Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
Incorporating Change 4, August 31, 2018

USD(A&S)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive (DoDD) 5000.01 (Reference (a)) and DoDD 5134.01 (Reference (cm)), reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through (cw).

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

c. Assigns, reinforces, and prescribes procedures for acquisition responsibilities related to cybersecurity in the Defense Acquisition System.

d. Incorporates and cancels Directive-type Memorandum 17-001 (Reference (cl)).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

4. RESPONSIBILITIES

a. Defense Acquisition Executive (DAE). The DAE is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DAE will act as the MDA for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. In accordance with Table 1 in Enclosure 1 of this instruction, the DAE may delegate authority to act as the MDA to the head of a DoD Component, who may further delegate the authority to the Component Acquisition Executive (CAE). The DAE may also delegate MDA authority to another OSD official as the DAE considers appropriate.

b. MDA. The MDA will establish procedures for assigned programs using this instruction as guidance. MDAs should limit mandatory procedures applicable to all assigned programs so as to not exceed the requirements for MDAPs or MAIS programs and other acquisition programs governed by this instruction or DoD Directive 5000.01 (Reference (a)). MDAs should tailor regulatory procedures in the document consistent with sound business practice and the risks associated with the product being acquired.

c. Heads of the DoD Components. The DoD Component Head will implement the procedures in this instruction and Reference (a). Component-required procedures will not exceed those specified in this instruction. When necessary, waivers or requests for exceptions to the provisions of this instruction will be submitted to the DAE, the DoD Chief Information Officer (DoD CIO), the Director, Operational Test and Evaluation (DOT&E), or the Director, Cost Assessment and Program Evaluation (DCAPE), via the CAE. Statutory requirements cannot be waived unless the statute permits.

d. Secretaries of the Military Departments. In addition to the responsibilities described in paragraph 4.c., the Secretary of the Military Department acquiring an MDAP will represent the customer (i.e., the DoD Component(s) fielding the system). The Secretary concerned, in coordination with the Chief of the Military Service fielding the system, will balance resources against priorities and ensure appropriate trade-offs are made among cost, schedule, technical feasibility, and performance throughout the life of the program.

e. Chiefs of the Military Services. The Chiefs of the Military Services fielding MDAPs will represent the customer and, with the Secretary of the Military Department acquiring the MDAP, balance resources against priorities and ensure that appropriate trade-offs are made among cost, schedule, technical feasibility, and performance throughout the life of the program. The Chief concerned will advise the MDA on trade-offs before Milestones A and B. As part of the MDA's Written Determination before Milestone A and Certification and Determination before Milestone B (these milestone information requirements are detailed in Table 2 in Enclosure 1), the MDA must determine that the Chief and the Secretary concur with the cost, schedule, technical feasibility, and performance trade-offs that have been made.

5. PROCEDURES

a. Overview

(1) Program Categories. The statutes governing defense acquisition programs are complex, and the categories into which a program falls will impact acquisition procedures. The designation of a program as an MDAP, a MAIS program, or a Major Weapons System; and the determination that the program is an Information System, a Defense Business System, or responds to an urgent need affect program procedures and policies.

(2) Program Structure. The structure of a DoD acquisition program and the procedures used should be tailored as much as possible to the characteristics of the product being acquired, and to the totality of circumstances associated with the program including operational urgency and risk factors.

(a) MDAs will tailor program strategies and oversight, including program information, acquisition phase content, the timing and scope of decision reviews and decision levels, based on the specifics of the product being acquired, including complexity, risk factors, and required timelines to satisfy validated capability requirements.

(b) When there is a strong threat-based or operationally driven need to field a capability solution in the shortest time, MDAs are authorized to implement streamlined procedures designed to accelerate acquisition system responsiveness. Statutory requirements will be complied with, unless waived in accordance with relevant provisions.

(c) In accordance with Section 806 of Public Law 114-92 (Reference (d)), the Secretary of Defense may waive acquisition law or regulation to acquire a capability that would not otherwise be available to the DoD Components. This waiver authority may not be delegated. Detailed provisions and requirements for this waiver are identified in Table 6 in Enclosure 1 of this instruction.

(3) Program Acquisition Categories (ACATs) and Types. All defense acquisition programs are designated by an ACAT (i.e., ACAT I through III) and type (e.g., MDAP, MAIS, or Major System). MDAPs are either estimated to achieve the statutorily defined MDAP cost threshold, or are designated as an MDAP by the DAE. Similarly, MAIS programs are either estimated to achieve the statutorily defined MAIS program cost threshold, or are designated a MAIS program by the DAE. MAIS programs are software intensive and typically have a lower investment level than MDAPs. A MAIS program that is estimated to attain the MDAP cost thresholds may be designated by the DAE as either an MDAP or a MAIS program. MDAP and MAIS program designations carry the greatest consequences in terms of management level, reporting requirements, and documentation and analysis to support program decisions. Enclosure 1 of this instruction identifies the information requirements associated with all standard program categories or types in tabular form. Table 1 in Enclosure 1 provides specific definitions, funding thresholds, and decision authorities. Some information systems are also designated as a National Security System or a Defense Business System. These designations are defined in statute and have procedural and policy consequences. Enclosure 11 addresses

Information Technology, and DoDI 5000.75 (Reference (cw)) describes Defense Business Systems.

(4) Program Decision Reviews and Milestones. The purpose of the decision reviews embedded in the acquisition procedures described in this section is to carefully assess a program's readiness to proceed to the next acquisition phase and to make a sound investment decision committing the Department's financial resources. Consequently, reviews will be issue and data focused to facilitate an examination of relevant questions affecting the decisions under consideration and to allow the MDA to judge whether the program is ready to proceed. The following policies will guide decision reviews:

(a) The MDA is the sole and final decision authority. Staff members and staff organizations support and facilitate the MDA's execution of that authority.

(b) The Defense Acquisition Board (DAB) will advise the DAE on critical acquisition decisions when the DAE is the MDA. The DAE or designee will chair the DAB. An Acquisition Decision Memorandum (ADM) will document decisions resulting from reviews. Similar procedures will be established at the Component level for use by other MDAs.

(c) Program Managers, under the supervision of Program Executive Officers (PEOs) and CAEs, are expected to design acquisition programs, prepare programs for decisions, and execute approved program plans.

(d) Overarching Integrated Product Teams (OIPTs) at the OSD level, and similar organizations within the DoD Components are expected to collectively assist the MDA in making sound investment decisions for the department, and to ensure programs are structured and resourced to succeed. These organizations are not decision bodies and they and their leaders do not supplant the authority of the Program Manager, PEO, CAE, or DAE.

(e) Issues should be resolved at the lowest level possible. When an issue cannot be resolved quickly at a lower level, the issue will be submitted to the MDA with complete and objective data necessary to support a decision.

(f) The documents prepared in support of the decision process (e.g., Acquisition Strategy, Systems Engineering Plan (SEP), Test and Evaluation Master Plan (TEMP), Life-Cycle Sustainment Plan (LCSP)) should generally not be prepared solely for staff review and approval, but be intended primarily for use within the program as planning and management tools that are highly specific to the program and tailored to meet program needs.

(g) DAB review preparation will be streamlined and efficient. Staff members will be provided with the data needed to support the review in accordance with scheduled submission dates established throughout this instruction. They will work to minimize the overhead burden placed on the DoD Components, PEOs, program managers, and their staffs. Staff reviews will focus on the substance of the program's content: affordability, requirements reasonableness, technical risk reduction, contracting strategy, schedule realism, testing provisions, funding adequacy, and future decision criteria. Reviewers will inform the DAB chairperson and MDA,

the OIPT leader, and the Military Service concerned of potential DAB issues. The MDA will prioritize key cost, schedule and performance issues to be addressed at the DAB. The Military Service concerned will address administrative or advisory comments. Similar procedures will be used for DoD Component-level reviews.

b. Relationship Between Defense Acquisition, Requirements, and Budgeting Processes

(1) Acquisition, requirements, and budgeting, are closely related and must operate simultaneously with full cooperation and in close coordination. Validated "Capability Requirements" provide the basis for defining the products that will be acquired through the acquisition system and the budgeting process determines Department priorities and resource allocations and provides the funds necessary to execute planned programs. Throughout a product's life cycle, adjustments may have to be made to keep the three processes aligned. Capability requirements may have to be adjusted to conform to technical and fiscal reality. Acquisition programs may have to adjust to changing requirements and funding availability. Budgeted funds may have to be adjusted to make programs executable or to adapt to evolving validated capability requirements and priorities. Stable capability requirements and funding are important to successful program execution. Those responsible for the three processes at the DoD level and within the DoD Components must work closely together to adapt to changing circumstances as needed, and to identify and resolve issues as early as possible.

