key performance parameters.

10.2.4. DoD Component Program Decision Review Processes

The decision review processes discussed in this section deal specifically with Acquisition Category ID and Acquisition Category IAM programs and selected Pre-Major Defense Acquisition Programs/Pre-Major Automated Information System Programs. DoD Component Acquisition Executives will develop tailored procedures that meet statutory intent for programs under their cognizance.

10.3. Role of Integrated Product Teams (IPTs)

Defense acquisition works best when all of the DoD Components work together. Cooperation and empowerment are essential. Per DoD Directive 5000.1, the Department's acquisition community shall implement the concepts of Integrated Product and Process Development (IPPD) and IPTs as extensively as possible.(*See Rules of the Road: A Guide for Leading Successful Integrated Product Teams*)

IPTs are an integral part of the Defense acquisition oversight and review process. For Acquisition Category ID and IAM programs, there are generally two levels of IPT: the Overarching Integrated Product Team and the Working-level Integrated Product Team(s). Each program should have an OIPT and at least one WIPT. WIPTs should focus on a particular topic such as cost/performance, test, or contracting. An Integrating Integrated Product Team (IIPT), which is itself a WIPT, should coordinate WIPT efforts and cover all topics not otherwise assigned to another IPT. IPT participation is the primary way for any organization to participate in the acquisition program.

10.3.1. Overarching IPT (OIPT) Procedures and Assessment

All Acquisition Category ID and IAM programs will have an OIPT to provide assistance, oversight, and review as the program proceeds through its acquisition life cycle. An appropriate official within OSD, typically the Director, Defense Systems or the Deputy to the Assistant Secretary of Defense for Networks and Information (ASD(NII)) for Command, control, Communications, Intelligence, Surveillance and Reconnaisance (C3ISR) and Information Technology (IT) Acquisition, will lead the OIPT for Acquisition Category ID programs. The Deputy to the ASD(NII) for C3ISR and IT Acquisition also leads the OIPT for Acquisition Category IAM programs. The OIPT for Acquisition Category IAM programs is called the NII OIPT. OIPTs should include the Program Manager, Program Executive Officer, DoD Component Staff, Joint Staff, and OSD staff involved in oversight and review of the particular Acquisition Category ID or IAM program. Other OIPTs, specifically those for Chem Bio and Space, will be lead and directed by similar executives.

The OIPT should form upon departmental intention to start an acquisition program. The OIPT charters the Integrating Integrated Product Team and Working-level Integrated Product Teams. The OIPT should consider the recommendations of the Integrating Integrated Product Team regarding the appropriate milestone for program initiation and the minimum information needed for the program initiation milestone review. OIPTs should meet, thereafter, as necessary over the life of the program. The OIPT leader should act to resolve issues when requested by any member of the OIPT, or when so directed by the Milestone Decision Authority. The goal is to resolve as many issues and concerns at the lowest level possible, and to expeditiously escalate issues that need resolution at a higher level. The OIPT should bring only the highest-level issues to the Milestone Decision Authority for decision.

The OIPT should normally convene 2 weeks before a planned decision point. It should assess the information and recommendations that the Milestone Decision Authority will receive. It should also assess family-of-system or system-of-system capabilities within and between functional portfolios (or areas) in support of integrated architectures developed by the Joint Staff in collaboration with the OSD, USAF (as DoD Space Milestone Decision Authority), and the DoD Components. If the program includes a pilot project, such as Total Ownership Cost Reduction, the Program Manager should report the status of the project to the OIPT. The OIPT should then assess progress against stated goals. The Program Manager's briefing to the OIPT should address interoperability and supportability (including spectrum supportability) with other systems, anti-tamper provisions, and indicate whether those requirements will be satisfied by the acquisition

strategy under review. If the program is part of a family-of-systems architecture, the Program Manager should brief the OIPT in that context. If the architecture includes less than Acquisition Category I programs that are key to achieving the expected operational capability, the Program Manager should also discuss the status of and dependence on those programs. The OIPT should review the programmatic risk issues of cost, schedule, and performance. The OIPT leader should recommend to the Milestone Decision Authority whether the anticipated review should go forward as planned.

For Acquisition Category ID decision points, the OIPT leader will provide the Defense Acquisition Board chair, co-chair, principals, and advisors with an integrated assessment using information gathered through the IPPD process. The OIPT assessment should focus on core acquisition management issues and should consider independent assessments, including technology readiness assessments, which the OIPT members normally prepare. These assessments typically occur in context of the OIPT review, and should be reflected in the OIPT leader's report. There should be no surprises at this point-all team members should work issues in real time and should be knowledgeable of their OIPT leader's assessment. OIPT and other staff members should minimize requirements for the program manager to provide pre-briefs independent of the OIPT process.

10.3.2. WIPT Procedures, Roles, and Responsibilities

Program manager, or designee, should form and lead an IIPT to support the development of strategies for acquisition and contracts, cost estimates, evaluation of alternatives, logistics management, training, cost-performance trade-offs, etc. Program manager, assisted by the IIPT, should develop a WIPT structure and propose the structure to the OIPT. The IIPT should coordinate the activities of the WIPTs and review issues they do not address. WIPTs should meet as required to help the program manager plan program structure and documentation and resolve issues. While there is no one-size-fits-all WIPT approach, the following basic tenets should apply:

- Program manager is in charge of the program.
- WIPTs are advisory bodies to the program manager.
- Direct communication between the program office and all levels in the acquisition oversight and review process is expected as a means of exchanging information and building trust.

Program manager or the program manager's representative should normally lead each WIPT. At the invitation of the program manager, an OSD action officer may co-chair WIPT meetings. The following roles and responsibilities should apply to all WIPTs:

- Assist the program manager in developing strategies and in program planning, as requested by the program manager.
- Establish a WIPT plan of action and milestones.
- Propose tailored documentation and milestone requirements.
- Review and provide early input to documents.
- Coordinate WIPT activities with the OIPT members.
- Resolve or elevate issues in a timely manner.

- Assume responsibility to obtain principals' concurrences on issues, documents, or portions of documents.

IPTs are critical to program success, and training is critical to IPT success. All IPT members for Acquisition Category ID and Acquisition Category IAM programs should receive formal, team-specific training and, as necessary, general IPT procedural training. The Acquisition Community Connection web site has additional information about WIPTs.

10.3.3. Industry Participation

Industry representatives may be invited to a WIPT or IIPT meeting to provide information, advice, and recommendations to the IPT; however, the following policy should govern their participation:

- Industry representatives will not be formal members of the IPT.
- Industry participation will be consistent with the Federal Advisory Committee Act.
- Industry representatives may not be present during IPT deliberations on acquisition strategy or competition sensitive matters, nor during any other discussions that would give them a marketing or competitive advantage.
- At the beginning of each meeting, the IPT chair should introduce each industry representative, including their affiliation, and their purpose for attending.
- The chair should inform the IPT members of the need to restrict discussions while industry representatives are in the room, and/or the chair should request the industry representatives to leave before matters are discussed that are inappropriate for them to hear.
- Support contractors may participate in WIPTs and IIPTs, but they may not commit the organization they support to a specific position. The organizations they support are responsible for ensuring the support contractors are employed in ways that do not create the potential for an organizational conflict of interest. Contractors supporting staff organizations may participate in Overarching Integrated Product Team (OIPT) discussions; however, they will not be permitted to represent the position of the supported organization and they may be asked to sign non-disclosure statements.

Given the sensitive nature of OIPT discussions, neither industry representatives nor support contractors may participate in OIPT discussions. However, the OIPT leader may permit contractors to make presentations to the OIPT when such views will better inform the OIPT, and will not involve the contractors directly in Government decision making.

10.4. Role of Exit Criteria

Milestone Decision Authorities should use exit criteria, when appropriate, to establish goals for Acquisition Category I and Acquisition Category IA programs during an acquisition phase. At each milestone decision point and at each decision review, the program manager, in collaboration with the IPT, will develop and propose exit criteria appropriate to the next phase or effort of the program. The OIPT will review the

proposed exit criteria and make a recommendation to the Milestone Decision Authority. Exit criteria approved by the Milestone Decision Authority will be published in the ADM.

System-specific exit criteria normally track progress in important technical, schedule, or management risk areas. Unless waived, or modified by the Milestone Decision Authority, exit criteria must be substantially satisfied for the program to continue with additional activities within an acquisition phase or to proceed into the next acquisition phase (depending on the decision with which they are associated). Exit criteria should not be part of the APB and are not intended to repeat or replace APB requirements or the phase-specific entrance criteria specified in DoD Instruction 5000.2. They should not cause program deviations. Status of approved exit criteria will be reported in the Defense Acquisition Executive Summary.

10.5. Role of Independent Assessments

Assessments, independent of the developer and the user, ensure an impartial evaluation of program status. However, requirements for independent assessments (for example, the independent cost estimate or technology readiness assessment) must be consistent with statutory requirements and good management practice. Senior acquisition officials should consider these assessments when making acquisition decisions. Staff offices that provide independent assessments should support the orderly and timely progression of programs through the acquisition process. IPTs should have access to independent assessments to enable full and open discussion of issues.

10.5.1. Independent Cost Estimate

10 USC 2434 requires that an independent life-cycle cost be prepared and provided to the milestone decision authority before the approval of a major defense acquisition program to proceed with either system development and demonstration, or production and deployment.

The OSD CAIG prepares the independent cost estimate and provides an assessment on the program's life-cycle cost to the Milestone Decision Authority.

10.5.2. Technology Maturity and Technology Readiness Assessments

Technology maturity is a measure of the degree to which proposed critical technologies meet program objectives; and, is a principal element of program risk. A technology readiness assessment examines program concepts, technology requirements, and demonstrated technology capabilities in order to determine technological maturity.

The program manager should identify critical technologies via the Work Breakdown Structure. In order to provide useful technology maturity information to the acquisition review process, technology readiness assessments of critical technologies and identification of Critical Program Information (CPI) must be completed prior to Milestone Decision points B and C.

The DoD Component Science and Technology (S&T) Executive directs the technology readiness assessment and, for Acquisition Category ID and Acquisition Category IAM programs, submits the findings to the CAE who should submit his or her report to the

DUSD(S&T) with a recommended technology readiness level (TRL) (or some equivalent assessment) for each critical technology. When the DoD Component S&T Executive submits his or her findings to the CAE, he or she should provide the DUSD(S&T) an information copy of those findings. In cooperation with the DoD Component S&T Executive and the program office, the DUSD(S&T) should evaluate the technology readiness assessment and, if he/she concurs, forward findings to the OIPT leader and DAB. If the DUSD(S&T) does not concur with the technology readiness assessment findings, an independent technology readiness assessment, under the direction of the DUSD(S&T), should be required. A summary table of TRL descriptions, Table 10.5.2.1, follows:

Technology Readiness Level	**Description**
1. Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2. Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3. Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
5. Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.
6. System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.

7. System prototype demonstration in an operational environment.	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.
8. Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9. Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

Table 10.5.2.1. TRL Descriptions

The use of TRLs enables consistent, uniform, discussions of technical maturity across different types of technologies. Decision authorities will consider the recommended TRLs (or some equivalent assessment methodology, e.g., Willoughby templates) when assessing program risk. TRLs are a measure of technical maturity. They do not discuss the probability of occurrence (i.e., the likelihood of attaining required maturity) or the impact of not achieving technology maturity.

For additional information, see the on-line TRA Handbook.

10.6. Information Sharing and DoD Oversight

10.6.1. Program Information

It is DoD policy to keep reporting requirements to a minimum. Nevertheless, complete and current program information is essential to the acquisition process. Consistent with the tables of required regulatory and statutory information in DoD Instruction 5000.2, decision authorities should require program managers and other participants in the defense acquisition process to present only the minimum information necessary to understand program status and make informed decisions. The Milestone Decision Authority should “tailor-in” program information case-by-case, as necessary. IPTs should facilitate the management and exchange of program information.

The program manager, the DoD Component, or the OSD staff prepares most program information. Some information requires approval by an acquisition executive. Other information is for consideration only. In most cases, information content and availability is more important than format.

Program Managers may use stand-alone documents or a single document to submit mandatory information. If the program manager submits stand-alone documents, the

program manager should minimize redundancy and not include the same information in each document.

Unless otherwise specified, all plans, waivers, certifications and reports of findings referred to in this Guidebook are exempt from licensing under one or more exemption provisions of DoD 8910.1-M.

10.6.2. Life-Cycle Management of Information

Program managers will comply with record keeping responsibilities under the Federal Records Act for the information collected and retained in the form of electronic records. (See DoD Directive 5015.2.) Electronic record keeping systems should preserve the information submitted, as required by 44 U.S.C. 3101, and implementing regulations. Electronic record keeping systems should also provide, wherever appropriate, for the electronic acknowledgment of electronic filings that are successfully submitted. Program managers should consider the record keeping functionality of any systems that store electronic documents and electronic signatures to ensure users have appropriate access to the information and can meet the Agency's record keeping needs.

10.6.3. Classification and Management of Sensitive Information

Program managers should review their programs to identify and document critical program information (CPI) requiring protection (DoD Directive 5200.39).

Program managers should also review their programs to identify controlled unclassified information (CUI). (CUI includes "FOUO" information as defined in DoD 5400.7-R and information with other approved markings requiring dissemination controls that are exempt from mandatory disclosure under the Freedom of Information Act (e.g., DoD Directive 5230.24, DoD Directive 5230.25, and Export Control Act.))

When necessary, program managers should develop security classification guides (SCGs) in accordance with DoD 5200.1-R.

10.7. Management Control

Program managers will implement internal management controls in accordance with DoD Directive 5000.1, DoD Instruction 5000.2, and DoD Directive 5010.38. APB parameters should serve as control objectives. Program managers should identify deviations from approved APB parameters and exit criteria as material weaknesses. Program managers should focus on results, not process.

Program managers will ensure that obligations and costs comply with applicable law. They should safeguard assets against waste, loss, unauthorized use, and misappropriation; properly record and account for expenditures; maintain accountability over assets; and quickly correct identified weaknesses.

10.8. Program Plans

Program plans describe the detailed activities of the acquisition program. Except as specified by DoD Instruction 5000.2, the program manager (in coordination with the

Milestone Decision Authority and Program Executive Officer) should determine the type and number of program plans needed to manage program execution.

10.9. Periodic Reports

Periodic reports should include only those reports required by the Milestone Decision Authority or statute. Except for the reports outlined in this section, the Milestone Decision Authority should tailor the scope and formality of reporting requirements.

10.9.1. Acquisition Program Baseline (APB) Reporting

10.9.1.1. Program Deviations

The program manager should maintain a current DoD Component and/or Program Manager estimate of the program being executed. This "current estimate" should reflect the President's Budget, adjusted for fact-of-life changes (i.e., already happened or unavoidable). The program manager should immediately notify the Milestone Decision Authority when a program deviation occurs. (See 10 USC 2433.)