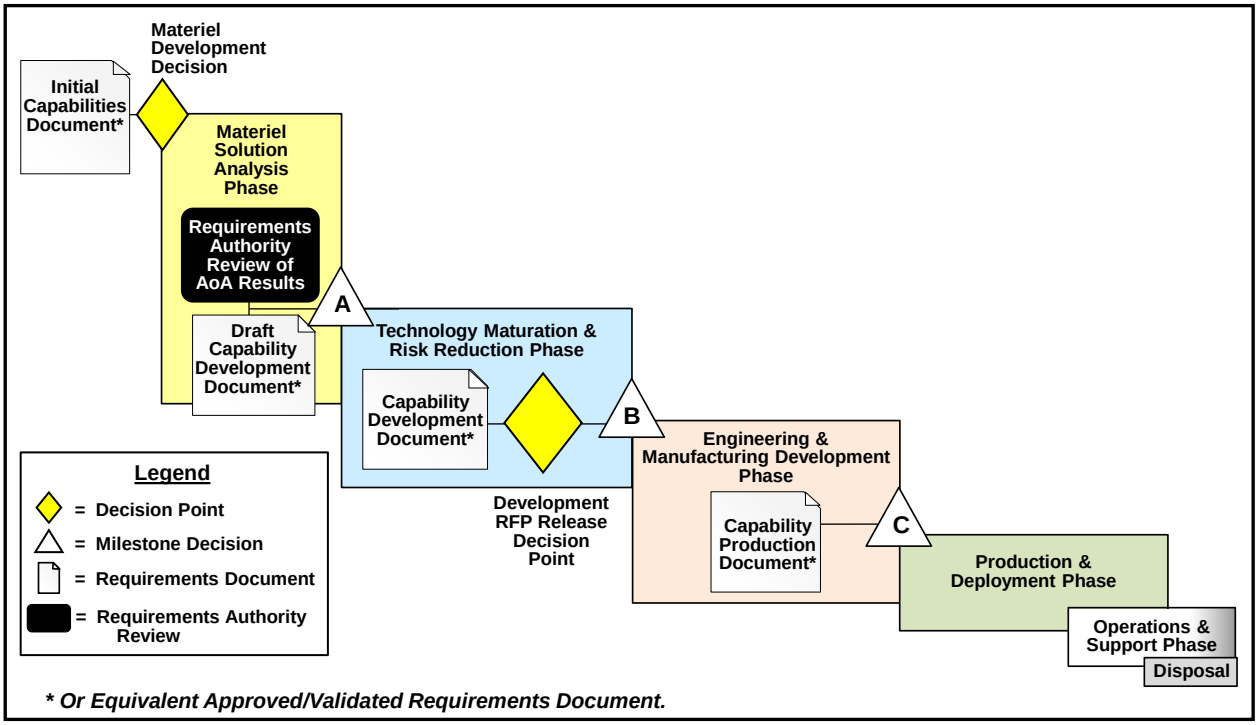
(2) Capability Requirements Process

(a) All acquisition programs respond to validated capability requirements. Figure 1 illustrates the interaction between the requirements process and the acquisition process. The Chairman of the Joint Chiefs of Staff, with the advice of the Joint Requirements Oversight Council (JROC), will assess and validate joint military requirements for MDAP and MAIS programs, and less-than-MDAP or MAIS programs designated either as "JROC Interest" or "Joint Capabilities Board Interest." When JROC validation authority is delegated in accordance with the Joint Capabilities Integration and Development System (JCIDS) process in Chairman of the Joint Chiefs of Staff Instruction 3170.01I (Reference (e)), the DoD Components will use variations of the JCIDS to validate their requirements. The validation authority for Defense Business System capability requirements is described in Reference (cw).

(b) Leadership of the acquisition and budget processes will be involved as advisors to the validation authority during consideration of initial or adjusted validation of capability requirements to ensure coordination across the three processes.

(c) The titles of capability requirements documents supported by JCIDS vary by the maturity of the capability gap to solution proposal and can vary by product classification. When the titles vary from the most typical Initial Capabilities Document (ICD), Capability Development Document (CDD), or Capability Production Document, the text will use the generic terms, "validated capability requirements document" or "equivalent requirements document."

Figure 1. Illustration of the Interaction Between the Capability Requirements Process and the Acquisition Process



(d) Capability requirements are not expected to be static during the product life cycle. As knowledge and circumstances change, consideration of adjustments or changes may be requested by acquisition, budgeting, or requirements officials. Configuration Steering Boards (CSBs), as described in paragraph 5d(5)(b) in this section, will also be used to periodically review program progress and identify opportunities for adjustment.

(3) Budgeting Process. The DoD budgeting process is based on the annual budget preparation cycle managed by the DCAPE and the Under Secretary of Defense (Comptroller) for the Deputy Secretary of Defense. This process produces a Future Years Defense Program (FYDP) that covers 5 years of spending. While individual program decisions fall under the DAE or designated MDA, DoD budget decisions are made separately at the Secretary or Deputy Secretary level, with the advice of the DAE and others. Within the DoD Components, MDAs will advise the Component budget authorities to ensure that acquisition programs are adequately funded and that program plans are consistent with programmed funding levels.

c. Generic and DoD-Specific Acquisition Program Models, Decision Points, and Phase Activities

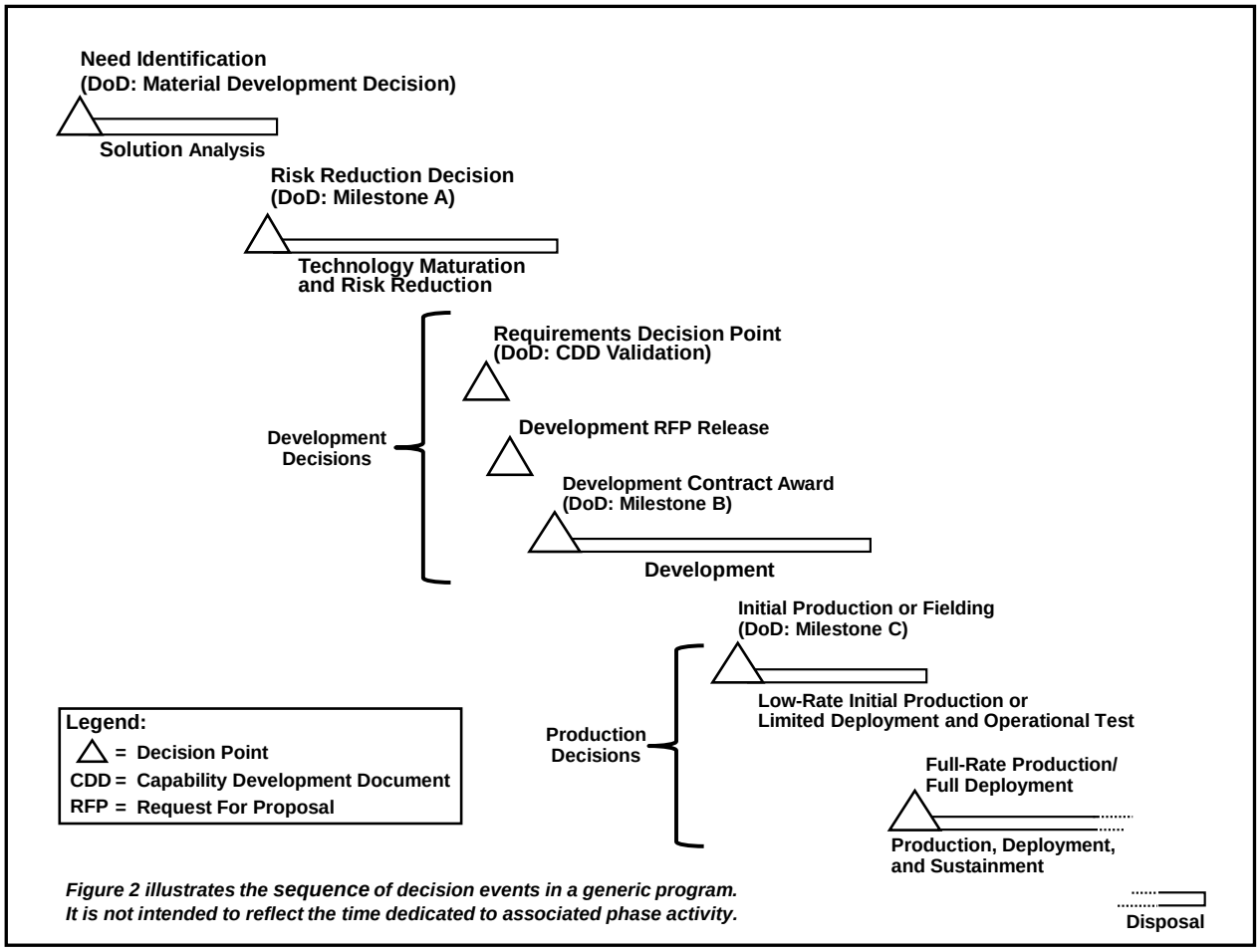
(1) This section is structured in increasing layers of detail and complexity, beginning with a very generic description of acquisition phases and decision points that could apply to almost any product life cycle, DoD or otherwise, followed by more specific commonly used DoD program models, and concluding with a description of the procedures used in most DoD

acquisition programs prior to any tailoring. DoD acquisition managers and staff should focus on the basics of sound acquisition planning, management, and decision making as discussed in this section as their primary responsibility—while also assuring compliance, as appropriate, with the specific requirements found in the tables that follow in Enclosures 1 and 13, and the direction in other applicable enclosures.

(2) Generic Acquisition Program Structure and Decision Points

(a) Generic Acquisition Program Structure. For reference, a generic product acquisition program would follow the structure depicted in Figure 2. Figure 2 illustrates the sequence of decision events in a generic program, which could be a Defense program or, except for the unique DoD terminology, a commercial product.

Figure 2. Generic Acquisition Phases and Decision Points



(b) Generic Acquisition Milestones and Decision Points

1. Need Identification, called the Materiel Development Decision by DoD, is the decision that a new product is needed and that activities to analyze alternative solutions will occur.

2. Risk Reduction Decision, called Milestone A by DoD, is an investment decision to pursue specific product or design concepts, and to commit the resources required to mature technology and/or reduce any risks that must be mitigated prior to decisions committing the resources needed for development leading to production and fielding.