10.9.1.2. Information Technology (IT) Program Deviations

40 USC 11317 requires the Component Acquisition Executive to identify, in the DoD Strategic Information Resource Management Plan, major IT acquisition programs that have significantly deviated from the cost, performance, or schedule goals established for the program.

10.9.1.3. Current Estimate

Program managers will report the current estimate of each APB parameter periodically to the Milestone Decision Authority. The Milestone Decision Authority will direct the frequency of the reporting. Program Managers will report current estimates for Acquisition Category I and IA programs quarterly in the DAES.

10.9.1.4. Program Deviation Reporting

When the program manager has reason to believe that the current estimate for the program indicates that a performance, schedule, or cost threshold value will not be achieved, he or she will immediately notify the Milestone Decision Authority of the deviation. Within 30 days of the occurrence of the program deviation, the program manager will notify the Milestone Decision Authority of the reason for the program deviation and the actions that need to be taken to bring the program back within the baseline parameters (if this information was not included with the original notification). Within 90 days of the occurrence of the program deviation, one of the following should have occurred: the program is back within APB parameters; a new APB (changing only those parameters that were breached) has been approved; or an OIPT-level program review has been conducted to review the program manager's proposed baseline revisions and make recommendations to the Milestone Decision Authority.

For Acquisition Category I programs, if one of the above three actions has not occurred within 90 days of the program deviation, the USD(AT&L) for Acquisition Category ID

programs, the ASD(NII) for Acquisition Category IAM programs, or the CAE, for Acquisition Category IC and/or Acquisition Category IAC programs, should hold a formal program review to determine program status.

10.9.2. Selected Acquisition Report (SAR)

In accordance with 10 U.S.C. 2432, the Secretary of Defense will submit a SAR to Congress for all Acquisition Category I programs. The program manager will use CARS software to prepare the SAR.

10.9.2.1. SAR Content and Submission

The SAR reports the status of total program cost, schedule, and performance, as well as program unit cost and unit cost breach information. For joint programs, the SAR reports the information by participant. Each SAR will include a full, life-cycle cost analysis for the reporting program, each of its evolutionary increments, as available, and for its antecedent program, if applicable.

The SAR for the quarter ending December 31 is the annual SAR. The program manager will submit the annual SAR within 60 days after the President transmits the following fiscal year's budget to Congress. Annual SARs will reflect the President's Budget and supporting documentation. The annual SAR is mandatory for all programs that meet SAR reporting criteria.

The program manager will submit SARs for the quarters ending March 31, June 30, and September 30 not later than 45 days after the quarter ends. Quarterly SARs are reported on an exception basis, as follows:

- The current estimate exceeds the Program Acquisition Unit Cost (PAUC) objective or the Average Procurement Unit Cost (APUC) objective of the currently approved APB, both in base-year dollars, by 15 percent or more;
- The current estimate includes a 6-month or greater delay, for any schedule parameter, that occurred since the current estimate reported in the previous SAR;
- Milestone B or Milestone C approval occurs within the reportable quarter.
- Pre-Milestone B projects may submit RDT&E-only reports, excluding procurement, military construction, and acquisition-related operations and maintenance costs. DoD Components should notify USD(AT&L) with names of the projects for which they intend to submit RDT&E-only SARs 30 days before the reporting quarter ends. USD(AT&L) should so notify Congress 15 days before reports are due.

Whenever USD(AT&L) proposes changes to the content of a SAR, he or she will submit notice of the proposed changes to the Armed Services Committees of the Senate and House of Representatives. USD(AT&L) may consider the changes approved, and incorporate them into the report, 60 days after the committees receive the change notice.

10.9.2.2. SAR Waivers

The Secretary of Defense may waive the requirement for submission of a SAR for a program for a fiscal year if:

- The program has not entered system development and demonstration;
- A reasonable cost estimate has not been established for the program; and,
- The system configuration for the program is not well defined.

As delegated by the Secretary of Defense, USD(AT&L) will submit a written notification of each waiver for a fiscal year to the Armed Services Committees of the Senate and House of Representatives not later than 60 days before the President submits the budget to Congress, pursuant to 31 U.S.C. 1105, in that fiscal year.

10.9.2.3. SAR Termination

USD(AT&L) will consider terminating SAR reporting when 90 percent of expected production deliveries or planned acquisition expenditures have been made, or when the program is no longer considered an Acquisition Category I program in accordance with 10 U.S.C. 2432.

10.9.3. Unit Cost Reports (UCR)

In accordance with 10 U.S.C. 2433, the program manager will prepare UCRs for all Acquisition Category I programs submitting SARs, except pre-Milestone B programs that are reporting RDT&E costs only.

10.9.3.1. UCR Content and Submission

The program manager will submit a written report on the unit costs of the program to the CAE on a quarterly basis. The written report should be in the DAES. The program manager should submit the report by the last working day of the quarter, in accordance with DAES submission procedures. Reporting should begin with submission of the initial SAR, and terminate with submission of the final SAR. Each report should include the current estimate of the PAUC and the APUC (in base-year dollars); cost and schedule variances, in dollars, for each of the major contracts since entering the contract; and all changes that the program manager knows or expects to occur to program schedule or performance parameters, as compared to the currently approved APB.

10.9.3.2. UCR Breach Reporting

The program manager will notify the CAE immediately, whenever he or she has reasonable cause to believe that the current estimate of either the PAUC or APUC (in base-year dollars) has increased by 15 percent (or more) over the PAUC or APUC objective of the currently approved APB (in base-year dollars), respectively. (This is a Congressionally-reportable unit-cost breach.)

If the CAE determines that there is an increase in the current estimate of the PAUC or APUC cost of at least 15 percent over the currently approved APB, the CAE should inform USD(AT&L) and the cognizant Head of the DoD Component. If the cognizant Head of the DoD Component subsequently determines that there is, in fact, an increase in the current estimate of the PAUC or APUC of at least 15 percent over the currently

approved APB, the Head of the DoD Component will notify Congress, in writing, of a breach. The notification will be not later than 45 days after the end of the quarter, in the case of a quarterly report; or not later than 45 days after the date of the report, in the case of the reasonable cause report. In either case, notification will include the date that the Head of the DoD Component made the determination.

In addition, the Head of the DoD Component will submit a SAR for either the fiscal year quarter ending on or after the determination date, or for the fiscal year quarter that immediately precedes the fiscal year quarter ending on or after the determination date. This SAR should contain the additional, breach-related information.

If the current estimate of the PAUC or APUC increases by at least 25 percent over the PAUC or APUC objective of the currently approved APB, USD(AT&L) must submit a written certification to Congress before the end of the 30 day period beginning on the day the SAR containing the unit cost information is required to be submitted to Congress. The certification must state the following:

- Such acquisition program is essential to the national security.
- There are no alternative programs that will provide equal or greater military capability at less cost.
- The new estimates of the PAUC or APUC are reasonable.
- The management structure for the acquisition program is adequate to manage and control the PAUC and the APUC.

If the Head of the DoD Component makes a determination of either a PAUC or APUC increase of 15 percent or more, and a SAR containing the additional unit-cost breach information is not submitted to Congress as required; or if the Head of the DoD Component makes a determination of a 25 percent increase in the PAUC or APUC, and a certification by the USD(AT&L) is not submitted to Congress as required; funds appropriated for RDT&E, procurement, or military construction may not be obligated for a major contract under the program. An increase in the PAUC or APUC of 25 percent or more resulting from the termination or cancellation of an entire program will not require USD(AT&L) program certification.

10.9.4. Defense Acquisition Executive Summary (DAES)

The DAES is a multi-part document, reporting program information and assessments; program manager, Program Executive Officer, CAE comments; and cost and funding data. The DAES provides an early-warning report to USD(AT&L) and ASD(NII). The DAES describes actual program problems, warns of potential program problems, and describes mitigating actions taken or planned. The program manager may obtain permission from USD(AT&L) or ASD(NII) to tailor DAES content. At minimum, the DAES should report program assessments (including interoperability), unit costs (10 U.S.C. 2433), and current estimates. It should also report the status of exit criteria and vulnerability assessments (31 U.S.C. 9106).

The DAES should present total costs and quantities for all years, as projected, through the end of the current acquisition phase. In keeping with the concept of total program reporting, the DAES should present best estimates for costs beyond the FYDP, if the

FYDP does not otherwise identify those costs. (The total program concept refers to system acquisition activities from Program Initiation through Production and Deployment.) The DAES should also report approved program funding for programs that are subsystems to platforms and whose procurement is reported in the platform budget line.

The Office of USD(AT&L), the Office of ASD(NII), the Offices of DoD CAEs, CIOs, and Program Executive Officers, and the program office should each establish DAES focal points.

10.9.4.1. DAES Reporting

USD(AT&L) will designate Acquisition Category I programs subject to DAES reporting and assign each program to a quarterly reporting group. ASD(NII) will designate Acquisition Category IA programs subject to DAES reporting and assign each program to a quarterly reporting group. Program managers will use CARS software to prepare the DAES, and submit both hard and electronic copies to USD(AT&L) by the last working day of the program's designated quarterly reporting month. Acquisition Category IA programs will submit an electronic copy of their DAES report to ASD(NII) 30 days after the end of the quarter. Program managers should not delay the DAES for any reason.

10.9.4.2. Out-of-Cycle DAES Reporting

There are two types of out-of-cycle DAES:

- The program manager should submit a DAES when there is reasonable cause to believe that a Nunn-McCurdy unit cost breach has occurred or will occur (10 U.S.C. 2433 (c) (reference). (Submitting DAES sections 5, 6.2, and 7, block #28, satisfy this requirement.)
- If submission of the DoD Component's POM or BES causes the program to deviate from the approved APB thresholds, the program manager will submit DAES sections 5, 6.2, and 8.

10.9.4.3. Consistency of DAES Information

DAES information should be consistent with the information in the latest ADM, APB, and other mandatory or approved program documentation.

10.10. Consolidated Acquisition Reporting System (CARS)

The Consolidated Acquisition Reporting System (CARS) is a personal computer-based data entry and reporting system combining both common and unique Defense Acquisition Executive Summary (DAES) and Selected Acquisition Report (SAR), and Acquisition Program Baseline (APB) components into a unified database from which DAES and SAR reports and APB documents can be printed.

Based upon an OSD enterprise decision, the use of CARS is mandatory for all MDAPs and MAIS acquisition programs, and must be employed to satisfy statutory requirements for SAR submission. However, non-MDAP and non-MAIS programs may also use the system.

CARS has three reporting modules that generate the APB, the SAR, and the DAES. The DAES and SAR include quarterly unit cost and unit cost breach exception reporting, respectively. Analysis routines are also included (for example, the Computational Module that supports the SAR cost change calculations, and SAR and DAES data checks). The Director, Acquisition Resources and Analysis, maintains a CARS "help line" for user support.

A unique program number (PNO) identification system controls the use of CARS. The Office of USD(AT&L) focal point assigns a PNO to each using Acquisition Category I program. The Office of ASD(NII) focal point assigns a PNO to each using Acquisition Category IA program.

The CARS software specifies the format of the APB, SAR, and DAES, except for narrative or memo-type information.

The three reporting modules share some, but not all, of the CARS data. For example, the DAES and SAR incorporate the APB parameters. The modules also share some contract information.

Only the appropriate Office of USD(AT&L) or DoD Component focal point can edit some of the CARS information, such as the SAR baseline and APB. The Milestone Decision Authority must approve SAR baseline and APB changes. The appropriate Office of USD(AT&L) or DoD Component focal point distributes disks containing the revised or new information.

The Director, Acquisition Resources and Analysis, has responsibility for the development, upgrade, and maintenance of CARS. Direct questions and requests for copies of the software should be directed to that organization. The CARS software includes mandatory instructions for preparing the APB, SAR, DAES, and UCR, including administrative procedures. The CARS web page also has the instructions.

CHAPTER 11
Program Management Activities

11.0. Overview

11.0.1. Purpose

The purpose of this chapter is to describe and explain some of the activities and decisions available to and required of the program manager as he or she manages and executes the program.

11.0.2. Contents

Chapter 11 covers the following topics:

- Joint Programs
- International Cooperation
- Integrated Program Management
- Earned Value Management
- Contract Management Reporting
- Risk Management
- Knowledge-Based Acquisition
- Performance-Based Business Environment
- Total Life Cycle Systems Management
- Integrated Product and Process Development
- Technical Representatives at Contractor Facilities
- Contractor Councils
- Government Property in the Possession of Contractors
- Integrated Digital Environment
- Simulation-Based Acquisition and Modeling and Simulation
- Independent Expert Review of Software-Intensive Programs

Additional information regarding Program Management can be found at the Acquisition Community Connection (ACC) Program Management Community of Practice web site.

11.1. Joint Programs

There are two aspects of "jointness" to consider when discussing joint program management: the jointness of the capability and the jointness of the development and production of the system.

11.1.1. Acquiring Joint Capabilities

As part of the Joint Capabilities Integration and Development System, the Joint Staff J-8, with the assistance of US Joint Forces Command and additional Joint Staff resources, evaluates all Joint Capabilities Integration and Development System documents, regardless of Acquisition Category or previous delegation decisions or Joint Planning Document decisions, to determine whether the proposal has joint force implications.

Section 1.3 provides a brief overview of the Joint Capabilities Integration and Development System. The Joint Staff documents, CJCSI 3170.01 and CJCSM 3170.01, provide full detail and direction on this topic.

11.1.2. Joint Acquisition Management

Acquisitions that contribute to joint capabilities may be managed as joint acquisition programs. A "joint acquisition" is any acquisition system, subsystem, component, or technology program with a strategy that includes funding by more than one DoD Component during any phase of a system's life cycle. DoD Instruction 5000.2 addresses DoD Component fiscal responsibilities associated with participation in programs under joint acquisition management.

11.1.2.1. Designation

Considering the assigned Joint Potential Designator and the recommendation of the Heads of the DoD Components, the Milestone Decision Authority decides whether to place the program under joint acquisition management. The Milestone Decision Authority should make this decision and, if appropriate, designate the Lead Executive DoD Component, as early as possible in the acquisition process.

The DoD Components should periodically review their programs to determine the potential for joint cooperation. The DoD Components should structure program strategies to encourage and to provide an opportunity for multi-Component participation.

11.1.2.2. Execution

The designated Lead Executive DoD Component for a joint acquisition should act on behalf of all DoD Components involved in the acquisition.

A Memorandum of Agreement should specify the relationship and respective responsibilities of the Lead Executive DoD Component and the other participating components. The Memorandum of Agreement should address system capabilities and the development of capabilities documents, funding, manpower, and the approval process for other program documentation.

The following additional considerations have proven effective in managing joint programs:

- The assignment of a Lead Executive DoD Component should consider the demonstrated best business practices of the DoD Components, including plans for effective, economical, and efficient management of the joint program; and the demonstrated willingness of the DoD Component to fund the core program, essential to meeting joint program needs.

- The Milestone Decision Authority and DoD Components should consolidate and co-locate the supporting efforts of the joint program at the Lead Executive DoD Component's program office, to the maximum extent practicable.
- The Component Acquisition Executive of the Lead Executive DoD Component should optimally use the acquisition organizations, test organizations, and other facilities of all Military Departments.
- The designated Lead Executive DoD Component selects the qualified program manager for the designated program under joint acquisition. The single program manager should then be fully responsible and accountable for the cost, schedule, and performance of the development system.
- If the joint program results from a consolidation of several different DoD Component programs, each with a separate program manager, the selected joint program manager should have the necessary responsibility and authority to effectively manage the overall system development and integration.
- A designated program under joint acquisition should have one quality assurance program, one program change control program, one integrated test program, and one set of documentation and reports (specifically: one set of capabilities documents, one Information Support Plan, one Test and Evaluation Master Plan, one Acquisition Program Baseline, etc.).
- The Milestone Decision Authority should designate the lead Operational Test Agency to coordinate all operational test and evaluation. The lead Operational Test Agency should produce a single operational effectiveness and suitability report for the program.
- Documentation for decision points and periodic reporting should flow only through the Lead Executive DoD Component acquisition chain, supported by the participating components.
- The program should use inter-DoD Component logistics support to the maximum extent practicable, consistent with effective support to the operational forces and efficient use of DoD resources.
- Unless statute, the Milestone Decision Authority, or a memorandum of agreement signed by all DoD Components directs otherwise, the Lead Executive DoD Component should budget for and manage the common Research, Development, Test, and Evaluation funds for the assigned joint programs.
- Individual DoD Components should budget for their unique requirements.

11.2. Considerations for International Cooperation

11.2.1. International Cooperative Programs

An international cooperative program is any acquisition system, subsystem, component, or technology program with an acquisition strategy that includes participation by one or more foreign nations, through an international agreement, during any phase of a system's life cycle. The key objectives of international cooperative programs are to reduce

weapons system acquisition costs through cooperative development, production, and support; and to enhance interoperability with coalition partners.

11.2.1.1. International Considerations and Program Strategy

Title 10 U.S.C. 2350a(e) requires an analysis of potential opportunities for international cooperation for all Acquisition Category I programs. DoD Directive 5000.1 and DoD Instruction 5000.2 specify the requirements for international considerations; amplifying guidance and information appears in this Guidebook. DoD Directive 5000.1 requires International Armaments Cooperation; requires interoperability with U.S. coalition partners; and establishes the preference for a cooperative development program with one or more Allied nations.

During the development of the initial acquisition strategy for a new program, the potential for international cooperative research, development, production, and logistic support should be addressed, and thereafter, the potential for international cooperation should be considered in every phase of the acquisition process. DoD Components should periodically review their programs to determine the potential for international cooperation. Milestone Decision Authorities may recommend forming international cooperative programs based on the international program acquisition strategy considerations; DoD Component Heads may also recommend forming international cooperative programs. The Milestone Decision Authority should make the decision to establish an international cooperative program as early as possible in the acquisition process.

The Milestone Decision Authority, with the advice and counsel of the DoD Components and the Joint Requirements Oversight Council, makes the decision to pursue an international cooperative program. The decision process should consider the following:

Demonstrated best business practices, including a plan for effective, economical, and efficient management of the international cooperative program;

Demonstrated DoD Component willingness to fully fund their share of international cooperative program needs;

The long-term interoperability and political-military benefits that may accrue from international cooperation; and

The international program's management structure documented in the international agreement. The designated program manager (U.S. or foreign) is fully responsible and accountable for the cost, schedule, and performance of the resulting system.

The DoD Component remains responsible for preparation and approval of most statutory, regulatory, and contracting reports and milestone requirements, as listed in DoD Instruction 5000.2. Documentation for decision reviews and periodic reports flow through the DoD Component acquisition chain, supported by the participating nation(s).

International cooperation can add stability to the program. DoD Instruction 5000.2 prevents DoD Components from terminating or reducing participation in some international cooperative programs without Milestone Decision Authority notification, and in some cases, Milestone Decision Authority approval.

Additional information may be found in the OSD/IC International Armaments Cooperation Handbook.

11.2.1.2. International Considerations within the Acquisition Management Framework

Department of Defense policy promotes international cooperative acquisition, technology and logistics activities, especially with allies and friends, that will enable the warfighter to be well prepared and supported for coalition operations. (USD(AT&L) Memorandum, International Cooperation in Acquisition, Technology and Logistics, April 27, 2004) International programs may be established at any point in the DoD Instruction 5000.2 defense acquisition management framework, when justified as a prudent business judgment. Figure 11.2.1.2.1. depicts the key considerations for each phase:

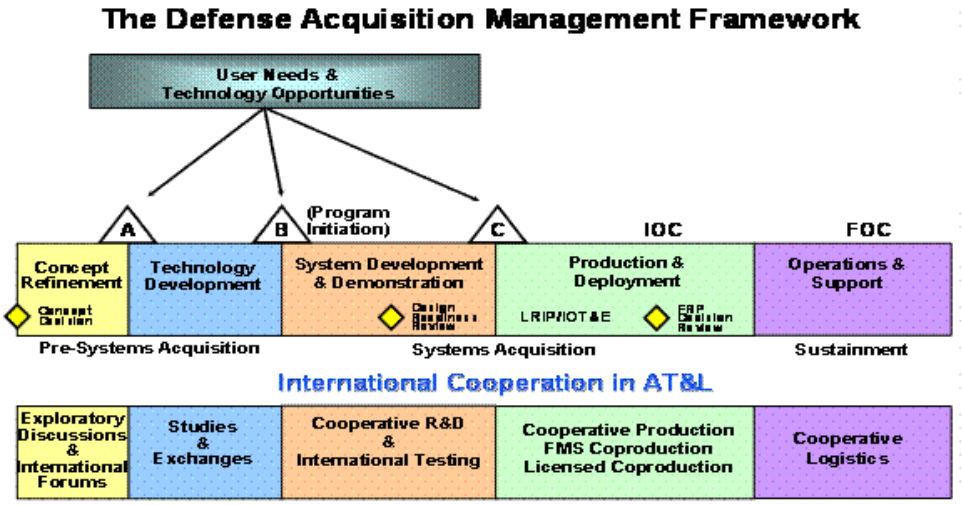

Figure 11.2.1.2.1. Key International Cooperative considerations during Acquisition.

Determination of User Needs & Exploring Technology Opportunities (Early Technology Projects). The efforts needed to identify cooperative development opportunities before entering into a formal acquisition program are often challenging, but such activities capitalize on high payoffs in cost savings and interoperability when successful. Formulation of cooperative development programs involves resolution of issues in the areas of requirements harmonization, cost sharing, work sharing, technology transfer, intellectual property rights, and many others. While multinational force compatibility may increase system acquisition cost, it can provide more cost-effective defense for the whole force through increased interoperability and reduced life-cycle costs. Cooperative opportunities identification and formulation should be pursued during the earliest stages of the pre-systems acquisition research and development process to maximize the chance for success. This includes during Advanced Technology Demonstrations, Joint Warfighting

Experiments, Advanced Concept and Technology Demonstrations, Concept Refinement, and Technology Development.

Using the Joint Capabilities Integration and Development System process, representatives from multiple DoD communities formulate broad, time-phased, operational goals, and describe requisite capabilities in the Initial Capabilities Document. They examine multiple concepts and materiel approaches to optimize the way the Department of Defense provides these capabilities. This examination includes robust analyses that consider affordability, technology maturity, and responsiveness.

Several important mechanisms available to provide insight into the needs of potential foreign partners are exploratory discussions, international forums, studies, and the exchanges of information and personnel:

Exploratory Discussions. Before entering into an international project, many forms of dialogue can take place with potential partners. These informal discussions are usually called exploratory discussions or technical discussions--they are NOT called "negotiations," which requires a legal authority and formal permission from the Office of the Secretary of Defense. The avoidance of any binding commitments on the part of the U.S. Government, and the absence of any draft, international agreements characterize exploratory discussions. Other than the two exclusions above, the parties may discuss most other topics, provided release authority has been obtained for any information provided by DoD representatives or defense contractors.

International Forums. There are many international forums dedicated to discussing mutual armaments needs and early technology projects. These forums include the Conference of National Armaments Directors (CNAD), whose U.S. representative is the USD(AT&L). The CNAD's subsidiaries are the "Main Armaments Groups," particularly the NATO Army Armaments Group (NAAG), NATO Navy Armaments Group (NNAG), and the NATO Air Force Armaments Group (NAFAG). The NATO Research and Technology Organization (RTO) conducts and promotes cooperative research and information exchange in NATO. The Technical Cooperation Program (TTCP) with Australia, Canada, New Zealand, and the United Kingdom is another multilateral forum dedicated to cooperation in conventional military technology development. In addition there are a number of bilateral forums, such as the U.S.-Japan Systems and Technology Forum and the U.S./Canadian Armaments Cooperation Management Committee that have a similar purpose.

Studies. It is normal for the DoD and potential partners to conduct studies before entering into a cooperative acquisition project. These studies can be conducted years before the project starts, and are often called feasibility studies, or pre-feasibility studies. Industry, government agencies, or a combination of both generally conduct the feasibility studies, with the objective of providing a technical appraisal of the feasibility of developing and producing equipment. These studies can develop input for the Analysis of Alternatives required by DoD before the start of a new acquisition program.

International Exchanges of Information and Personnel. A common source for cooperative program opportunity identification is the Defense Research, Development, Test and Evaluation Information Exchange Program (IEP), which provides a standardized way of conducting bilateral science and technology information exchange (formerly

called data exchange). The IEP has proven extremely useful as a means of cooperative opportunities formulation. Another source for identifying cooperative opportunities is the Engineer and Scientist Exchange Program (ESEP).

Pre-Systems Acquisition. Decisions made during the Concept Refinement and Technology Development phases of Pre-Systems Acquisition generally define the nature of the entire program. Once the program enters the System Development and Demonstration phase, it is difficult to adopt major changes without significant schedule or cost adjustments. Consequently, the decision to include international partners needs to be addressed as early as possible, preferably during development of the Initial Capabilities Document, but no later than during the Concept Refinement phase.

To meet the requirements of 10 U.S.C. 2350a (e), the acquisition strategy for an Acquisition Category I program must address the following areas:

a) Is a similar project in development or production by NATO, a NATO organization, a member nation of NATO, a major non-NATO ally, or friendly foreign country?

b) If so, the acquisition strategy provides an assessment of that project as to whether or not it could satisfy or be modified to satisfy U.S. military requirements.

c) An assessment of the advantages and disadvantages with regard to program timing, developmental and life cycle costs, technology sharing, and Rationalization, Standardization, Interoperability (RSI) of a cooperative development program.

d) Provide a specific recommendation whether or not a cooperative program should be explored.

e) What alternate forms of cooperation could be appropriate for the project?

Except for e) above, these considerations are based on 10 U.S.C. 2350a requirements. They force the consideration of alternative forms of international cooperation. Even if cooperative development is impractical, cooperative production, foreign military sales, licensed production, component/subcomponent co-development, or incorporation of subsystems from allied or friendly foreign sources should be considered and may be appropriate.

DoD Components should fully investigate potential cooperative opportunities as part of the acquisition strategy development. Program proponents should consult with the appropriate international programs organization to obtain assistance in addressing international considerations during acquisition strategy development for programs in all acquisition categories.

System Development and Demonstration Phase. After program initiation, during System Development and Demonstration, key elements of the system design are defined, and system/subsystem development begins. Major changes often present schedule delays that program managers are unwilling to accept; however, there have been numerous examples of successful subsystem cooperative development partnerships that have been formed during the System Development and Demonstration Phase. Once a program has reached this phase, absent cooperation in earlier stages, there will be only limited opportunity to bring other nations on as full cooperative development partners. Consequently, if the opportunity for cooperation in subsystem development arises prior to or during System

Development and Demonstration, consult with the appropriate international programs organization to obtain further assistance.

Foreign Comparative Testing. A viable alternative to development is the acquisition of commercial items. While individual acquisition programs can conduct evaluations with their own resources, the Foreign Comparative Testing (FCT) Program offers a structured and funded means for program offices to evaluate the suitability of a foreign developed item for purchase in lieu of developing a similar U.S. item.

International Test Operations Procedures. The International Test Operations Procedures (ITOP) program provides for international agreements that document state-of-the-art test techniques for technical testing of military material and allows the exchange of test data to avoid redundant testing when foreign equipment is purchased. Currently there are over 130 ITOPs with Germany, France, and the UK covering a variety of test types and/or equipment class. Through ITOPs, the U.S. has access to latest test technology and procedures of our allies, which could possibly be utilized by DoD program managers. The ITOP program is managed at OSD by the Office of the Director, Operational Test and Evaluation (DOT&E).

Production and Deployment Phase. There are three basic mechanisms for transfer of U.S. produced defense articles and associated production capability to other nations. The first two, (1) Foreign purchase and (2) Foreign co-production of a U.S. developed system, fall under the purview of the Defense Security Cooperation Agency (DSCA). The Department of State is responsible for transfer of defense articles and associated production capability under export licenses. Both DSCA and the Defense Technology Security Administration coordinate closely with the cognizant DoD Component regarding the development and implementation of DoD co-production policy in their respective areas of responsibility. USD(AT&L) is responsible for oversight of the third basic mechanism, (3) Cooperative production. Cooperative production is a joint or concurrent international production arrangement arising from a cooperative development project. Examples of this type of production program are the Rolling Airframe Missile (RAM) and the Multi-Functional Information Distribution System (MIDS). Cooperative production falls under the authority of the Arms Export Control Act (AECA) Section 2751.

Operations & Support Phase. Cooperative logistics refers to cooperation between the U.S. and allied or friendly nations or international organizations in the logistical support of defense systems and equipment. Cooperative logistics is part of the acquisition process, but as a substantial part of military operations, much of the implementation process involves Security Assistance processes and procedures.

Cooperative logistics support includes:

- Logistics Cooperation international agreements (IAs), used to improve sharing of logistics support information and standards, and to monitor accomplishment of specific cooperative logistics programs;
- Acquisition and Cross-Servicing Agreements;
- Host Nation Support;
- Cooperative Logistics Supply Support Arrangements;

- Cooperative Military Airlift Agreements;
- War Reserve Stocks for Allies;
- Agreements for acceptance and use of real property or services;
- Standardization of procedures under America/Britain/Canada/Australia/New Zealand auspices;
- International Standardization Agreements developed in conjunction with member nations of the North Atlantic Treaty Organization and other allies and coalition partners, as described in DoD 4120.24-M, Defense Standardization Program (DSP) Policies and Procedures and as listed in the ASSIST database;
- Consideration of the interoperability implications of these agreements when constructing Work Breakdown Structures; and
- Planning support provide by the Program Manager's Tool.