3. The decision to commit resources to the development of a product for manufacturing and fielding, called Engineering and Manufacturing Development (EMD) by DoD, follows completion of any needed technology maturation and risk reduction. DoD breaks this commitment into three related decisions: (1) a requirements decision point (called the CDD Validation Decision by DoD); (2) a decision to release a solicitation for development to industry, called the Development Request for Proposals (RFP) Release Decision Point; and (3) a decision to award the contract(s) for development, called Milestone B by DoD. Formally, the development contract award authorized at DoD's Milestone B is the critical decision point in an acquisition program because it commits the organization's resources to a specific product, budget profile, choice of suppliers, contract terms, schedule, and sequence of events leading to production and fielding. In practice however, almost all of these decisions have to be made prior to the release of the RFP to industry in order to inform the bidders' proposals. For DoD, the Development RFP Release Decision Point is the point at which plans for the program must be most carefully reviewed to ensure all risks are understood and under control, the program plan is sound, and that the program will be affordable and executable.

a. Requirements Decision Point (CDD Validation Decision for DoD). The point at which the major cost and performance trades have been completed and enough risk reduction has been completed to support a decision to commit to the set of requirements that will be used for preliminary design activities, development, and production (subject to reconsideration and refinement as knowledge increases).

b. Development RFP Release Decision. The point at which planning for development is complete and a decision can be made to release an RFP for development (and possibly initial production) to industry.

c. Development Decision, called Milestone B by DoD. The development decision commits the resources (authorizes proceeding to award of the contract(s)) needed to conduct development leading to production and fielding of the product.

4. The decision to enter production follows development and testing. For DoD, the production decision is normally broken into two DoD decisions: (1) Low-Rate Initial Production (LRIP), called Milestone C by DoD, or Limited Deployment; and (2) the Full-Rate Production or Full Deployment Decision.

a. The Initial Production Decision. The production decision, based primarily on developmental testing results and usually also informed by an operational assessment, commits the resources (i.e., authorizes proceeding to award the contract(s)) required to enter production and begin deployment of the product. Evidence from testing that the product design is stable is the critical consideration for this decision. The commitment to enter production is very expensive and difficult to reverse.

b. Full Rate Production or Full Deployment Decision. The decision, following completion of operational testing of representative initial production products, to scale up production and/or deployment.

5. While these generic decision points and milestones are standard, MDAs have full latitude to tailor programs in the most effective and efficient structure possible, to include eliminating phases and combining or eliminating milestones and decision points, unless constrained by statute. Paragraph 5d provides more detail about the standard structure, milestones, and decision points as they apply to most defense acquisition programs. Enclosure 1 includes tables of specific requirements for the various statutory and regulatory categories of programs. Enclosures 11 and 13 provide additional information about Information Technology programs (described in Enclosure 11) and Urgent Capability Acquisitions (described in Enclosure 12); cybersecurity is described in Enclosure 13. Defense Business Systems are described in Reference (cw).

(3) Defense Acquisition Program Models

(a) Paragraphs 5c(3)(b) through 5c(3)(e) describe four basic models that serve as examples of defense program structures tailored to the type of product being acquired or to the need for accelerated acquisition. Two additional hybrid models combine the features of multiple basic models. Each basic model is tailored to the dominant characteristics of the product being acquired (e.g., hardware intensive products such as most weapons systems). The hybrids are described because many products will require combining models, such as a weapons systems development that includes significant software development. Acquisition programs should use these models as a starting point in structuring a program to acquire a specific product.

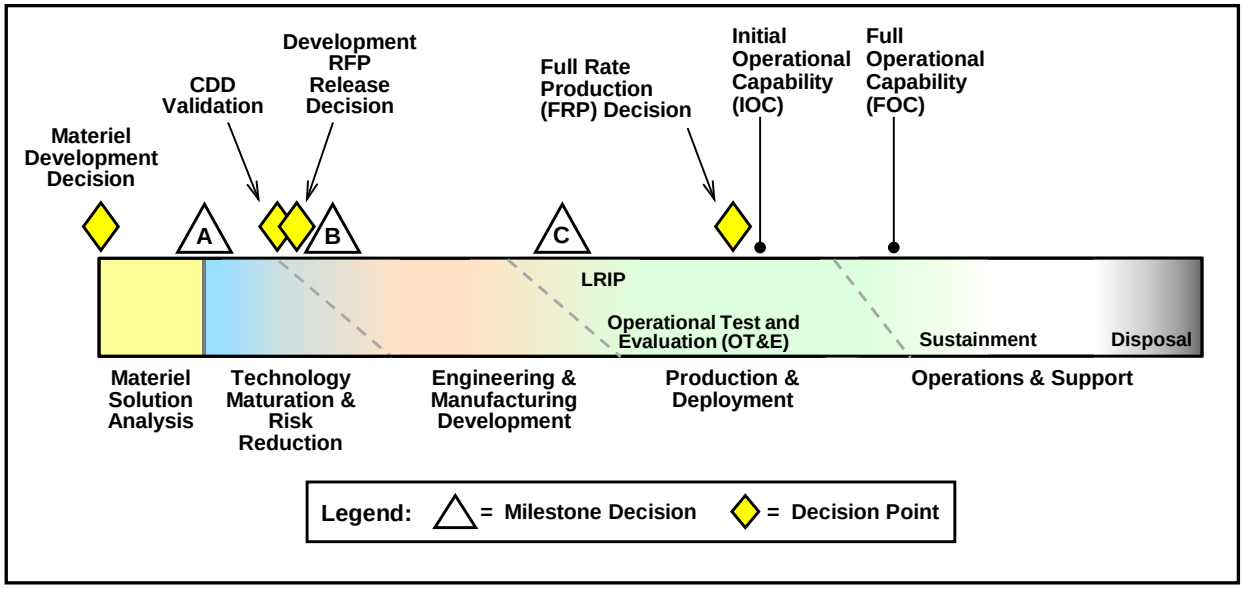
1. The models provide baseline approaches. A specific program should be tailored to the unique character of the product being acquired.

2. All of the models contain requirements and product definition analysis, risk reduction, development, testing, production, deployment, and sustainment phases punctuated by major investment decisions at logical programmatic and contractual decision points. Progress through the acquisition management system as depicted in any of these models or in a tailored variation depends on obtaining sufficient knowledge about the capability to be provided and risks and costs remaining in the program to support a sound business decision to proceed to the next phase.

3. Figures and brief descriptions are provided for each model. The figures illustrate the typical sequence of events and activities. A dotted diagonal line and color blending imply overlapping activities.

(b) Model 1: Hardware Intensive Program. Figure 3 is a model of a hardware intensive development program such as a major weapons platform. This is the classic model that has existed in some form in all previous editions of this instruction. It is the starting point for most military weapon systems; however, these products almost always contain software development resulting in some form of Hybrid Model A (paragraph 5c(3)(f)1 describes Hybrid Model A).

Figure 3. Model 1: Hardware Intensive Program



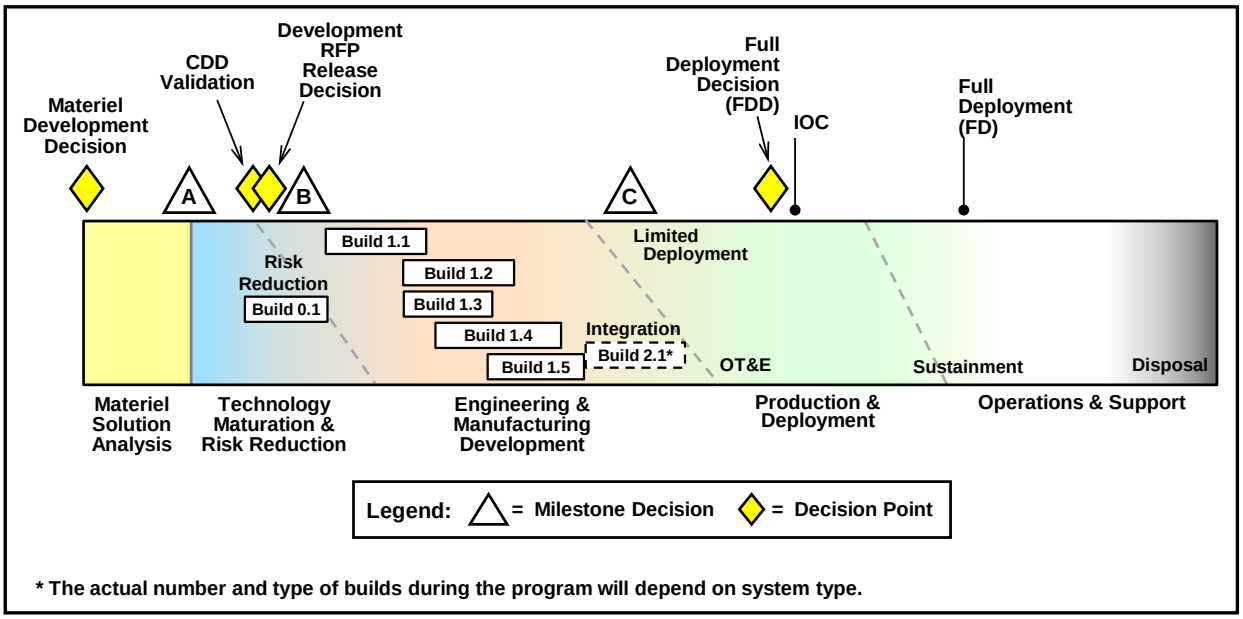
(c) Model 2: Defense Unique Software Intensive Program. Figure 4 is a model of a program that is dominated by the need to develop a complex, usually defense unique, software program that will not be fully deployed until several software builds have been completed. The central feature of this model is the planned software builds – a series of testable, integrated subsets of the overall capability – which together with clearly defined decision criteria, ensure adequate progress is being made before fully committing to subsequent builds.