Each participant or party involved in cooperative logistics agreements should benefit from the agreement. Benefits could be tangible, such as the U.S. receiving support for its naval vessels when in a foreign port; or intangible, such as the foreign nation receiving the implied benefit of a visible, U.S. naval presence in the region. Other cases are more obviously quid-pro-quo: cross-servicing agreements, for example. In a cross servicing agreement, each party receives the equivalent of the materiel or services provided to the other party. Besides the obvious material benefits, such agreements have the collateral effects of opening dialog and creating relationships between the parties. Such dialog and relationships may serve to strengthen political bonds. While not a program manager responsibility, DoD acquisition personnel should be aware of the international consequences of their activities and appropriately support such efforts.

11.2.1.3. International Cooperative Program Protection

Program protection considerations play a major role in international cooperative programs for obvious reasons. The program manager should consider technology security factors when developing an international cooperative program. The Defense Technology Security Administration, in concert with DoD Component technology security organizations, is the focal point within the DoD for technology security. Program managers should contact their DoD Component technology security organization early enough in the process to ensure that technology security factors that may affect cooperative efforts are taken into consideration.

The program manager should consider technology release in the initial planning of an international cooperative program through a review of National Disclosure Policy foreign disclosure guidance and development of the foreign disclosure and export control elements of the program's Technology Assessment/Control Plan. Early consideration of National Disclosure Policy requirements and foreign disclosure/export control planning in an international cooperative program should enable the international program to avoid major cost, schedule, and performance goal impacts.

DoD Instruction 5000.2, paragraphs 3.4.2, 3.7.1, and Table E3.T2., establish international cooperative program protection policy. Chapter 8 of this Guidebook provides additional insights into this policy.

11.2.1.3.1. Classification Guide

In addition to the Program Protection Plan required by all programs containing Critical Program Information, DoD Directive 5200.1 requires international programs to develop a classification guide for all programs containing classified information of either party. The classification guide identifies the items or information to be protected in the Program, and indicates the specific classification to be assigned to each item.

11.2.1.3.2. Program Security Instruction (PSI)

A Program Security Instruction (PSI) details security arrangements for the program and harmonizes the requirements of the Participants' national laws and regulations. Using the USD(AT&L) international agreements streamlined procedures authorized by DoD Instruction 5000.2, the International Agreements Generator will lead the program manager through the considerations for, and the development of, a PSI. Additional information about the PSI is found in the International Armaments Cooperation Handbook.

If all security arrangements to be used in an international program are in accordance with an existing industrial security arrangement between the Participants, a separate PSI is not required.

11.2.1.3.3. Delegation of Disclosure Authority Letter (DDL)

Per DoD Instruction 5000.2, a written authorization to disclose any classified or controlled unclassified information must be obtained prior to entering discussions with potential foreign partners. The authorization for release of classified information (developed or used during any part of the lifecycle of the program) to any potential or actual foreign participants in the program will be in the form of a Delegation of Disclosure Authority Letter (DDL) (DoD Directive 5230.11) or other written authorization issued by the DoD Component Foreign Disclosure Office. The authorization for release of classified or controlled unclassified information must comply with DoD Component policies for release of such information.

11.2.1.3.4. Technology Release Roadmap (TRR)

Prior to the System Design and Demonstration phase of an acquisition program with substantial international involvement by foreign industry, the program manager should prepare an export control TRR as part of their Technology Assessment/Control Plan. This TRR will project when export licenses will be required in support of the acquisition

process, and when critical milestones regarding national disclosure policy implementation will need to be addressed. The TRR must be consistent with the program's Technology Assessment /Control Plan (TA/CP), security classification guide, and other disclosure guidance.

The TRR accomplishes the following:

- Provides early DoD Component planning for the program's proposed technology releases to foreign industry consistent with the National Disclosure Policy.

- Provides early planning for higher-level (i.e., above DoD Component-level) special technical reviews and approvals (i.e. Low Observable/Counter Low Observable, anti-tamper, cryptography) needed in support of proposed technology releases to foreign industry.

- Establishes a detailed export license approval planning process for U.S.-foreign industry cooperation to meet critical program and contract timelines.

The TRR includes three sections: 1) A timeline mapping key projected export licenses against the program acquisition schedule; 2) A definition of the technologies involved in each export license; and 3) A list of U.S. contractors (exporters) as well as foreign contractors (end users) for each license.

11.2.2. OUSD(AT&L) – Related International Agreement Procedures

An International Agreement (IA) is any agreement concluded with one or more foreign governments including their agencies, instrumentalities, or political subdivisions, or with an international organization. The IA delineates respective responsibilities and is binding under international law. IAs are required by U.S. law for all international cooperative projects.

Per DoD Instruction 5000.2, all AT&L-related international agreements may use the USD(AT&L)-issued streamlined procedures found in this Guidebook and in the *International Armaments Cooperation Handbook*, rather than following the lengthy documentation requirements mandated by DoD Directive 5530.3, International Agreements.

11.2.2.1. Preparation and Documentation

The following considerations apply to the preparation of and documentation associated with AT&L-related international agreements:

- Program managers or project leaders consult with the DoD Component's international programs organization, as well as foreign disclosure, legal, and comptroller personnel, to develop international agreements.

- The DoD Components develop international agreements in accordance with the provisions of the most recent version of DoD International Agreement Generator computer software.
- Prior to initiating formal international agreement negotiations, the DoD Components prepare a Request for Authority to Develop and Negotiate (RAD) that consists of a cover document requesting such authority and a Summary Statement of Intent (SSOI) that describes the DoD Component's proposed approach to negotiations.
- Prior to signing an international agreement, the DoD Components prepare a Request for Final Approval (RFA) that consists of a cover document requesting such authority, a revised SSOI that describes the outcome of negotiations, and the full text of the international agreement to be signed on behalf of the Department of Defense.
- The DoD Components should use the Streamlining I Coordination Process described in section 11.2.2.3.2. for both the Request for Authority to Develop and Negotiate and the Request for Final Approval. They should apply to Office of the USD(AT&L)/International Cooperation to be delegated authority to use Streamlining II procedures for processing International Agreements. If Streamlining II authority is or has been delegated, the DoD Component should use the process in section 11.2.2.3.2. (As of June 2005, the Office of the USD(AT&L)/International Cooperation has only delegated Streamlining II authority to the Department of the Navy.)

11.2.2.2. OUSD(AT&L) Oversight

OUSD(AT&L)/International Cooperation (IC) provides the following international agreement oversight support:

- Approves and makes available the following agreement process guidance:
  - Request for Authority to Develop (RAD);
  - Request for Final Approval (RFA);
  - Summary Statement of Intent (SSOI);
  - Arms Export Control Act Section 27 Project Certification format requirements; and
  - DoD International Agreement Generator computer software.
- Approves the following agreement process actions:
  - RADs and RFAs for Memoranda of Understanding (MOU)/Memoranda of Agreement (MOA);
  - Project Agreements and Arrangements (PAs);
  - Arms Export Control Act Section 65 Loan Agreements;
  - End-User Certificate (EUC) Waivers (See DoD Directive 2040.3.);

- The Foreign Military Sales of items which have not completed operational test and evaluation successfully (Yockey Waivers); and
- DoD Component requests for DoD International Agreement Generator text deviations or waivers requested in RAD and RFA submissions.

- Delegates PA negotiation authority under the Streamlining I approval process to specifically designated DoD Components.
- Certifies DoD Component international agreement processes to the Streamlining II standards prior to delegation of RAD/RFA authority to a DoD Component.
- Decertifies a DoD Component international agreement process in the event minimum quality standards are not maintained.
- Resolves RAD/RFA coordination process disputes.
- Supports satisfaction of the following statutory requirements:
- Obtains USD(AT&L) determination under 10 U.S.C. 2350a(b) for all international agreements that rely upon this statute as their legal authority;
- Notifies Congress of all Arms Export Control Act Section 27 (see 22 U.S.C. Section 2767, "Authority of President to enter into cooperative projects with friendly foreign countries") international agreements a minimum of 30 calendar days prior to authorizing agreement signature; and
- Conducts interagency coordination with the Department of State, Department of Commerce, and the Department of the Treasury (see 22 U.S.C. 2767 and DoD Directive 5530.3).

11.2.2.3. Coordination Processes

There are two accredited international agreement coordination processes: Streamlining I and Streamlining II.

11.2.2.3.1. International Agreement Streamlining I Process

OUSD(AT&L)/IC uses the following Streamlining I process unless it has delegated coordination authority to the DoD Component:

Request for Authority to Develop and Negotiate (RAD) MOUs and MOAs. The DoD Component prepares the RAD and obtains OUSD(AT&L)/IC approval prior to initiating MOU or MOA negotiations. If applicable, the DoD Component develops and submits Coalition Warfare (CW) Initiative funding requests associated with the RAD, in accordance with the CW Management Plan. OUSD(AT&L)/IC conducts DoD and interagency coordination, as appropriate, using a standard review period of 21 working days, which may expedited at OUSD(AT&L)/IC's discretion.

Request for Authority to Develop and Negotiate (RAD) PAs and Section 65 Loan Agreements. Unless OUSD(AT&L)/IC delegates PA negotiation authority, the DoD Component prepares a RAD and obtains OUSD(AT&L)/IC approval prior to initiating Program Authorization (PA) or Section 65 Loan Agreement negotiations. OUSD(AT&L)/IC conducts interagency coordination, as appropriate, using a standard

review period of 15 working days, which may be expedited at OUSD(AT&L)/IC's discretion.

Negotiation. Generally, within 9 months of receipt of RAD authority, the DoD Component negotiates the international agreement in accordance with the provisions of the most recent version of DoD International Agreement Generator.

Request for Final Approval to Conclude (RFA) MOUs and MOAs. The DoD Component prepares the RFA and obtains OUSD(AT&L)/IC approval prior to signing the MOU or MOA. RFAs for agreements relying upon Arms Export Control Act (AECA) Section 27 of the Arms Export Control Act as the legal authority for the international agreement will also include a Project Certification. OUSD(AT&L)/IC conducts interagency coordination, as appropriate, based upon a standard review period of 21 working days, which may be expedited at OUSD(AT&L)/IC's discretion. OUSD(AT&L)/IC provides Congress with any required AECA Section 27 notifications.

Request for Final Approval to Conclude (RFA) PAs and Section 65 Loan Agreements. The DoD Component submits RFAs notifying OUSD(AT&L)/IC of its intention to sign PAs and Section 65 Loan Agreements prior to concluding such agreements. AT&L/IC conducts interagency coordination, as appropriate, based upon a review period of 15 working days, which may be expedited at OUSD(AT&L)/IC's discretion. OUSD(AT&L)/IC provides Congress with any required AECA Section 27 notifications.

11.2.2.3.2. International Agreement Streamlining II Process

OUSD(AT&L)/IC may delegate approval authority for the Request for Authority to Develop and Negotiate/Request for Final Approval (RAD/RFA) for all international agreements associated with programs with a total program value of less than $25M (in FY01 constant dollars) and for Acquisition Category II and Acquisition Category III programs to the DoD Component Acquisition Executive. The DoD Component Acquisition Executive may subsequently re-delegate RAD/RFA authority for programs with a total program value of less that $10M (in FY01 constant dollars) and Acquisition Category III programs to the Head of the DoD Component's international programs organization. The following procedures will apply:

The DoD Components will obtain the concurrence of their legal, financial management, and foreign disclosure organizations prior to approving RADs/RFAs.

The DoD Components will forward coordination disputes to OUSD(AT&L)/IC for resolution.

The DoD Components will send Notices of Intent to Negotiate (NINs) or Notices of Intent to Conclude (NICs) to OUSD(AT&L)/IC for all approved RADs and RFAs. NINs will include the DoD Component’s approval document and program SSOI. NICs will also include the final international agreement text to be signed, plus an AECA Section 27 Project Certification, if required. The DoD Components will not sign international agreements until a 15-working-day period (for PAs and Loans) or 21-working-day period (for MOUs) after AT&L/IC receipt of the NIC has elapsed and any required 10 U.S.C.

2350a approval or Arms Export Control Act (AECA) Section 27 Congressional notification process has been completed.

OUSD(AT&L/IC) may, at its discretion, decide to waive these rules on a case-by-case basis and require that certain agreements receive specific OUSD(AT&L/IC) approval before conclusion.

OUSD(AT&L)/IC will use Notices of Intent to Negotiate (NINs), NICs and other relevant information to verify DoD Component international agreement process quality.

Generally, within 9 months of receipt of RAD authority, DoD Component personnel will negotiate the international agreement in accordance with the provisions of the most recent version of DoD International Agreement Generator.

11.2.2.3.3. Coordination of Requests for Authority to Develop and Negotiate (RADs), Requests for Final Approval (RFAs), Notices of Intent to Negotiate (NINs), and Notices of Intent to Conclude (NICs) Relating to Nuclear, Chemical, and Biological (NCB) Fields.

The Office of the USD(AT&L)/International Cooperation coordinates all international agreements (including Memoranda of Understanding, Project Arrangements, other similar agreements) and Information Exchange Program annexes relating to NCB warfare technologies (including defenses against such technologies) with the Assistant to the Secretary of Defense (Nuclear and Chemical and Biological Defense Programs) prior to approving the agreement. DoD policy requires this coordination for NCB-related RADs for project arrangements under Streamlining I authority, and for NINs and NICs under Streamlining II authority.

11.2.3. Acquisition and Cross-Servicing Agreements (ACSA)

Acquisition and Cross-Servicing Agreements are bilateral international agreements that allow for the provision of cooperative logistics support under the authority granted in 10 U.S.C. Sections 2341-2350. They are governed by DoD Directive 2010.9, “Acquisition and Cross-Servicing Agreements” and implemented by CJCS Instruction 2120.01, “Acquisition and Cross-Servicing Agreements.” ACSAs are intended to provide an alternative acquisition option for logistics support in support of exercises or exigencies.

11.2.3.1. Types of Acquisition and Cross-Servicing Agreements (ACSA) Authorities

Title 10 of the United States Code provides two legal authorities for foreign logistic support, supplies, and services: an Acquisition-only Authority, and a Cross-Servicing Authority, which includes an acquisition authority and a transfer authority.

Acquisition-Only Authority. 10 U.S.C. 2341, "Authority to acquire logistic support, supplies, and services for elements of the armed forces deployed outside the United States," authorizes elements of the U.S. Armed Forces, when deployed outside the United States, to acquire logistic support, supplies, and services from eligible foreign entities on a reimbursable basis. The authority is not reciprocal and does not require an approved

ACSA in place. Acquisition-only authority may be used with the governments of NATO members, NATO and its subsidiary bodies, the United Nations Organization, any regional organization of which the United States is a member, and any other countries which meet one or more of the following criteria:

- Has a defense alliance with the United States;
- Permits the stationing of members of the armed forces in such country or the home porting of naval vessels of the United States in such country;
- Has agreed to preposition materiel of the United States in such country; or
- Serves as the host country to military exercises which include elements of the armed forces or permits other military operations by the armed forces in such country.