1. Examples of this type of product include military unique command and control systems and significant upgrades to the combat systems found on major weapons systems such as surface combatants and tactical aircraft.

2. Several software builds are typically necessary to achieve a deployable capability. Each build has allocated requirements, resources, and scheduled testing to align dependencies with subsequent builds and to produce testable functionality to ensure that progress is being achieved. The build sequencing should be logically structured to flow the workforce

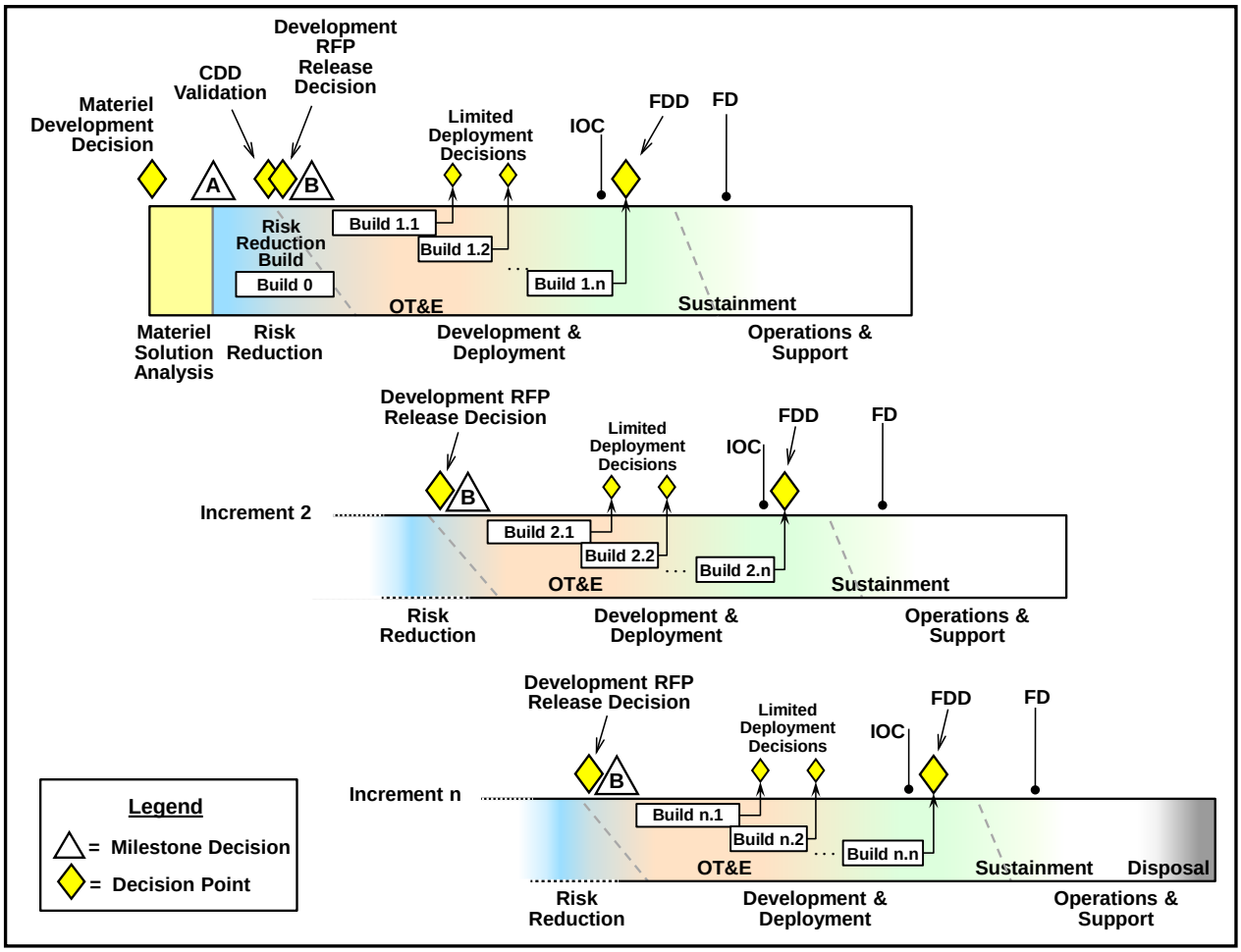
from effort to effort smoothly and efficiently, while reducing overall cost and schedule risk for the program.

Figure 4. Model 2: Defense Unique Software Intensive Program



(d) Model 3: Incrementally Deployed Software Intensive Program. Figure 5 is a model that has been adopted for many Defense Business Systems. It also applies to upgrades to some command and control systems or weapons systems software where deployment of the full capability will occur in multiple increments as new capability is developed and delivered, nominally in 1- to 2-year cycles. The period of each increment should not be arbitrarily constrained. The length of each increment and the number of deployable increments should be tailored and based on the logical progression of development and deployment for use in the field for the specific product being acquired.

Figure 5. Model 3: Incrementally Deployed Software Intensive Program



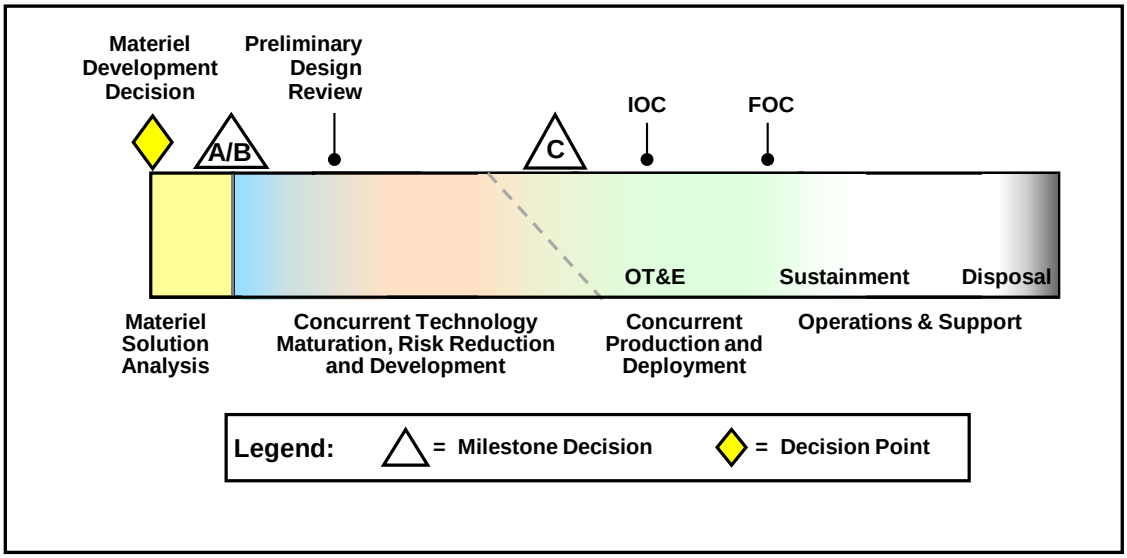
1. This model is distinguished from the previous model by the rapid delivery of capability through multiple acquisition increments, each of which provides part of the overall required program capability. Each increment may have several limited deployments; each deployment will result from a specific build and provide the user with a mature and tested sub-element of the overall incremental capability. Several builds and deployments will typically be necessary to satisfy approved requirements for an increment of capability. The identification and development of technical solutions necessary for follow-on capability increments have some

degree of concurrency, allowing subsequent increments to be initiated and executed more rapidly.

2. This model will apply in cases where commercial off-the-shelf software, such as commercial business systems with multiple modular capabilities, are acquired and adapted for DoD applications. An important caution in using this model is that it can be structured so that the program is overwhelmed with frequent milestone or deployment decision points and associated approval reviews. To avoid this, multiple activities or build phases may be approved at any given milestone or decision point, subject to adequate planning, well-defined exit criteria, and demonstrated progress. An early decision to select the content for each follow-on increment (2 through N) will permit initiation of activity associated with those increments. Several increments will typically be necessary to achieve the required capability.

(e) Model 4: Accelerated Acquisition Program. Figure 6 is a model that applies when schedule considerations dominate over cost and technical risk considerations. This model compresses or eliminates phases of the process and accepts the potential for inefficiencies in order to achieve a deployed capability on a compressed schedule. The model shows one example of tailoring for accelerated acquisition and many others are possible. This type of structure is used when technological surprise by a potential adversary necessitates a higher-risk acquisition program. Procedures applicable to urgent needs that can be fulfilled in less than 2 years are a subset of this model and are discussed in Enclosure 12.

Figure 6. Model 4: Accelerated Acquisition Program

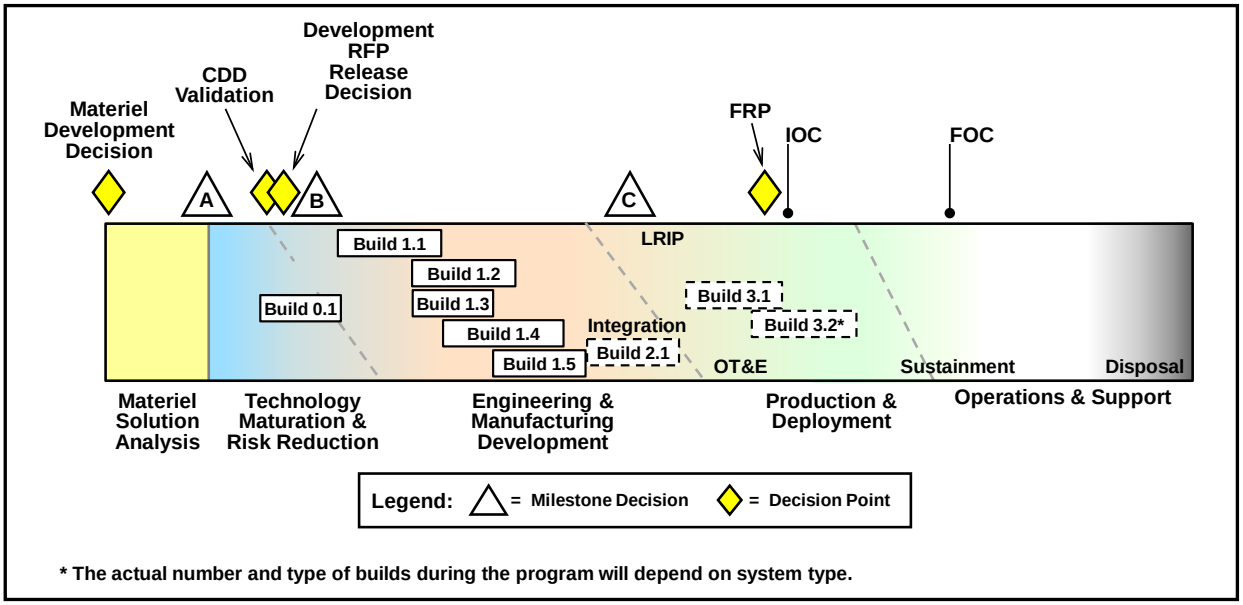


(f) Models 5 and 6: Hybrid Acquisition Programs

1. Figure 7 is a model depicting how a major weapons system combines hardware development as the basic structure with a software intensive development that is occurring simultaneously with the hardware development program. In a hardware intensive

development, the design, fabrication, and testing of physical prototypes may determine overall schedule, decision points, and milestones, but software development will often dictate the pace of program execution and must be tightly integrated and coordinated with hardware development decision points.

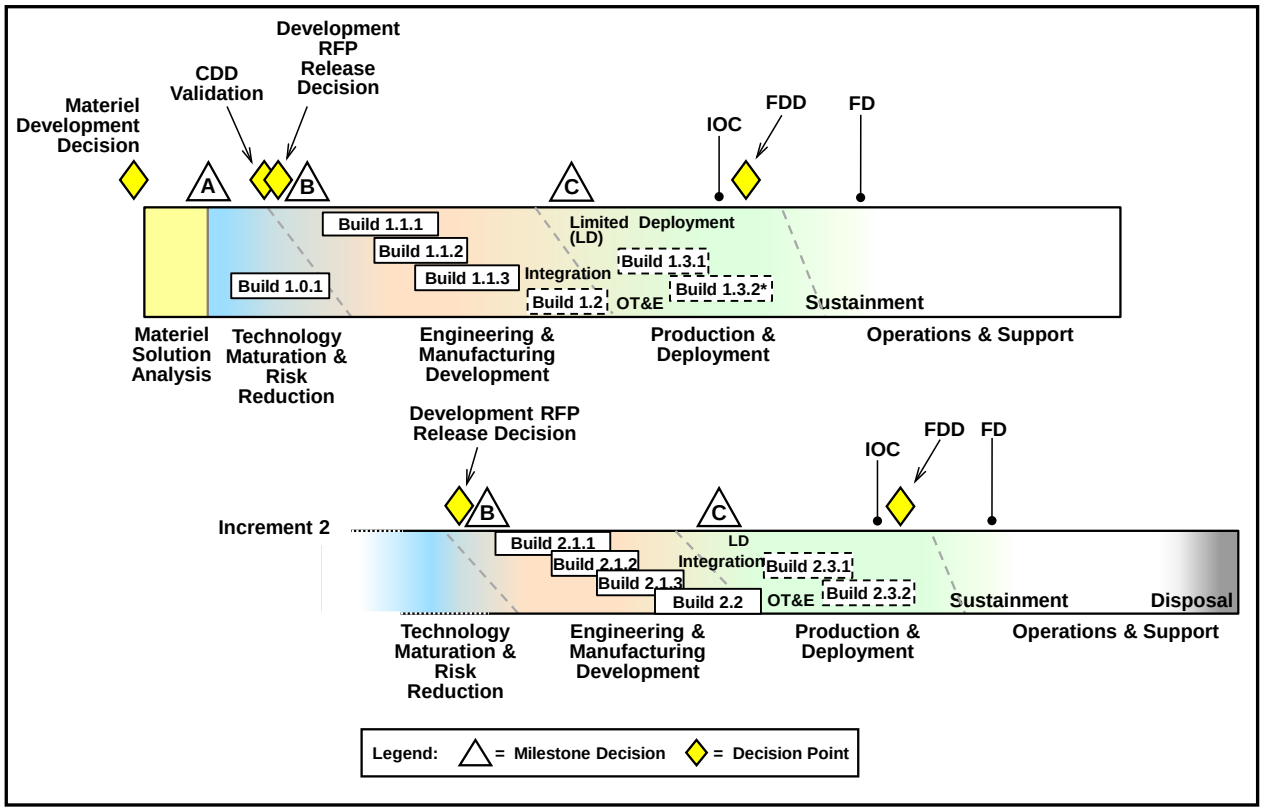
Figure 7. Model 5: Hybrid Program A (Hardware Dominant)



2. In the hybrid "A" model, software development should be organized into a series of testable software builds, as depicted in Figure 7. These builds should lead up to the full capability needed to satisfy program requirements and Initial Operational Capability (IOC). Software builds should be structured so that the timing of content delivery is synchronized with the need for integration, developmental and operational testing in hardware prototypes. The Milestone B decision to enter EMD and the Milestone C decision to enter Production and Deployment (P&D) should include software functional capability development maturity criteria as well as demonstrated technical performance exit criteria.

3. Figure 8, Model 6: Hybrid Model B (Software Dominant), depicts how a software intensive product development can include a mix of incrementally deployed software products or releases that include intermediate software builds. All of the comments about incremental software fielding associated with Model 3 in paragraph 5c(3)(d) apply to this model as well. This is a complex model to plan and execute successfully, but depending on the product it may be the most logical way to structure the acquisition program.

Figure 8. Model 6: Hybrid Program B (Software Dominant)



(g) Risk Management in Hybrid Models. Highly integrated complex software and hardware development poses special risks to program cost and schedule performance. Technical, cost, and schedule risks associated with hardware and software development must be managed throughout the program's life cycle and will be a topic of special interest at all decision points and milestones.

d. Acquisition Process Decision Points and Phase Content. The procedures in subparagraphs 5d(1) through 5d(14) are general and are applicable to the acquisition program models previously described and to variations in them. Tailoring is always appropriate when it will produce a more efficient and effective acquisition approach for the specific product. Non-MDAP and non-MAIS programs will use analogous DoD Component processes. Additional or modified procedures applicable to Information Technology and to Defense Business System programs are described in Enclosure 11 of this instruction and in Reference (cw), respectively, and procedures applicable to urgent needs are described in Enclosure 12.

(1) Materiel Development Decision

(a) The Materiel Development Decision is based on a validated initial requirements document (an ICD or equivalent requirements document) and the completion of the Analysis of Alternatives (AoA) Study Guidance and the AoA Study Plan. This decision directs execution of the AoA, and authorizes the DoD Component to conduct the Materiel Solution Analysis Phase. This decision point is the entry point into the acquisition process for all defense acquisition products; however, an "acquisition program" is not formally initiated (with the accompanying statutory requirements) until Milestone B, or at Milestone C for those programs that enter directly at Milestone C. DoD Components may have conducted enough analysis to support preliminary conclusions about the desired product at this point. If so, that analysis may be used by the MDA to narrow the range of alternatives. If not, requirements are likely to be less well-defined or firm, and a wider range of alternatives will need to be considered.

(b) At the Materiel Development Decision, the DCAPE, (or DoD Component equivalent) will present the AoA Study Guidance, and the AoA lead organization will present the AoA Study Plan. In addition, the Component will provide the plan to staff and fund the actions that will precede the next decision point (usually Milestone A) including, where appropriate, competitive concept definition studies by industry.

(c) If the Materiel Development Decision is approved, the MDA will designate the lead DoD Component; determine the acquisition phase of entry; and identify the initial review milestone, usually, but not always, a specific milestone as described in one of the program models. MDA decisions will be documented in an ADM. The approved AoA Study Guidance and AoA Study Plan will be attached to the ADM.

(2) Materiel Solution Analysis Phase

(a) Purpose. The purpose of this phase is to conduct the analysis and other activities needed to choose the concept for the product that will be acquired, to begin translating validated capability gaps into system-specific requirements including the Key Performance Parameters (KPPs) and Key System Attributes (KSAs), and to conduct planning to support a decision on the acquisition strategy for the product. AoA solutions, key trades among cost, schedule, and performance, affordability analysis, risk analysis, and planning for risk mitigation are key activities in this phase.

(b) Phase Description

1. Minimum funding required for this phase is normally that needed to analyze and select an alternative for materiel development, and to complete the activities necessary to support a decision to proceed to the next phase; technology development and concept analysis and design efforts may also be funded in this phase.