Cross-Servicing Authority. 10 U.S.C. 2342, "Cross-servicing agreements," authorizes the Department of Defense, upon coordination with the Secretary of State, to conclude reciprocal agreements with foreign countries and regional and international organizations for the provision of logistics, support, supplies and services. A current listing of these agreements and countries and organizations eligible to negotiate them is maintained by the Director for Logistics, The Joint Staff (J-4). DoD Directive 2010.9 provides the official process for nominating countries for eligibility for such agreements as well as for concluding them.

11.2.3.2. Permitted and Prohibited Uses of Acquisition and Cross-Servicing Agreements (ACSA)

ACSA is for the transfer of logistics, support, supplies, and services only. Per Section 4.5 of DoD Directive 2010.9, items that may not be acquired or transferred under ACSA authority include weapons systems; the initial quantities of replacement and spare parts for major end items of equipment covered by tables of organization and equipment, tables of allowances and distribution, or equivalent documents; and major end items of equipment. Specific items that may not be acquired or transferred under ACSA authority include guided missiles; naval mines and torpedoes; nuclear ammunition and included items such as warheads, warhead sections, projectiles, demolition munitions, and training ammunition; cartridge and propellant-actuated devices; chaff and chaff dispensers; guidance kits for bombs or other ammunition; and chemical ammunition (other than riot control agents). General purpose vehicles and other items of non-lethal military equipment not designated as Significant Military Equipment on the United States Munitions List promulgated pursuant to 22 U.S.C. 2778, may be leased or loaned for temporary use. Specific questions on the applicability of certain items should be referred to the Combatant Command's legal office for review and approval.

11.2.3.3. Repayment of ACSA Obligations

In addition to the use of cash and subject to the agreement of the parties, ACSA obligations may be reconciled by either Replacement-in-Kind or Equal Value Exchange. ACSA obligations not repaid by Replacement-in-Kind or Equal Value Exchange automatically convert to cash obligations after one year.

Replacement in Kind (RIK). RIK allows the party receiving supplies or services under the ACSA to reconcile their obligation via the provision or supplies and services of an identical or substantially identical nature to the ones received. As an example, a country may provide extra water to the United States during a training exercise with the proviso that the United States will provide the same amount of water during a future exercise.

Equal Value Exchange (EVE). EVE enables the party receiving supplies or services under the ACSA to reconcile their obligation via the provision of supplies or services that are considered to by both parties to be of an equal value to those received. As an example, a country may provide extra water to the United States during a training exercise in exchange for the United States providing extra ammunition.

11.2.3.4. ACSA Implementation

DoD Directive 2010.9 and CJCS Instruction 2120.01 provide management guidance on initiating ACSA orders, receiving support, reconciling bills, and maintaining records. As this is a Combatant Command-managed program, organizations interested in acquiring logistics, support, supplies and services should work through the applicable logistics branch to receive further guidance on this topic.

11.2.4. Summary of International Cooperation Guidance and Resources

International cooperation offers the opportunity to achieve cost savings from the earliest phases of Pre-Systems Acquisition throughout the life cycle, while enhancing interoperability with coalition partners. All DoD acquisition personnel, in consultation with the appropriate international programs organizations, should strive to identify and pursue international cooperative programs in accordance with DoD 5000 policy. Specific topics are found in the OSD/IC International Armaments Cooperation Handbook at the OSD/IC website.

11.3. Integrated Program Management

The program manager should obtain integrated cost and schedule performance data at an appropriate level of summarization to monitor program execution. The program manager should require contractors and government activities to use internal management control systems that accomplish the following:

- Relate time-phased budgets to specific tasks identified in the statement of work;
- Produce data that indicate work progress;
- Properly relate cost, schedule, and work accomplishment; and
- Produce data that is valid, timely, and auditable.

Unless waived by the Milestone Decision Authority, the program manager should require that the management control systems used to plan and control contract performance comply with American National Standards Institute/Electronic Industries Alliance Standard 748, *Earned Value Management Systems* (ANSI/EIA-748) (see USD(AT&L) policy memorandum dated March 7, 2005). The program manager should not impose a

specific system or method of management control or require a contractor to change its system, provided it complies with ANSI/EIA-748.

11.3.1. Earned Value Management (EVM)

EVM is a key integrating process in the management and oversight of acquisition programs, to include information technology projects. It is a management approach that has evolved from combining both government management requirements and industry best practices to ensure the total integration of cost, schedule, and work scope aspects of the contract. Unless waived by the MDA, EVM applies to contracts described below. For more information on EVM, refer to the Office of the Secretary of Defense EVM web site, the Defense Contract Management Agency web site, or the EVM Community of Practice web site on the Acquisition Community Connection knowledge sharing system.

11.3.1.1. Earned Value Management (EVM) Applicability

The requirement for EVM applies to cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements that meet the dollar thresholds prescribed in USD(AT&L) policy memorandum dated March 7, 2005. The application thresholds (total contract value including planned options in then-year dollars) are summarized below:

- $20 million or greater – EVM implementation compliant with ANSI/EIA-748 is required. No formal Earned Value Management System (EVMS) validation is required.
- $50 million or greater – EVM implementation compliant with ANSI/EIA-748 is required. An EVMS that has been formally validated and accepted by the cognizant contracting officer is required.

The program manager should implement EVM on applicable contracts within acquisition, upgrade, modification, or materiel maintenance programs, including highly sensitive classified programs, major construction programs, and automated information systems. EVM should be implemented on applicable contracts wherein the following circumstances exist: (1) the prime contractor or one or more subcontractors is a non-U.S. source; (2) contract work is to be performed in government facilities, or (3) the contract is awarded to a specialized organization such as the Defense Advanced Research Projects Agency. In addition, EVM should be implemented on applicable contracts designated as major capital acquisitions in accordance with Office of Management and Budget Circular A-11, Part 7, *Planning, Budgeting, Acquisition, and Management of Capital Assets*.

The application of EVM is not required on contracts, subcontracts, intra-government work agreements, and other agreements valued at less than $20 million (total contract value including planned options). The decision to implement EVM on these contracts is a risk-based decision at the discretion of the program manager. The program manager is required to conduct a cost-benefit analysis before deciding to implement EVM on these contracts. The purpose of the cost-benefit analysis is to explain the rationale for the decision to require cost/schedule visibility into the contract and to substantiate that the benefits to the government outweigh the associated costs. See the DoD Earned Value Management Implementation Guide (EVMIG) for additional guidance on applying EVM

on contracts valued at less than $20 million. If the value of a contract is expected to grow to reach or exceed $20 million, the program manager should consider imposing an EVM requirement on the contract.

The application of EVM is not required on contracts, subcontracts, intra-government work agreements, and other agreements less than 12 months in duration, including options. The decision to implement EVM on these contracts is a risk-based decision at the discretion of the program manager. If the duration of a contract is expected to grow to reach or exceed 12 months, the program manager should consider imposing an EVM requirement on the contract.

The application of EVM on Firm-Fixed Price (FFP) contracts, subcontracts, intra-government work agreements, and other agreements is discouraged regardless of dollar value. If knowledge by both parties requires access to cost/schedule data, the first action is to re-examine the contract type (e.g., fixed price incentive). However, in extraordinary cases where cost/schedule visibility is required and cannot be obtained using other means, the program manager is required to obtain a waiver for individual contracts from the MDA. In these cases, the program manager is required to conduct a business case analysis that includes rationale for why a cost or fixed price incentive contract was not the proper contracting vehicle. When appropriate, the business case analysis should be included in the acquisition approach section of the program acquisition strategy. See the DoD EVMIG for additional guidance on applying EVM on FFP contracts.

If a contract type is mixed, the EVM policy should be applied separately to the different parts (contract types). See the DoD EVMIG for additional guidance on applying EVM on mixed type contracts.

The application of EVM to work efforts that are not discrete in nature (non-schedule based) (i.e., level of effort, time and materials, and services) should be considered on a case-by-case basis. The nature of the work associated with the contract should be used to determine the value of obtaining EVM information and the appropriate EVM methodology to be applied. In cases where the nature of the work does not lend itself to meaningful EVM information, it may be appropriate to waive the EVM requirement. When appropriate, waiver requests should be included in the program acquisition strategy. If the EVM requirement is waived for a contract due to the nature of the work, the program manager should implement an alternative method of management control to provide advanced warning of potential performance problems. Waivers from the EVM policy should be the exception not the rule because they are necessary only in cases where a cost or incentive contract is being used for non-schedule based work, which is typically accomplished using a FFP contract. See the DoD EVMIG for additional guidance on applying EVM on non-schedule based work efforts.

11.3.1.2. Earned Value Management (EVM) Requirements

The program manager should use Defense Federal Acquisition Regulation Supplement (DFARS) clauses 252.242-7005 and 252.242-7006 to place the Earned Value Management System (EVMS) compliance requirement in solicitations and contracts valued at or greater than $20 million but less than $50 million.

The program manager should use DFARS clauses 252.242-7001 and 252.242-7002 to place the EVMS validation requirement in solicitations and contracts valued at or greater than $50 million.

Note: Until there is a final rule on the new DFARS clauses, the existing clauses (252.242-7001 for solicitations and 252.242-7002 for contracts) should be used. For contracts valued at or greater than $50 million, these clauses should be applied directly. For contracts valued at or greater than $20 million but less than $50 million, the following paragraph should be included in the statement of work: *"In regards to DFARS 252.242-7001 and 252.242-7002, the contractor is required to have an Earned Value Management System that complies with ANSI/EIA-748; however, the government will not formally accept the contractor's management system (no compliance review)."* While not required, if a risk-based decision is made to require EVM on cost or incentive contracts valued at less than $20 million or Firm-Fixed Price contracts, the above paragraph should be included in the statement of work.

11.3.1.3. Integrated Baseline Reviews (IBRs)

An IBR is a joint assessment of the Performance Measurement Baseline (PMB) conducted by the government program manager and the contractor. The IBR is not a one-time event. It is a process, and the plan should be continually evaluated as changes to the baseline are made (modifications, restructuring, etc.). IBRs should be used as necessary throughout the life of a project to facilitate and maintain mutual understanding of:

- The scope of the PMB consistent with authorizing documents;
- Management control processes;
- Risks in the PMB associated with cost, schedules, and resources; and
- Corrective actions where necessary.

IBRs should be scheduled as early as practicable and the timing of the IBRs should take into consideration the contract period of performance. The process should be initiated not later than 180 calendar days (6 months) after: (1) contract award, (2) the exercise of significant contract options, and (3) the incorporation of major modifications.

IBRs are also performed at the discretion of the program manager or within a reasonable time after the occurrence of major events in the life of a program. These events may be completion of the preliminary design review, completion of the critical design review, a significant shift in the content and/or time phasing of the PMB, or when a major milestone such as the start of the production option of a development contract is reached. Continuous assessment of the PMB will identify when a new IBR should be conducted.

In accordance with USD(AT&L) policy memorandum dated March 7, 2005, program managers are required to conduct IBRs on all cost or incentive contracts that require the implementation of EVM (contracts valued at or greater than $20 million). However, conducting the IBR is not dependent on the contractor's Earned Value Management System (EVMS) being formally validated as complying with the EVMS guidelines in ANSI/EIA-748. Subcontracts, intra-government work agreements, and other agreements

should also require IBRs as applicable. The scope of the IBRs should be tailored to the nature of the work effort.

See Section 4.3.4.4. for more information on IBRs. See the Program Managers' Guide to the Integrated Baseline Review Process and the DoD Earned Value Management Implementation Guide for additional guidance on IBRs.

11.3.1.4. Contract Performance Management Reporting

The Contract Performance Report (CPR) and the Integrated Master Schedule (IMS) apply to all contracts that meet the EVM applicability requirements in USD(AT&L) policy memorandum dated March 7, 2005. On contracts valued at or greater than $20 million but less than $50 million, it is recommended that CPR and IMS reporting be tailored. See the DoD Earned Value Management Implementation Guide for additional guidance on tailoring reporting.

A common Work Breakdown Structure (WBS) that follows the DoD Work Breakdown Structure Handbook (MIL-HDBK-881A) is required for the Contract Performance Report (CPR), Integrated Master Schedule (IMS), and Contractor Cost Data Report (CCDR). Except for high-cost or high-risk elements, the required level of reporting detail should not normally exceed level three of the contract WBS.

The use of electronic media is required for all reports unless disclosure of this information would compromise national security. All data should be in a readable digital format (e.g., pdf files are not acceptable). The American National Standards Institute (ANSI) X12 standard (839 transaction set), the United Nations Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT) standard (PROCST message), or the XML equivalent are the accepted formats. On-line access to the data may be provided to augment formal submission.

11.3.1.4.1. Contract Performance Report (CPR)

The CPR provides contract cost and schedule performance data that is used to identify problems early in the contract and forecast future contract performance. The CPR should be the primary means of documenting the ongoing communication between the contractor and the program manager to report cost and schedule trends to date and to permit assessment of their effect on future performance.

The program manager should obtain a CPR (DD Form 2734) on all cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $20 million. The CPR is not typically required for cost or incentive contracts valued at less than $20 million, contracts less than 12 months in duration, or Firm-Fixed Price contracts regardless of dollar value. The DoD Earned Value Management Implementation Guide (EVMIG) discusses some circumstances where the CPR may be appropriate for contracts in these categories.

Data Item Description (DID) DI-MGMT-81466A should be used to obtain the CPR. The contracting officer and contractor should negotiate reporting provisions in the contract, including frequency and selection of formats, level of detail, submission dates, variance thresholds and analysis, and the contract WBS to be used. The program manager should tailor the CPR to the minimum data necessary for effective management control,

particularly on contracts valued at less than $50 million. See the DoD EVMIG for additional guidance on tailoring CPR reporting.

In exceptional cases, the contractor may determine that the performance measurement budget or existing contract schedule cannot be achieved and no longer represents a reasonable basis for management control. With government approval, the contractor may implement an Over Target Baseline or Over Target Schedule. For cost-reimbursement contracts, the contract budget base excludes changes for cost growth increases, other than for authorized changes to the contract scope.

11.3.1.4.2. Integrated Master Schedule (IMS)

The IMS is a time-based schedule containing the networked, detailed tasks necessary to ensure successful program/contract execution. The IMS is traceable to the integrated master plan, the contract work breakdown structure, and the statement of work. The IMS is used to verify attainability of contract objectives, to evaluate progress toward meeting program objectives, and to integrate the program schedule activities with all related components.