2. The validated ICD and the AoA Study Plan will guide the AoA and Materiel Solution Analysis Phase activity. The analysis will be conducted in accordance with the

procedures in Enclosure 9 of this instruction, and focus on identification and analysis of alternatives; measures of effectiveness; key trades between cost and capability; total life-cycle cost, including sustainment; schedule; concepts of operations; and overall risk. The AoA will inform and be informed by affordability analysis, cost analysis, sustainment considerations, early systems engineering analyses, threat projections, and market research.

3. Prior to the completion of this phase, the DoD Component combat developer will prepare a Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP) that will include the operational tasks, events, durations, frequency, operating conditions and environment in which the recommended materiel solution is to perform each mission and each phase of a mission. The CONOPS/OMS/MP will be provided to the Program Manager and will inform development of the plans for the next phase including: acquisition strategy, test planning, and capability requirements trades. It will be provided to industry as an attachment for the next acquisition phase RFP.

4. This phase ends when a DoD Component has completed the necessary analysis and the activities necessary to support a decision to proceed to the next decision point and desired phase in the acquisition process. The next phase can be Technology Maturation and Risk Reduction (TMRR), EMD, or P&D, depending on the actions needed to mature the product being acquired. Each of these phases has associated decision points to authorize entry: Milestone A, Development RFP Release and Milestone B, or Milestone C. Each decision point and phase has information requirements identified in Table 2 in Enclosure 1 of this instruction, and other criteria as defined in paragraphs 5d(3) through 5d(14) in this instruction.

(c) Program Office Establishment and Next Phase Preparation. During the Materiel Solution Analysis Phase, the CAE will select a Program Manager and establish a Program Office to complete the necessary actions associated with planning the acquisition program with emphasis on the next phase. The Program Manager will review the information requirements for the upcoming decision event and may submit a request for waiver to statutory (when authorized by statute) and regulatory requirements to the to the cognizant approval authority (e.g., MDA, DoD CIO, DOT&E, DCAPE, JROC). The MDA will conduct a DAB planning meeting approximately 6 months before a DAB that includes RFP release decisions. The purpose of the meeting will be to ensure timely review of the business approach and other key elements of program planning before completion of the RFPs. An approved Acquisition Strategy will inform development of the final RFPs for the next phase of the program.

(3) Milestone A

(a) The Milestone A decision approves program entry into the TMRR Phase and release of final RFPs for TMRR activities. The responsible DoD Component may decide to perform technology maturation and risk reduction work in-house and/or award contracts associated with the conduct of this phase. Competitive prototypes are part of this phase unless specifically waived by the MDA. Key considerations are:

1. The justification for the preferred materiel solution.

2. The affordability and feasibility of the planned materiel solution.

3. The scope of the capability requirements trade space and understanding of the priorities within that trade space.

4. The understanding of the technical, cost, and schedule risks of acquiring the materiel solution, and the adequacy of the plans and programmed funding to mitigate those risks prior to Milestone B.

5. The efficiency and effectiveness of the proposed acquisition strategy (including the contracting strategy and the intellectual property (IP) strategy) in light of the program risks and risk mitigation strategies.

6. The projected threat and its impact on the materiel solution.

(b) At the Milestone A Review:

1. The Program Manager will present the approach for acquiring the preferred materiel solution including: the Acquisition Strategy, the business approach, framing assumptions, an assessment of program risk and how specific technology development and other risk mitigation activities will reduce the risk to acceptable levels, and appropriate "Should Cost" management targets. Table 2 of Enclosure 1 lists program information requirements and identifies approval authorities for those requirements. Program Manager requests to tailor or waive information requirements associated with the next decision event may be submitted to the MDA at this milestone and at each subsequent program milestone. When the MDA is the approval authority for an information requirement, the MDA may approve the Program Manager's request to tailor or waive that requirement. When another official is the approval authority for an information requirement, the MDA may endorse, but cannot approve, a Program Manager's request to tailor or waive that requirement. An ADM will document decisions by the MDA or other approval officials to tailor or waive information requirement.

2. The DoD Component will:

a. Present an affordability analysis and proposed affordability goals based on the resources that are projected to be available to the DoD Component in the portfolio(s) or mission area(s) associated with the program under consideration. The analysis will be supported by a quantitative assessment of all of the programs in the prospective program's portfolio or mission area that demonstrates the ability of the Component's estimated budgets to fund the new program over its planned life cycle. Affordability analyses are not intended to produce rigid, long-range plans; their purpose is to inform current decisions about the reasonableness of embarking on long-term capital investments at specific capability levels. The affordability analysis will support the Component's proposed affordability goals for unit production and sustainment costs for MDA approval and inclusion in the Milestone A ADM. Enclosure 8 details the policy for affordability analyses and constraints.

b. Submit a DoD Component cost estimate and DoD Component cost position for the preferred solution(s) identified by the AoA. Enclosure 10 covers cost estimating in greater detail.

c. Demonstrate that the program will be fully funded within the FYDP at Milestone A.

3. If Milestone A is approved, the MDA will make a determination on the materiel solution, the plan for the TMRR Phase, any Program Manager information requirement waiver requests, release of the final RFP, and specific exit criteria required to complete TMRR and enter EMD. The MDA will document these decisions in an ADM.

(c) If substantive changes to the plan approved at Milestone A are required as a result of the source selection process, the DoD Component will notify the MDA who may, at his or her discretion, conduct an additional review prior to contract awards.

(4) TMRR Phase

(a) Purpose. The purpose of this phase is to reduce technology, engineering, integration, and life-cycle cost risk to the point that a decision to contract for EMD can be made with confidence in successful program execution for development, production, and sustainment.

(b) Phase Description

1. This phase should include a mix of activities intended to reduce the specific risks associated with the product to be developed. This includes additional design trades and requirements trades necessary to ensure an affordable product and executable development and production programs. Capability requirements are matured and validated, and affordability caps are finalized during this phase. The TMRR Phase requires continuous and close collaboration between the program office and the requirements communities and authorities. During this phase, any realized Should Cost management savings should normally be used to further reduce program risk and future program costs. Enclosure 2 describes baseline cost control and the use of Should Cost management.

2. This phase normally includes competitive sources conducting technology maturation and risk reduction activities and preliminary design activities up to and including a Preliminary Design Review (PDR) prior to source selection for the EMD Phase. Competitive risk reduction prototypes will be included if they will materially reduce engineering and manufacturing development risk at an acceptable cost. If competitive prototyping is not considered feasible, single prototypes at the system or subsystem level will be considered.

3. There are a number of ways to structure this phase which should be tailored to reduce the specific risks associated with the product being acquired. Technology Readiness Levels, described in the Technology Readiness Assessment (TRA) Guidance (Reference(f)), should be used to benchmark technology risk during this phase; however, these indices are rough benchmarks, and not conclusive about the degree of risk mitigation needed prior to development.

Deeper analysis of the actual risks associated with the preferred design and any recommended risk mitigation must be conducted and provided to the MDA.

(c) The Acquisition Strategy will guide this phase. Multiple technology development demonstrations, defined in the acquisition strategy, may be necessary before the operational user and materiel developer can substantiate that a preferred solution is feasible, affordable, and supportable; satisfies validated capability requirements; and has acceptable technical risk. Critical program information will be identified during this phase and program protection measures to prevent disclosure of critical information will be implemented consistent with section 13 in Enclosure 3. Planning for EMD, production, developmental and operational test, and life-cycle sustainment of proposed products will occur during this phase. The government will update the program IP Strategy (see paragraph 6a(4) of Enclosure 2) to ensure the ability to compete future sustainment efforts consistent with the Acquisition Strategy to include competition for spares and depot repair.

(d) During this phase, and timed to support CDD validation (or its equivalent), the Program Manager will conduct a systems engineering trade-off analysis showing how cost and capability vary as a function of the major design parameters. The analysis will support the assessment of refined KPPs/KSAs in the CDD. Capability requirements proposed in the CDD (or equivalent requirements document) should be consistent with program affordability goals.

(e) Subsequent to CDD validation, the Program Manager will conduct additional requirements analysis including: requirements decomposition and allocation, definition of internal and external interfaces, and design activities leading to a PDR. Unless waived by the MDA, the PDR will occur prior to Milestone B.

(f) Program Planning. During the TMRR Phase, the Program Manager will plan the balance of the program and prepare for subsequent decision points and phases. The Program Manager will submit an updated Acquisition Strategy for MDA approval in sufficient time to inform development of the RFP for the next phase. The updated Acquisition Strategy will describe the overall approach to acquiring the capability to include the program schedule, risks, funding, and the business strategy. The business strategy will describe the rationale for the contracting approach and how competition will be maintained throughout the program life cycle, and detail how contract incentives will be employed to support the Department's goals.

(g) Life-Cycle Considerations During the TMRR Phase

1. Planning for the sustainment phase should begin in this phase, when requirements trades and early design decisions are still occurring. The Program Manager will finalize sustainment requirements and decompose them into more detailed requirements to support the PDR and for the following uses:

a. Support system and product support package design trades.

b. Support test and evaluation (T&E) planning.

c. Provide performance metrics definition for product support contracts and organic support requirements.

d. Provide logistics requirements, workload estimates, and logistics risk assessment.

2. The Program Manager will integrate the product support design into the overall design process, and assess enablers that improve supportability, such as diagnostics and prognostics, for inclusion in the system performance specification. As the design matures, the Program Manager will ensure that life-cycle affordability is a factor in engineering and sustainment trades.

(5) CDD Validation and CSBs

(a) CDD Validation

1. During the TMRR Phase, the requirements validation authority will validate the CDD (or equivalent requirements document) for the program. This action will precede the Development RFP Release Decision Point and provides a basis for preliminary design activities and the PDR that will occur prior to Milestone B unless waived by the MDA. Active engagement between acquisition leadership, including the MDA and the requirements leadership, including the validation authority (the JROC for MDAP and MAIS programs), during the development and review of proposed requirements trades is essential to ensuring that the validated requirements associated with the program continue to address the priorities of the DoD Component and the joint force in a cost effective and affordable way. The MDA (and CAE when the MDA is the DAE) will participate in the validation authorities' review and staffing of the CDD (or equivalent requirements document) prior to validation, to ensure that requirements are technically achievable, affordable, and testable, and that requirements trades are fully informed by systems engineering trade-off analyses completed by the Program Manager or the DoD Component.

2. The KPPs and KSAs included in the validated CDD, will guide the efforts leading up to PDR, and inform the Development RFP Release Decision Point. As conditions warrant, changes to KPPs and KSAs may be proposed to the applicable capability requirements validation authority. All non-KPP requirements (when delegated by the capability requirements validation authority) are subject to cost-performance trades and adjustments to meet affordability constraints. Cost performance trades (for non-KPP requirements) will be coordinated with the cognizant capability requirements validation authority.

(b) CSBs. For ACAT I and ACAT IA programs, and following CDD Validation, the Acquisition Executive of each DoD Component will form and chair a CSB with broad executive membership including senior representatives from the Office of the USD(AT&L) (including the Assistant Secretary of Defense for Acquisition), the Joint Staff (Director of Force Structure, Resources, and Assessments, J-8), DOT&E (or designated representative), and the DoD CIO; empowered representatives from the Service Chief of Staff and comptroller offices of the Military Department concerned; representatives from other Military Departments where

appropriate; the Military Deputy to the CAE; the PEO; and other senior representatives from OSD and the DoD Component, as appropriate, in accordance with section 814 of Public Law (P.L.) 110-417 (Reference(g)). A DoD Component equivalent board will serve as the CSB for an ACAT IA program that is a DBS. DoD Components should form appropriate level and composition CSBs for lower ACAT programs.

1. The CSB will meet at least annually, and more frequently as capability requirements or content trades are needed, to review all requirements changes and any significant technical configuration changes for ACAT I and IA programs in development, production, and sustainment that have the potential to result in cost and schedule impacts to the program. The CSB will review potential capability requirements changes and propose to the requirements validation authority those changes that may be necessary to achieve affordability constraints on production and sustainment costs or that will result in a more cost-effective product. Changes that increase cost will not be approved unless funds are identified and schedule impacts are addressed. The CSB will monitor changes in program requirements and ensure that the Service Chief, in consultation with the Secretary of the Military Department concerned and the JROC, approves of any proposed changes that could have an adverse effect on program cost, schedule, or performance. Program requirements will fall under the cognizance of the CSB upon receipt of a validated CDD or other validated requirements document, and before the Development RFP Release Decision Point. CSBs may also be formed earlier in the program at the discretion of the CAE.

2. The Program Manager, in consultation with the PEO and the requirements sponsor, will, on at least an annual basis, identify and propose to the CSB a set of recommended requirements changes to include descoping options that reduce program cost and/or moderate requirements and changes needed to respond to any threat developments. These options will be presented to the CSB with supporting rationale addressing operational implications. The chair of the CSB will recommend to the DoD Component requirements authority, the validation authority, and the DAE (if an ACAT ID or MAIS program and KPPs are affected) which of these options should be implemented.

(6) Development RFP Release Decision Point

(a) This decision point authorizes the release of RFPs for EMD and often for LRIP or Limited Deployment options. This review is the critical decision point in an acquisition program. The program will either successfully lead to a fielded capability or fail, based on the soundness of the capability requirements, the affordability of the program, and the executability of the acquisition strategy. The acquisition strategy is put into execution at this decision point by asking industry for bids that comply with the strategy. Release of the RFP for EMD sets in motion all that will follow. This is the last point at which significant changes can be made without a major disruption.

(b) The purpose of the Development RFP Release Decision Point is to ensure, prior to the release of the solicitation for EMD, that an executable and affordable program has been planned using a sound business and technical approach. One goal at this point is to avoid any major program delays at Milestone B, when source selection is already complete and award is

imminent. Therefore, prior to release of final RFPs, there needs to be confidence that the program requirements to be bid against are firm and clearly stated; the risk of committing to development and presumably production has been or will be adequately reduced prior to contract award and/or option exercise; the program structure, content, schedule, and funding are executable; and the business approach and incentives are structured to both provide maximum value to the government and treat industry fairly and reasonably.

(c) At the Development RFP Release Decision Point, the Program Manager will summarize TMRR Phase progress and results, and review the Acquisition Strategy for the EMD Phase. Specific attention will be given to overall affordability; the competition strategy and incentive structure; provisions for small business utilization; source selection criteria including any "best value" determination; framing assumptions; engineering and supportability trades and their relationship to validated capability requirements; the threat projections applicable to the system; Should Cost targets; risk management plans; and the basis for the program schedule.

(d) Documents required for the Development RFP Release Decision Point will be submitted no later than 45 calendar days prior to the review. These documents may have to be updated for final approval by the appropriate authority prior to Milestone B and any associated EMD contract awards based on the results of the source selection. For programs for which the DAE is the MDA, appropriate sections of the EMD RFP and its attachments will be reviewed by relevant OSD staff personnel in support of this decision point, after obtaining specific authority in writing from the cognizant contracting officer.

(e) For MDAPs and major systems, the MDA will determine the preliminary LRIP quantity (or the scope of limited deployment for MAIS programs) at the Development RFP Release Decision Point. LRIP quantities will be the minimum needed to provide production representative test articles for operational test and evaluation (OT&E) (as determined by DOT&E for MDAPS or special interest programs), to establish an initial production base for the system and provide efficient ramp up to full-rate production, and to maintain continuity in production pending completion of operational testing. The final LRIP quantity for an MDAP (with rationale for quantities exceeding 10 percent of the total production quantity documented in the Acquisition Strategy) must be included in the first Selected Acquisition Report submitted to Congress after quantity determination. Table 5 in Enclosure 1 provides details about the Selected Acquisition Report.

(f) For incrementally deployed software intensive programs, the MDA will determine the preliminary scope of limited deployment that will be adequate to evaluate fielding plan execution and support OT&E prior to a Full Deployment Decision for each capability increment.

(g) Decisions resulting from the Development RFP Release Decision Point will be documented in an ADM. The ADM will document specific criteria required for Milestone C approval including needed test accomplishments, LRIP quantities, affordability requirements, and FYDP funding requirements. Table 2 in Enclosure 1 of this instruction identifies the requirements that must be satisfied at this review.

(7) PDR. During the TMRR Phase, and unless waived by the MDA, a PDR will be conducted so that it occurs before Milestone B and prior to contract award for EMD. The timing of the PDR relative to the Development RFP Release Decision Point is at the discretion of the DoD Component. The Component should balance the need for more mature design information to support source selection with the costs of either: (1) extending multiple sources' design activities from the PDR until award of the full EMD contract or (2) having a gap in development prior to EMD award. Unless waived by the MDA, PDR results will be assessed by the MDA prior to the MDA Certification and Determination pursuant to section 2366b of Title 10, U.S. Code (Reference (h)) and Milestone B approval for MDAPs (hereafter, U.S. Code citations are presented as [title #] U.S.C. [section #], e.g., "10 U.S.C. 2366b"). Table 6 in Enclosure 1 of this instruction lists required waiver documentation and actions.

(8) Milestone B

(a) This milestone provides authorization to enter into the EMD Phase and for the DoD Components to award contracts for EMD. It also commits the required investment resources to the program. Most requirements for this milestone should be satisfied at the Development RFP Release Decision Point; however, if any significant changes have occurred, or if additional information not available at the Development RFP Release Decision Point could impact this decision, it must be provided at the Milestone B. Milestone B requires final demonstration that all sources of risk have been adequately mitigated to support a commitment to design for production. This includes technology, engineering, integration, manufacturing, sustainment, and cost risks. Validated capability requirements, full funding in the FYDP, and compliance with affordability goals for production and sustainment, as demonstrated through an independent cost estimate (ICE), are required. The framing assumptions central to shaping the program's cost, schedule, and performance expectations are also required.

(b) Milestone B is normally the formal initiation of an acquisition program with the MDA's approval of the Acquisition Program Baseline (APB). The APB is the agreement between the MDA and the Program Manager and his or her acquisition chain of command that will be used for tracking and reporting for the life of the program or program increment (see section 4 in Enclosure 1 of this instruction for additional policy regarding APBs). The APB will include the affordability caps for unit production and sustainment costs. Affordability caps are established as fixed cost requirements equivalent to KPPs.

(c) At the milestone, the MDA will:

1. Approve the LRIP quantity or the scope of limited deployment, as applicable.

2. Specify the technical event-based criteria for initiating production or making deployment decisions.

3. Decide whether to accept any Program Manager information waiver requests for the next decision event.

4. Document decisions in an ADM.

(d) Table 2 in Enclosure 1 identifies the statutory and regulatory requirements for Milestone B.

(9) EMD Phase

(a) Purpose. The purpose of the EMD Phase is to develop, build, and test a product to verify that all operational and derived requirements have been met, and to support production or deployment decisions.