The program manager should obtain an IMS on all cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $20 million. The IMS is applicable to development, major modification, and low rate initial production efforts; it is not typically applied to full rate production efforts. It is also not normally required for contracts valued at less than $20 million, contracts less than 12 months in duration, or Firm-Fixed Price contracts regardless of dollar value. The DoD Earned Value Management Implementation Guide (EVMIG) discusses some circumstances where the IMS may be appropriate for contracts in these categories.

DID DI-MGMT-81650 should be used to obtain the IMS. The contracting officer and contractor should negotiate reporting provisions in the contract, including level of detail, submission dates, and frequency of the schedule risk analysis. The program manager should tailor the IMS to the minimum data necessary for effective management control, particularly on contracts valued at less than $50 million. See Section 4.5.2. for more information on the IMS. See the DoD EVMIG for additional guidance on tailoring IMS reporting.

11.3.1.5. Earned Value Management System (EVMS) Compliance, Validation, and Surveillance

The Defense Contract Management Agency (DCMA) is DoD's Executive Agent for Earned Value Management. In its role as Executive Agent, DCMA has responsibility for EVMS compliance, validation, and surveillance.

11.3.1.5.1. Earned Value Management System (EVMS) Compliance and Validation

The requirements for EVMS compliance and validation are determined based on the EVM application thresholds in paragraph 11.3.1.1. The requirement for EVMS compliance applies to cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $20 million. The basis for

EVMS compliance is ANSI/EIA-748. The contractor demonstrates EVMS compliance through the use of management processes and program reporting that are consistent with ANSI/EIA-748. The requirement for EVMS validation applies only to those contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $50 million. Validation is achieved by conducting a formal review of the processes defined and used by the contractor to manage major acquisitions that assesses the capability of the contractor's proposed system to comply with the EVMS guidelines in ANSI/EIA-748. It determines that the contractor is using the system as one of its primary program management processes; that the contractor has properly implemented the system on the contract; and that the contractor is using the data from its system in reports to the government. See the DoD Earned Value Management Implementation Guide for additional guidance on EVMS compliance and validation.

11.3.1.5.2. Earned Value Management System (EVMS) Surveillance

Surveillance is required for all contract efforts that require the implementation of EVM compliant with ANSI/EIA-748, regardless of whether a formal system validation is required. Prior to contract award and for the life of the contract, surveillance should be conducted on a recurring basis and should evaluate both the continuing capability of the contractor's EVMS and the validity of the internal and external performance information generated by the system. The results of surveillance efforts should be documented and identified deficiencies should be monitored and corrected. The responsibility and requirement for government surveillance of contracts should be based on the effectiveness of the contractor's implementation of internal management controls. See the DoD Earned Value Management Implementation Guide for additional guidance on surveillance activity.

11.3.2. Other Contract Management Reporting

The reports described in this section apply to many defense contracts. They help to ensure effective program management.

11.3.2.1. Contract Funds Status Report (CFSR)

The CFSR supplies funding data about defense contracts to program managers for:

- Updating and forecasting contract funds requirements;
- Planning and decision making on funding changes in contracts;
- Developing funds requirements and budget estimates in support of approved programs;
- Determining funds in excess of contract needs and available for deobligation;
- Obtaining rough estimates of termination costs; and
- Determining if sufficient funds are available by fiscal year to execute the contract.

The program manager should obtain a CFSR (DD Form 1586) on contracts over 6 months in duration. The CFSR has no specific application thresholds; however, the

program manager should carefully evaluate application to contracts valued at less than $1.5 million (in then-year dollars).

DID DI-MGMT-81468 should be used to obtain the CFSR. The contracting officer and contractor should negotiate reporting provisions in the contract, including level of detail and reporting frequency. The program manager should require only the minimum data necessary for effective management control. The CFSR should not be applied to Firm-Fixed Price contracts unless unusual circumstances dictate specific funding visibility.

11.3.2.2. Contractor Cost Data Reporting (CCDR)

CCDR is the primary means that the Department of Defense uses to collect data on the costs incurred by DoD contractors in performing DoD programs (Acquisition Category ID and IC). DoD Instruction 5000.2 makes CCDR mandatory. This data enables reasonable program cost estimates and satisfies other analytical requirements. The Chair, Cost Analysis Improvement Group (CAIG), ensures consistent and appropriate CCDR application throughout the Department of Defense by defining the format for submission of CCDRs and CCDR system policies, and by monitoring implementation.

CCDR coverage extends from Milestone B or equivalent to the completion of production in accordance with procedures described in this section. Unless waived by the Chair, CAIG, CCDR reporting is required on all major contracts and subcontracts that support Acquisition Category ID and IC programs, regardless of contract type, when the contracts are valued at more than $50 million (FY 2002 constant dollars). CCDR reporting is not required for contracts priced below $7 million. The CCDR requirement on high-risk or high-technical-interest contracts priced between $7 and $50 million is left to the discretion of the Cost Working-Level Integrated Product Team.

Exclusions. CCDR reporting is not required for procurement of commercial systems, or for non-commercial systems bought under competitively awarded, firm fixed-price contracts, as long as competitive conditions continue to exist.

Reporting. For Acquisition Category ID and IC programs, the program manager should use the IPPD process to develop the CCDR plan and forward it to the Chair, CAIG, for approval. CCDR plan approval should occur before issuing industry a solicitation for integration contracts. The CCDR plan reflects the proposed collection of cost data, by Work Breakdown Structure, for a program. The plan describes the report format to be used and the reporting frequency.

A cost-effective reporting system requires tailoring the CCDR plan and appropriately defining the program Work Breakdown Structure.

To support CCDR, each DoD Component designates, by title, an official who accomplishes the following:

- Ensures that policies and procedures are established for implementing CCDR, including CCDR data storage and distribution to appropriate DoD officials.
- Reviews all Acquisition Category I program CCDR plans and CCDR plan changes for compliance with CCDR guidance and the program Work Breakdown Structure, and forwards same to the CAIG.

- Advises the Chair, CAIG, annually, of the status of all CCDR programs, and addresses delinquent or deficient CCDR and its remedial action.

The Defense Cost and Resource Center periodically assesses the need for field reviews of contractor implementation of CCDR for Acquisition Category ID and IC programs. DoD Component Cost Centers assess the need for field reviews of less than Acquisition Category I programs.

The following general guidelines apply to all Acquisition Category ID, IC, II, and III programs. In general, the level of detail and frequency of reporting of Acquisition Category II and III programs is normally less than the level and frequency applied to Acquisition Category I programs:

- Level of Cost Reporting. Routine reporting is at the contract Work Breakdown Structure level three for prime contractors and key subcontractors. Only low-level elements that address high-risk, high-value, or high-technical-interest areas of a program require detailed reporting below level three. The Cost WIPT identifies these lower-level elements early in CCDR planning.
- Frequency. The Cost WIPT defines CCDR frequency for development and production contracts to meet the needs of the program for cost data early in CCDR planning. CCDRs are fundamentally a "returned" (or actual) cost reporting system. Contractors generally do not need to file cost data while work is still pending. Thus, for production contracts, contractors normally submit CCDR reports upon the delivery of each annual lot. For developmental contracts, the contractor typically files CCDR reports after major events such as first flight or completion of prototype lot fabrication, before major milestones, and upon contract completion. In general, quarterly or annual reporting requirements do not meet the above guidance.

11.3.2.3. Software Resources Data Report (SRDR)

SRDR is a recent initiative with a primary purpose to improve the ability of the Department of Defense to estimate the costs of software intensive programs. DoD Instruction 5000.2 requires that data be collected from software development efforts-with a projected value greater than $25 million (FY 2002 dollars)-contained within major automated information systems (Acquisition Category IA) and major defense acquisition programs (Acquisition Category IC and Acquisition Category ID).

Data collected from applicable projects describe the type and size of the software development, and the schedule and labor resources needed for the development. There are three specific data items to be provided:

1. Initial Government Report (DD Form 2630-1), records the government program manager's estimate-at-completion for the project. This report is due 180 days prior to contract award, and is forwarded as part of the Cost Analysis Requirements Description.
2. The Initial Developer Report (DD Form 2630-2), records the initial estimates by the developer (i.e., contractor or government central design activity). This report is due 60 days after contract award.

3. The Final Developer Report (DD Form 2630-3), is used to report actual experience. This item is due within 60 days after final delivery.

For particularly small or large software developments, the program manger may choose to shorten or lengthen the submission deadlines, accordingly. Also, for projects with multiple releases, the program manager may elect to combine the SRDR reporting of incremental releases within a single contract, and provide SRDR data items for the overall project.

Further information is available in an on-line SRDR Manual. This manual provides additional background and technical details about the data collection. In particular, the manual contains information about the process by which each project defines, collects, and submits the data. The manual also contains sample data items, and provides suggested language to include in a request for proposal for this reporting requirement.

11.3.3. Quality Management

According to American National Standards Institute (ANSI), International Organization for Standardization (ISO), and American Society for Quality (ASQ), international standard ANSI/ISO/ASQ Q9000-2000 (ISO 9000), *Quality Management Systems—Fundamentals and Vocabulary*:

- Quality is the degree to which a set of inherent characteristics fulfils requirements. It may apply to a product or process. Inherent characteristics may be physical, sensory, behavioral, temporal, ergonomic, functional, etc.
- Quality management represents the organized activities to direct and control an organization with regard to quality.
- Quality assurance is the part of quality management focused on providing confidence that quality requirements will be fulfilled.

While the DoD program manager should encourage and support the contractor's efforts to assure quality, ultimately, the prime contractor is responsible. Therefore, from a DoD perspective, a key program success factor is selecting contractors that can demonstrate effective quality management. This subject is discussed in Section 11.3.3.1.

The contract should provide incentive to the contractor to deliver products or services that provide value beyond the basic requirement. Without additional incentives, the systems engineering process will normally lead to decisions that satisfy requirements at the lowest cost. It may however be possible to incentivize the contractor to (1) exceed a basic requirement such as mean time between failures or (2) generate a higher level for an important derived requirement (e.g., one that affects operational flexibility, maintainability, supportability, etc.). Section 11.3.3.2 discusses this topic.

Government Contract Quality Assurance (GCQA) determines if contractual requirements have been met prior to acceptance of supplies and services. GCQA is conducted by the program manager and Defense Contract Management Agency (DCMA) as identified in contract administration delegations to DCMA by the Contracting Officer. Section

11.3.3.3 discusses some best practices for setting quality assessment and oversight requirements for the GCQA function, tailored to the expected risks.

11.3.3.1. Differentiating Among Offerors on the Basis of Quality

A contractor's quality management system is used to direct and control the organization with regard to quality. Quality management is an enterprise level process, driven by senior leadership involvement, to support the delivery of high quality products and services by ensuring that all aspects of quality are considered and acted upon by every element of the organization. The fundamental goal is to provide objective insight to assure that: customer requirements are thoroughly analyzed and understood; processes are defined and capable; and the resulting product meets the customer's needs. It interacts with systems engineering technical processes and technical management processes by focusing on both the quality of the system and the quality of the processes being used to create the system. Quality management provides objective insight into processes and work products for all stakeholders including program team members, management, suppliers, customers, and users involved with the development, manufacture, operation, and support of a system.

The quality management process begins **early in the life cycde** and continues throughout. The principal elements of the quality management process include.

- Objectively evaluating performed processes, work products, product/process design and services against the applicable process descriptions, standards, procedures, policies, and documented expectations.
- Understanding the full scope of customer requirements, assessing risks associated with meeting those requirements, and verifying that they are satisfied.
- Identifying and documenting noncompliance issues, especially those affecting cost, schedule, productivity, and performance.
- Using tools and techniques in a disciplined manner to determine root causes of noncompliance issues.
- Addressing noncompliance issues by initiating and tracking corrective and preventative actions to assure the root cause(s) of the defect/deficiency has been identified and removed.
- Providing feedback to program managers, their staff, and corporate managers to identify lessons learned, improve process robustness for future projects, and evaluate trends.

While the quality management focus is on the key aspects of the product realization process (e.g., requirements, design, make/buy decisions, supplier management, production), it also encompasses supporting processes such as contracting and training. Both value-added activities and continuous process improvement should be stressed and encouraged.

Further information about quality management may be found in ISO 10005 Quality Management - Guidelines for Quality Plans and at Process and Product Quality Assurance CMMI-SE/SW/IPPD, v1.1 Continuous Representation and EIA/IS-731.1 FA 2.8 Ensure Quality.

Program managers should allow contractors to define and use their preferred quality management system as long as it meets the needs of the program. International quality standard ISO 9001-2000, *Quality Management Systems - Requirements,* and AS 9100B:2004, *Quality Management Systems - Aerospace Requirements,* define process-based quality management systems and are acceptable for use on contracts per FAR 46.202-4, *Higher-Level Contract Quality Requirements*. AS 9100 contains additional requirements beyond ISO 9001. While it was developed for the aerospace sector, AS 9100 is applicable to and preferable for most complex DoD systems. Program managers should consider the use of additional requirements (such as those contained in the *Missile Defense Agency Assurance Provisions*) beyond ISO 9001 as appropriate.

Other sector specific quality management systems acceptable under FAR 46.202-4 include:

- TL 9000, Quality System Requirements for the telecommunications industry
- ISO/IEC 90003:2004, Software engineering -- Guidelines for the application of ISO 9001:2000 to computer software
- QS-9000 or ISO/TS 16949:2002, ISO 9000 harmonized standards for automotive suppliers of production materials and service parts in North America

To improve a contractor's quality management system, standards bodies encourage registration based upon an impartial third party evaluation. The DoD does not require registration of a contractor's quality management system because registration does not guarantee product or service quality. Reasons why DoD does not require registration include the following:

- Registrars (auditors) do not look at the product;
- There have been instances where a registered contractor delivered a deficient product;
- Many companies pursue registration of their quality management system as a goal in itself or as a marketing tool; and
- Some registrars are less demanding.

Compliance to a standard such as ISO 9001 or AS 9100 does not, in itself, guarantee product or service quality. These standards are management system standards that identify requirements for processes within an organization, describe expected tasks and outcomes, and explain how the processes and tasks integrate to produce required inputs and outputs. Standards are meant to enable the organization to develop a set of processes that, if done by qualified persons using appropriate tools and methods with appropriate leadership involvement, will enable a **capability** for delivering high quality products or services.

Product or service quality is achieved through the implementation of a strategic plan to integrate all business and technical functions that result in the consistent application of proven, capable processes within an organization. Managers must ensure that all management systems are working toward the same goals and are not creating conflicting or dysfunctional behavior. Implementing a standard is of little use if the financial system rewards individuals for delivering non-conforming products/services. Because everything a contractor does should be related to the quality of its products or services, a contractor's quality management system should be the basis for integrating all other management systems within an enterprise. Therefore, look for the following elements of a quality management system in proposals:

- Effective policies and procedures that encourage the use of the system;
- Organizations with defined authorities and responsibilities;
- Objectives to drive people, processes, and the system;
- Method to analyze and resolve quality problems;
- Metrics that reflect desired outcomes;
- Interacting processes to transform inputs into outputs; and
- Records as evidence of what happened.

The following subsections describe several broad areas that have had a significant impact on quality. They provide additional guidance on items the program office and the contracting office should ask for in Requests for Proposals and evaluators should look for in proposals to make a better assessment of a contractor's quality. These items may be used to differentiate among offerors. Depending on the specific situation, there may also be other areas (e.g., competent personnel for special processes) where information should be sought.

11.3.3.1.1. Customer Satisfaction

Customer satisfaction, when quantified, is a valuable enterprise-level outcome metric. DoD has recognized the importance of customer-satisfaction performance measures. Since the passage of the Federal Acquisition Streamlining Act of 1994, all Federal Departments and Agencies have initiated procedures to record contractor performance on in-process contracts and to use past contractor performance information in source selection.

Too often in the past, DoD relied heavily upon detailed technical and management proposals and contractor experience to compare the relative strengths and weaknesses of offers. This practice often allowed offerors that could write outstanding proposals, but had less than stellar performance, to "win" contracts even when other competing offerors had significantly better performance records and, therefore, represented a higher probability of meeting the requirements of the contract. Emphasizing past performance in source selection, can help ensure that the winning teams (prime contractors and major subcontractors) are likely to meet performance expectations. When evaluating past

performance data, consideration should be given to the relevancy, complexity and ultimate mission success of the contract.

Beyond DoD's past performance information, an RFP may ask for further evidence of customer satisfaction such as data tabulated from customer surveys or from complaints and equally important, how changes were made because of the results.

Supplier assessment programs may also be helpful in understanding how well a company is able to satisfy its customers. Suppliers have demonstrated some degree of customer satisfaction when they are accredited by a group of companies, in a particular sector, that joined together to agree on criteria and a process for assessing, exchanging and publishing supplier data to facilitate business relationships. For example, Nadcap is a worldwide cooperative program of major companies designed to manage a cost effective consensus approach to special processes and products and provide continual improvement within the aerospace industry; the Coordinating Agency for Supplier Evaluations (C.A.S.E.) exchanges and publishes non-prejudicial supplier data to help make informed supplier selections. Reports from consumer organizations or the media may also be useful.

11.3.3.1.2. Supply Chain Quality Management

Because quality deficiencies for non commercial-off-the-shelf (COTS) products often occur in the lower tiers, prime contractors should have insight at least two levels down their supply chain. Prime contractors, in addition to having approved vendor (i.e., subcontractor) lists, should ask their subcontractors' about planned suppliers. These subcontractors should also have insight two levels down their supply chain and flow the same requirement down to their suppliers, etc. For COTS products, all contractors should use approved sources.

It is important for DoD program managers to inform their prime contractors of their interest in quality throughout the supply chain. Therefore, through requests for proposals and corresponding proposal evaluation factors, the program office and the contracting office should request and evaluate evidence of effective supply chain management. The evidence should reflect the following characteristics:

- Relationships with suppliers that promote and facilitate communication to improve the effectiveness and efficiency of processes that add value;
- The use of supplier development programs focused on continuous improvement;
- Strategic partnerships with suppliers, over the product life cycle, that are based on a clear understanding of the partners' and customers' needs and expectations in order to improve the joint value proposition of all stakeholders;
- Processes that effectively and efficiently monitor, evaluate, verify, and improve the suppliers' ability to provide the required products with a focus on defect prevention rather than defect detection;

- Right of access for both the prime contractor and the Government to supplier facilities and documentation where applicable; and
- Requirements for the supplier to flow down analogous quality management system provisions to its subcontractors.

11.3.3.1.3. Top Management Involvement

Quality will permeate all levels of a company only if top management provides the leadership necessary to drive and reinforce that behavior. RFPs should also ask for evidence of top management support for quality. The following list identifies important factors in evaluating the effectiveness of top management support:

- Establishing a corporate strategic vision, objectives, policies and procedures that reflect a commitment to quality both inhouse and in suppliers' facilities;
- Communicating, at every opportunity, organizational direction and values regarding quality;
- Providing structures and resources to support full implementation of a quality management system;
- Soliciting quantitative and qualitative feedback on the effectiveness and efficiency of quality management and taking actions based on that feedback, even when change may be difficult;
- Establishing a quality policy, at the highest level in the company, that commits to continuously improving processes and exceeding customer expectations;
- Reviewing the quality management system periodically with particular attention paid to achieving goals and objectives throughout the organization, customer satisfaction, and the exchange of ideas for continuous improvement;
- Setting ambitious quality objectives and promulgating them through quality policy;
- Demonstrating importance put on quality functions by providing for independent reporting channels; and
- Establishing management accountability with emphasis on quality results and customer satisfaction.

11.3.3.1.4. Continual Improvement of Performance

An offeror with effective quality management will seek continual improvement of its processes, product designs, and thereby products by improving its overall performance, efficiency, and effectiveness. Such behavior increases the likelihood of increasing customer satisfaction and enhancing an organization's competitive posture.

More specifically, all processes have defined inputs and outputs as well as the required activities, actions and resources. Therefore, process improvement encompasses both:

1. Improving conformance to the defined process and

2. Improving the defined process itself to add value and eliminate waste.

Such process improvement invariably leads to (work and end) product improvement and consequently increased customer satisfaction.

When asking for evidence of a strong commitment to continual improvement in a request for proposal, the following list provides considerations for evaluating a response.

- How conditions are created to promote innovation;
- How open two-way communications are encouraged;
- How corrective actions are treated as an improvement tool;
- How change is approached on a systematic, consistent basis, to include follow-through implementation, verification and documentation;
- How people are provided with the authority, technical support and necessary resources for change;
- How continuous improvement process tools are deployed company-wide;
- How self assessments, benchmarking, competitor analysis, and other metrics are used to evaluate process performance and drive improvement; and
- How capability and maturity models or reviews support an effective continual improvement process and provide both insights to the improvement process itself and objective evidence of success.

11.3.3.2. Incentivizing Higher Quality in Contracts

Contract incentives can be structured to ensure quality by contributing to the contractor's value proposition. Factors that are typically important aspects of a contractor's value proposition include:

- Customer satisfaction;
- Planning stability;
- Good financial performance; and
- Improved cash flow.

Listed below are examples of contract incentives that can be made available to the prime contractor and the prime contractor can in turn make available to subcontractors under the appropriate conditions:

- Increased fee;
- Extended contract length;
- Follow-on contracts awarded;
- Accelerated progress payments;
- Shared savings; and
- Opportunities for return on investments (some of which may increase the contractor's competitiveness on other contracts).

The following are some potential ways to use these contract incentives to improve quality, and at the same time, improve other product characteristics that are of value to DoD. Their applicability depends on the specific situation.

- Warranties. The program manager could treat the warranty as a fixed price option per item. If there are no failures, the contractor keeps the money that DoD paid for the warranty. To reduce the price of the warranty, the program manager could consider a situation where DoD pays to repair the first failure and the contractor warranties the next "n" failures. Typically the warranty should exclude combat damage, abuse, misuse, and other factors out of the contractors' control.
- Award Fee for Product Support Contracts. The program manager could make the fee a function of operational availability.
- Award Fee for Product Development Contracts. The program manager could make the fee a function of successful operational test and evaluation.
- Progress Payments. The program manager could make payments (or advances on the award fee) contingent on successful corrective actions taken to alleviate quality deficiencies. The program manager could also establish an agreement with the contractor to repay the fee with interest if future measurements do not meet the conditions necessary for the entire amount of the fee to be awarded.
- Share of Savings. The contract could encourage the contractor to invest in facilities, non recurring engineering, technology insertion, etc. that will result in improved performance and reduced costs. The program manager could then use the value engineering clause to repay the investment and give the contractor a share in the savings generated.

In building such relationships, the program manager should avoid actions that encourage risky behavior by the contractor. For example, by insisting on reducing cost, accelerating the schedule, improving performance beyond demonstrated technology limits, etc. the contractor may be forced to forgo quality-related processes. This may not only defeat the purpose of contractual incentives but also negate the other quality activities discussed in this section.

11.3.3.3. Government Contract Quality Assurance (GCQA)

GCQA is a joint responsibility between the program office and Defense Contract Management Agency (DCMA). Interdisciplinary skills (such as quality assurance, industrial specialist, engineering, and software) are needed.

Establish open and effective communication with DCMA. DCMA uses Contract Data Package Recommendation/Deficiency Reports (DD Form 1716) for the following:

- To improve contract data packages;
- When essential information is required as a basis for inspection/acceptance or shipment is incorrect, incomplete, unclear or unavailable; or

- When there is a conflict, ambiguity, noncompliance or other problem area between the contractor and Government concerning contractual requirements.

The DD form 1716 is an important avenue of communication for DCMA to resolve contractual issues with the Procuring Activity and to understand and meet expectations and needs of their customers.

11.3.3.3.1. Formulating the Government Contract Quality Assurance (GCQA) Approach

For defense acquisition programs, the program manager should conduct a customer outcome strategy meeting (i.e., a post award conference) soon after the Systems Development and Demonstration contract award. At this meeting, the participants should:

- Identify desired customer/user expectations and outcomes;
- Determine the program risks that may negatively impact those outcomes;
- Analyze those risks to assess the potential consequences; and
- Define performance measures associated with the desired outcomes.

The program manager should ensure that some of these performance measures relate to key processes in the acquisition framework. For example, the performance measures should be linked to the entrance and exit criteria of the systems engineering technical reviews and the Milestone programmatic reviews during both the Systems Development and Demonstration Phase and the Production and Deployment Phase of the acquisition management framework.

The program manager should form a GCQA team and allow it the flexibility to formulate a risk-based quality assurance surveillance strategy designed to ensure that customer outcomes are achieved. The surveillance strategy should focus on the effectiveness of the contractor's product realization process which includes:

- Planning of Product Realization;
- Customer-Related Processes;
- Design and Development;
- Purchasing and Supplier Management;
- Production and Service Provision;
- Control of Monitoring and Measuring Devices; and
- Inspection, Test, Verification and Validation.

The surveillance strategy should also cover the contractor's continual improvement process. To be effective, this process should be data driven and the data should (1) be used to address both actual and predicted problems, and (2) should be revised to remain connected to process changes. In addition, include both periodic audits of the contractor's quality management system as well as product examinations in the

surveillance strategy. Both independence and the use of criteria in conducting audits and surveillance are critical to providing objective, meaningful insight.

As performance data are collected, the GCQA team should adapt the surveillance strategy based on risks identified and the need for special surveillance of critical safety items, critical characteristics or processes, mission critical items, key characteristics, etc. When planned results are not achieved, the program manager should ensure that preventive and corrective actions are developed and implemented. The GCQA team should extend the surveillance to verify that such actions accomplished their objectives.

11.3.3.3.2. Government Contract Quality Assurance (GCQA) Inspections

For item-managed contracts, detailed guidance on when to require GCQA at source or destination is contained in the FAR, Part 46.

The program manager should use destination inspection for contracts or purchase orders under $250,000 for the reprocurement of items with no significant technical requirements, no critical characteristics, no special features, and no specific acquisition concerns, and where there is confidence in the contractor. Such inspections are limited to kind, count and condition. This may involve preservation, packaging, and marking (if applicable). Put FAR 52.246-1 on the contract. Use FAR 52.246-2 without FAR 52.246-11 only in those rare circumstances where there is reason to believe that there may be a problem.

Typically, source inspection is appropriate for complex / critical items where:

- The verification of technical characteristics requires in-process controls;
- Product quality cannot be adequately determined through basic end item product examination; or
- The contractor is experiencing or exhibiting difficulty controlling product characteristics.

The program manager should put both FAR 52.246-2 and FAR 52.246-11 on the contract. FAR 52.246-2 allows Government access to the facility and requires the contractor to develop and maintain an inspection system. FAR 52.246-11 requires the contractor to implement a higher level quality management system.

The responsible technical authority should prepare a Quality Assurance Letter of Instruction through the contracting officer to ensure that appropriate product specifications, drawings, and inspection and test instructions, including critical characteristics, are available and/or identified for use by the Defense Contract Management Agency. GCQA at the source encompasses one or more of the following based on defined risk:

- Product Examinations. Examinations of product characteristics to ensure they meet contract requirements. Depending on the identified risks, the Government CQA surveillance strategy might include various product examination techniques, such as inspecting, testing, witnessing, verifying by use of objective evidence, and analyzing Government or contractor performance data.
- Process Reviews. Reviews to determine the suitability, adequacy, and effectiveness of the process to achieve product outputs that meet contract requirements.
- System Assessments/Audits. Systematic, independent assessments and audits of the various elements of the contractual quality management system impacting process or product quality.
- Management and program reviews and meetings: Maintains open channels of communication.

11.3.3.3.3. Government Contract Quality Assurance (GCQA) for Critical Safety Items (CSIs)

Special attention must be paid to CSIs regardless of whether they are item-managed or program-managed. DFARS 246.103 states that the activity responsible for technical requirements may prepare instructions covering the type and extent of Government inspections for acquisitions that have critical applications (e.g., safety) or have unusual requirements. Section 4.4.21 discusses CSIs as a systems engineering design consideration. It provides a definition and links to some additional reference material.

The contracting officer should clearly mark the front page of the solicitation/contract with the words "Critical Safety Item." This raises the alertness level and makes everyone aware that CSIs are involved in the contract. When CSIs are determined after contract award, the responsible technical authority should use the words "Critical Safety Items" in the subject line of a Quality Assurance Letter of Instruction (QALI). All critical and major characteristics, the extent of inspection required, and the associated acceptance criteria should be described either in the contract or in the QALI. In addition, the technical authority should provide criteria for special inspections, process verification, or similar requirements. Acceptance criteria should also include additional instructions for situations where a CSI is purchased from a distributor, a CSI is purchased on a commercial contract, or CSI critical characteristics cannot be fully examined at a prime contractor's facility. To assure the communications loop is closed with Defense Contract Management Agency (DCMA), the QALI should request acknowledgement and DCMA acceptance of duties included within. The form should be returned to the responsible technical authority that transmitted the QALI.

Public Law 108-136, "National Defense Authorization Act for FY04," Section 802, Quality Control in the Procurement of Aviation Critical Safety Items and Related Services, "… requires that the head of the design control activity for aviation critical safety items establish processes to identify and manage the procurement, modification, repair, and overhaul of aviation critical safety items." DoD procedures for managing aviation CSIs are contained in Joint Service instruction, "Management of Aviation

Critical Safety Items," and the Joint Aeronautical Logistics Commanders' Aviation Critical Safety Items (CSIs) Handbook. Additionally, per DFARS 246.407, the head of the design control activity is the approval authority for acceptance of any nonconforming aviation critical safety items or nonconforming modification, repair, or overhaul of such items.

DCMA relies on the Procuring Activity's knowledge and involvement to determine whether an item is correctly categorized as a critical item. If DCMA questions the critical categorization of an item, the lack of a critical characterization of an item, or a CSI designation, DCMA will contact the Procuring Office to discuss the reasons behind the decision, gain a better understanding of the situation or customers needs, and request additional information. The Procuring Office should contact DCMA personnel whenever they have a concern, question, or possess additional information important to achieving customer outcomes.

11.4. Risk Management

The program manager and others in the acquisition process should take an active role in identifying and understanding program uncertainties, whether they have a negative or positive impact on the program baseline. An assessment of cost, schedule, or performance against a program baseline is not credible or realistic if uncertainties are not recognized and in some manner incorporated into estimates and assessments in a transparent manner.

The impact of uncertainty in particular areas of the program, on particular estimates and assessments, should be analyzed and understood.

To obtain additional information related to Risk Management such as: various risk management processes, assessment techniques, handling methods, and monitoring tools, go to the Risk Management Community of Practice at the Acquisition Community Connection; or go to the Risk Management Guide for DoD Acquisition, Fifth Edition (Version 2.0) Defense Acquisition University.

11.5. Knowledge-Based Acquisition

Knowledge-based acquisition is a management approach which requires adequate knowledge at critical junctures (i.e., knowledge points) throughout the acquisition process to make informed decisions. DoD Directive 5000.1 calls for sufficient knowledge to reduce the risk associated with program initiation, system demonstration, and full-rate production. DoD Instruction 5000.2 provides a partial listing of the types of knowledge, based on demonstrated accomplishments, that enable accurate assessments of technology and design maturity and production readiness.

Implicit in this approach is the need to conduct the activities that capture relevant, product development knowledge. And that might mean additional time and dollars. However, knowledge provides the decision maker with higher degrees of certainty, and enables the program manager to deliver timely, affordable, quality products.

The following knowledge points and ensuing considerations coincide with decisions along the acquisition framework:

Program Initiation. Knowledge should indicate a match between the needed capability and available resources before a program starts. In this sense, *resources* is defined broadly, to include technology, time, and funding.

Considering the knowledge associated with technology, the knowledge should be based on demonstrated accomplishments. By requiring proven technology before a program starts, we reduce uncertainty. Rather than addressing technology development and product development, the program manager and Milestone Decision Authority can focus on product development, because they *know* the technology is available. DoD Instruction 5000.2 enforces this concept with the following policy:

> *Technology developed in S&T or procured from industry or other sources shall have been demonstrated in a relevant environment or, preferably, in an operational environment to be considered mature enough to use for product development in systems integration. Technology readiness assessments, and where necessary, independent assessments, shall be conducted. If technology is not mature, the DoD Component shall use alternative technology that is mature and that can meet the user's needs.*

Design Readiness Review. Knowledge should indicate that the product can be built consistent with cost, schedule, and performance parameters. This means design stability and the expectation of developing one or more workable prototypes or engineering development models. DoD Instruction 5000.2 lists the specific factors that contribute to such knowledge.

Production Commitment. Based on the demonstrated performance and reliability of prototypes or engineering development models, knowledge prior to the production commitment should indicate the product is producible and meets performance criteria. DoD Instruction 5000.2 lists some of the specific factors that contribute to such knowledge.

Full-Rate Production Decision. Based on the results of testing initial production articles and refining manufacturing processes and support activities, knowledge prior to committing to full-rate production should indicate the product is operationally capable; lethal and survivable; reliable; supportable; and producible within cost, schedule, and quality targets.

11.6. Implementing a Performance-Based Business Environment (PBBE)

A Performance-Based Business Environment relates the business considerations of the acquisition strategy to the Life-cycle considerations of Systems Engineering, Life-Cycle Logistics, and Human Systems Integration. The following considerations apply:

- As part of acquisition reform, the Military Departments and Defense Agencies reviewed all military specifications and standards, canceling unnecessary documents, replacing many with non-government standards, and rewriting others to state requirements in performance terms. In cases where they defined military-unique requirements that could not be restated in performance terms without jeopardizing safety, reliability, or performance, the military specifications and standards were retained.

- Today, the Department of Defense relies on more than 30,000 federal and industry standards, to include performance specifications, international standardization agreements, non-government standards, and commercial item descriptions, as well as defense specifications and standards. In October 2002, the Defense Standardization Executive approved a Joint Materiel Standards Roadmap, developed in response to a June 6, 2001, tasking from the Under Secretary of Defense (Acquisition, Technology, and Logistics). The roadmap defines a course of action to ensure that materiel standards used by the Department of Defense, both commercial and government, continue to support the warfighters' operational requirements for joint Service and coalition interoperability and dramatically reduce the logistics footprint, as articulated in the Force-centered Logistics Enterprise. The objective of the roadmap is to reduce the number of endorsed standards to those required to support these objectives and enable the development of an automated tool to assist Program Managers.
- Because of our success in transforming military specifications and standards and the way that we apply them on contracts, it is no longer required to obtain a waiver from the Milestone Decision Authority to cite military specifications or standards in solicitations and contracts. Elimination of the waiver requirement should not be perceived as a return to the “old way of doing business,” where military specifications and standards were often routinely applied to contracts. Every program office should assess requirements and apply only those specifications and standards necessary to define essential needs and manage risk. Program Executive Officers, Program Managers, and others in the acquisition and technical communities should ensure appropriate use of specifications and standards in their programs.
- The Department of Defense will normally use performance specifications (i.e., DoD performance specifications, commercial item descriptions, and performance-based non-Government standards) when purchasing new systems, major modifications, upgrades to current systems, and commercial items for programs in all acquisition categories. The Department of Defense additionally will normally emphasize conversion to performance specifications for the re-procurement of existing systems where supported by a business case analysis; for programs in all acquisition categories.
- If performance specifications are not practicable, or if stating requirements in performance terms is not practicable because of essential interface or interoperability requirements, the Department of Defense may state its needs using prescriptive requirements (i.e. dimensions, materials, etc.).
- The most recent version of MIL-STD-882, DoD Standard Practice for System Safety, listed in the ASSIST database, should be used to manage a program's Environment, Safety, and Occupational Health (ESOH) risks.
- Military specifications and standards contained in contracts and product configuration technical data packages for re-procurement of items already in inventory should:

- Be streamlined to remove non-value-added management, process, and oversight specifications and standards;
- When justified as economically beneficial over the remaining product life cycle by a business case analysis, be converted to performance-based acquisition and form, fit, function, and interface specifications to support programs in on-going procurement, future re-procurement, and post-production support.

- The Director, Naval Nuclear Propulsion, determines the specifications and standards for naval nuclear propulsion plants in accordance with 42 U.S.C. 7158 and E.O. 12344.
- DoD Instruction 4120.24 and DoD 4120.24-M contain additional standardization guidance.

The program manager should structure a PBBE to accomplish the following:

- Convey product definition to industry in performance terms;
- Use systems engineering and management practices, including affordability, Integrated Product and Process Development, and support, to fully integrate total Life-cycle considerations;
- Emphasize past performance;
- Motivate process efficiency and effectiveness up and down the entire supplier base-primes, subcontractors and vendors-through the use of contractor-chosen commercial products, practices, and processes;
- Encourage Life-cycle risk management versus risk avoidance;
- Simplify acquisition;
- Transfer acquisition tasks to industry where cost effective, risk-acceptable, and where commercial capabilities exist; and
- Use performance specifications or convert to performance specifications during reprocurement of systems, subsystems, components, spares, and services beyond the initial production contract award; and during post-production support to facilitate technology insertion and modernization of operational weapons systems.

Systems that benefit from a PBBE include highly interoperable systems, high-tech/high-cost systems, high return on investment systems, systems requiring a high degree of logistics readiness and/or technology insertion opportunity, and/or systems with a high total ownership cost and/or a long predicted life.

11.7. Total Life Cycle Systems Management (TLCSM)

The TLCSM approach to major systems decision making is a way to account for some of the total ownership categories that are difficult to address. The TLCSM approach, which is principally a Program Manager responsibility, requires programs to base major decisions on system-wide analyses and the Lifecycle consequences of those decisions on system performance and affordability. Examples of these analyses are the business cases

and cost estimates that support the acquisition (i.e., affordability assessments, analyses of alternatives, cost-performance trades, and iterative establishment of program cost goals). The refined, detailed, and discrete Lifecycle cost estimates used within the program office should support internal, program office decision making such as the evaluation of engineering changes or in competitive source selections.

11.8. Integrated Product and Process Development (IPPD)

IPPD is the DoD management technique that simultaneously integrates all essential acquisition activities through the use of multidisciplinary teams to optimize design, manufacturing, and supportability processes. One of the key IPPD tenets is multidisciplinary teamwork through Integrated Product Teams.

IPPD facilitates meeting cost and performance objectives from product concept through production, including field support. The 10 tenets of IPPD can be summarized into the following 5 principles:

- Customer Focus
- Concurrent Development of Products and Processes
- Early and Continuous Life-Cycle Planning
- Proactive Identification and Management of Risk
- Maximum Flexibility for Optimization and Use of Contractor Approaches

11.9. Technical Representatives at Contractor Facilities

Program managers should maximize the use of Defense Contract Management Agency (DCMA) personnel at contractor facilities. Program managers and DCMA Contract Management Offices should jointly develop and approve program support plans for all Acquisition Category I program contracts to ensure agreement on contract oversight needs and perspectives.

The program manager should only assign technical representatives to a contractor's facility as necessary, and as agreed to by the Director, DCMA. A Memorandum of Agreement should specify the duties of the technical representative and establish coordination and communication activities. Technical representatives shall not perform contract administration duties as outlined in Federal Acquisition Regulation (FAR) Section 42.302(a).

11.10. Contractor Councils

DCMA supports the formation of management, sector, and/or corporate councils by each prime contractor under DCMA cognizance that provide Acquisition Category I, Acquisition Category IA, or Acquisition Category II program support. These councils provide an interface with the Contract Management Office Commander; the Defense Contract Audit Agency Resident Auditor; representatives from all affected acquisition management activities (including program managers, Item Managers, and Standard Procurement System Component Team Leaders), or designated representatives for any of the above listed individuals. Acquisition managers or designees should support both

council activities and council-sponsored Working-Level Integrated Product Teams. Acquisition managers should assist the councils and keep all the stakeholders informed about issues affecting multiple acquisition programs, work issues quickly, and elevate unresolved issues to appropriate levels for resolution. These councils may identify and propose acquisition process streamlining improvements. Acquisition managers should assist and encourage councils to coordinate and integrate program audit and review activity, support and promote civil-military integration initiatives, and accept contractor Standard Procurement System proposals and other ideas that reduce total ownership cost while meeting performance-based specifications.

The program office staff should interface with contractors' councils, keeping in mind that such councils are not Federal Advisory Committees under FACA. The staff may find that these councils strengthen the corporate relationship with the Department of Defense, provide an interface between company representatives and acquisition managers, communicate acquisition reform initiatives, or even resolve issues. In leading corporate endeavors, such as Standard Procurement System proposals, civil-military integration ideas, or other initiatives designed to achieve efficiencies for the company, these councils may ultimately produce savings for the Government.

11.11. Government Property in the Possession of Contractors (GPPC)

All program managers who own or use GPPC should emphasize reducing GPPC and prevent unnecessary additions of GPPC. The program manager should assign GPPC management authority within the program office, and identify needed actions, reviews, and reports. The management of all GPPC, special tooling, and special test equipment, and decisions about retention, disposition, and delivery requirements should be well informed and timely. Government property left with the contractor but not needed for performance of the contract should be stored under a funded storage agreement. GPPC no longer needed for current contract performance or future needs should be promptly disposed of or reutilized in accordance with applicable laws and regulations. The program manager should document decisions regarding GPPC in the contract file.

GPPC includes Government property that is not "owned" by the program manager, but is "used" on the program. Government property may only be furnished to contractors under the criteria, restriction, and documentation requirements addressed in FAR 45.3.

11.12. Integrated Digital Environment (IDE)

DoD policy requires the maximum use of digital operations throughout the system life cycle. The program IDE is part of the larger DoD IDE. It should keep pace with evolving automation technologies and provide ready access to anyone with a need-to-know, as determined by the program manager.

Program managers should establish a data management system within the IDE that allows every activity involved with the program to cost-effectively create, store, access, manipulate, and exchange digital data. This includes, at minimum, the data management needs of the system engineering process, modeling and simulation activities, test and evaluation strategy, support strategy, and other periodic reporting requirements.

Industry partners have been strongly encouraged to develop and implement IDE solutions that best meet the needs of their preferred business model. The program IDE should take maximum advantage of and have minimum impact on existing industry solutions. Solicitations should require IDE proposals to support system life cycle activities. Unless analysis verifies prohibitive cost or time delays, or a potential compromise of national security, new contracts should require the contractor to provide on-line access to programmatic and technical data. Contracts should give preference to on-line access (versus data exchange) through a contractor information service or existing IT infrastructure. While contracts should minimally specify the required functionality and data standards, the data formats of independent standards-setting organizations should take precedence. The issue of data formats and transaction sets should be independent of the method of access or delivery.

The program manager should use existing infrastructure (e.g., Internet or wireless LANs) when practicable.

The program manager should address the status and effectiveness of the IDE at milestone reviews and at other appropriate decision points and/or program reviews.

11.13. Simulation-Based Acquisition (SBA) and Modeling and Simulation (M&S)

SBA is the robust and interactive use of M&S throughout the product life cycle. The program manager should employ SBA and M&S during system design, test and evaluation, and modification and upgrade. The program manager should collaborate with operational users and consider industry inputs during SBA/M&S program planning. Planning should include the application, support, documentation, and reuse of M&S; and the integration of SBA/M&S across functional disciplines.

The following additional considerations are useful during SBA/M&S planning activities:

- Plan for SBA/M&S and make necessary investments early in the acquisition life cycle.
- Use verified, validated, and accredited models and simulations, and ensure credible applicability for each proposed use.
- Use data from system testing during development to validate the use of M&S.
- Use SBA/M&S to supports efficient test planning, pre-test results prediction, and the validation of system interoperability; and supplement design qualification, actual T&E, manufacturing, and operational support;
- Involve the OTA in SBA/M&S planning to support both developmental test and operational test objectives.
- Have DIA review and validate threat-related elements.

11.14. Independent Expert Review of Software-Intensive Programs

The program manager for an Acquisition Category ID or IC program that requires software development to achieve the needed capability should convene an independent expert program review after Milestone B and prior to the system Critical Design Review.

The program manager, or other acquisition official in the program chain of command up to the CAE, should also consider independent expert program reviews for Acquisition Category IA, II, and III programs. The independent expert review team should report review findings directly to the program manager.