(b) Phase Description

1. General. EMD completes all needed hardware and software detailed design; systemically retires any open risks; builds and tests prototypes or first articles to verify compliance with capability requirements; and prepares for production or deployment. It includes the establishment of the initial product baseline for all configuration items.

a. Design. The system design effort usually includes a standard series of design reviews prior to test article fabrication and/or software build or increment coding. Multiple design iterations may be necessary to converge on a final design for production. The SEP, described in section 2 in Enclosure 3 of this instruction, provides the basis for design activities.

b. Post-Milestone B PDR. If a PDR prior to Milestone B has been waived, the Program Manager will plan for a PDR as soon as feasible after program initiation.

2. Developmental Test and Evaluation (DT&E). Developmental testing and evaluation provides feedback to the Program Manager on the progress of the design process and on the product's compliance with contractual requirements. DT&E activities also evaluate the ability of the system to provide effective combat capability, including its ability to meet its validated and derived capability requirements, including the verification of the ability of the system to achieve KPPs and KSAs, and that initial system production and deployment and OT&E can be supported. The effort requires completion of DT&E activities consistent with the TEMP. Successful completion of adequate testing with production or deployment representative prototype test articles will normally be the primary basis for entering LRIP or Limited Deployment. Enclosure 4 includes more detailed discussions of DT&E requirements.

3. Early OT&E Events. Independent operational assessments, conducted by the Component operational test organization, will normally also occur during EMD. These events may take the form of independent evaluation of developmental test results or of separate dedicated test events such as Limited User Tests. Developmental and operational test activities should, to the extent feasible, be planned in conjunction with one another to provide as efficient an overall test program as possible. Enclosures 4 and 5 provide more detailed discussions of DT&E and OT&E.

(c) Preparation for Production, Deployment, and Sustainment. During EMD, the Program Manager will finalize designs for product support elements and integrate them into a comprehensive product support package. Early in the EMD Phase, the Program Manager's initial product support performance requirements allocations will be refined based on the results of engineering reviews. Later in this phase, programs will demonstrate product support performance through test, to ensure the system design and product support package meet the sustainment requirements within the affordability caps established at Milestone B.

(d) EMD Phase Completion. The EMD Phase will end when: (1) the design is stable; (2) the system meets validated capability requirements demonstrated by developmental and initial operational testing as required in the TEMP; (3a) manufacturing processes have been effectively demonstrated and are under control; (3b) software sustainment processes are in place and functioning; (4) industrial production capabilities are reasonably available; and (5) the system has met or exceeds all directed EMD Phase exit criteria and Milestone C entrance criteria. EMD will often continue past the initial production or fielding decision until all EMD activities have been completed and all requirements have been tested and verified.

(e) Concurrency Between EMD and Production. In most programs for hardware intensive products, there will be some degree of concurrency between initial production and the completion of developmental testing; and perhaps some design and development work, particularly completion of software, that will be scheduled to occur after the initial production decision. Concurrency between development and production can reduce the lead time to field a system, but it also can increase the risk of design changes and costly retrofits after production has started. Program planners and decision authorities should determine the acceptable or desirable degree of concurrency based on a range of factors. In general, however, there should be a reasonable expectation, based on developmental testing of full-scale EMD prototypes, that the design is stable and will not be subject to significant changes following the decision to enter production. At Milestone B, the specific technical event-based criteria for initiating production or fielding at Milestone C will be determined and included in the Milestone B ADM.

(f) Release of the P&D RFP. If the strategy and associated business arrangements planned and approved at Milestone B have been changed as a result of EMD phase activity, or if the validated capability requirements have changed, an updated Acquisition Strategy will be submitted for MDA review and approval prior to the release of the RFP for competitive source selection or the initiation of sole source negotiations. In any event, an updated Acquisition Strategy will be submitted prior to Milestone C and contract award, consistent with the procedures specified in this document. Paragraph 6a in Enclosure 2 provides additional detail about the Acquisition Strategy.

(g) Additional EMD Phase Requirements

1. Inherently Government Functions and Lead System Integrators (LSI). Program managers will emphasize the importance of appropriate checks and balances when contractors perform acquisition-related activities and ensure that the government is singularly responsible for the performance of inherently governmental functions. If the Acquisition Strategy for a major system calls for the use of a LSI, a contract will not be awarded to an offeror

that either has or is expected to acquire a direct financial interest in the development or construction of an individual system or an element of a system of systems within the major system under the LSI. Exceptions may be granted by the MDA, as provided in 10 U.S.C. 2410p (Reference (h)), that require certification to the Committees on Armed Services of the Senate and House of Representatives. Table 6 in Enclosure 1 of this instruction provides details about the exception reporting.

2. Advanced Procurement of Long Lead Production Items. The MDA may authorize long lead at any point during EMD or at the Development RFP Release Decision or Milestone B, subject to the availability of appropriations. These items are procured in advance of a Milestone C production decision in order to provide for a more efficient transition to production. The amount of long lead appropriate for a given program depends on the type of product being acquired. The product's content dictates the need for early purchase of selected components or subsystems to implement a smooth production process. Long lead authorization will be documented in an ADM and limited in content (i.e., listed items) and/or dollar value within the authorizing ADM.

(10) Milestone C

(a) Milestone C and the Limited Deployment Decision are the points at which a program or increment of capability is reviewed for entrance into the P&D Phase or for Limited Deployment. Approval depends in part on specific criteria defined at Milestone B and included in the Milestone B ADM. The following general criteria will normally be applied: demonstration that the production/deployment design is stable and will meet stated and derived requirements based on acceptable performance in developmental test events; an operational assessment; mature software capability consistent with the software development schedule; no significant manufacturing risks; a validated Capability Production Document (CPD) or equivalent requirements document; demonstrated interoperability; demonstrated operational supportability; costs within affordability caps; full funding in the FYDP; properly phased production ramp up; and deployment support.

1. In making Milestone C and Limited Deployment decisions, the MDA will consider any new validated threat environments that were not included in the CPD and might affect operational effectiveness, and will consult with the requirements validation authority as part of the production decision making process to ensure that capability requirements are current.

2. MDA decisions at Milestone C and Limited Deployment Decisions will be documented in an ADM following the review. Table 2 in Enclosure 1 identifies the statutory and regulatory requirements that will be satisfied at Milestone C.

(b) High-Cost First Article Combined Milestone B and C Decisions. Some programs, notably spacecraft and ships, will not produce prototypes during EMD for use solely as test articles because of the very high cost of each article. In this case, the first articles produced will be tested and then fielded as operational assets. These programs may be tailored by measures such as combining the development and initial production investment commitments. When this is the case, a combined Milestone B and C will be conducted. Additional decision

points with appropriate criteria may also be established for subsequent low rate production commitments that occur prior to OT&E and a Full-Rate Production Decision.

(11) Production and Deployment (P&D) Phase

(a) Purpose. The purpose of the P&D Phase is to produce and deliver requirements-compliant products to receiving military organizations.

(b) Phase Description. In this phase, the product is produced and fielded for use by operational units. The phase encompasses several activities and events: LRIP, Limited Deployment, OT&E, and the Full-Rate Production Decision or the Full Deployment Decision followed by full-rate production or full deployment. In this phase, all system sustainment and support activities are initiated if they haven't already commenced. During this phase the appropriate operational authority will declare IOC when the defined operational organization has been equipped and trained and is determined to be capable of conducting mission operations. During this phase Should Cost management and other techniques will be used continuously to control and reduce cost.

1. LRIP and Limited Deployment. LRIP establishes the initial production base for the system or capability increment, provides the OT&E test articles, provides an efficient ramp up to full-rate production, and maintains continuity in production pending OT&E completion. While this portion of the phase should be of limited duration so that efficient production rates can be accomplished as soon and as economically as possible, it should be of sufficient duration to permit identification and resolution of any deficiencies prior to full-rate production. Limited Deployment for software developments is principally intended to support OT&E and can, consistent with the program strategy, be used to provide tested early operational capability to the user prior to full deployment.

2. OT&E. The appropriate operational test organization will conduct operational testing in a realistic threat environment. The threat environment will be based on the program's Validated On-line Life-cycle Threat Report and appropriate scenarios. For MDAPs, MAIS programs, and other programs on the DOT&E Oversight List, the DOT&E will provide a report providing the opinion of the DOT&E as to whether the program is operationally effective, suitable, and survivable before the MDA makes a decision to proceed beyond LRIP. For programs on the DOT&E Oversight List, operational testing will be conducted in accordance with the approved TEMP and operational test plan. If LRIP is not conducted for programs on the DOT&E Oversight List, fully production-representative articles must nonetheless be provided for the conduct of the required operational testing. Enclosures 4 and 5 provide details about developmental and operational testing and the TEMP.

(12) Full-Rate Production Decision or Full Deployment Decision. The MDA will conduct a review to assess the results of initial OT&E, initial manufacturing, and limited deployment, and determine whether or not to approve proceeding to Full-Rate Production or Full Deployment. Continuing into Full-Rate Production or Full Deployment requires demonstrated control of the manufacturing process, acceptable performance and reliability, and the establishment of adequate sustainment and support systems.

(a) In making the Full-Rate Production Decision or the Full Deployment Decision, the MDA will consider any new validated threat environments that might affect operational effectiveness, and may consult with the requirements validation authority as part of the decision making process to ensure that capability requirements are current.

(b) Except as specifically approved by the MDA, critical deficiencies identified in testing will be resolved prior to proceeding beyond LRIP or limited deployment. Remedial action will be verified in follow-on test and evaluation.

(c) The decision to proceed into full-rate production or full deployment will be documented in an ADM. Table 2 in Enclosure 1 identifies the statutory and regulatory requirements associated with this decision.

(13) Full-Rate Production or Full Deployment. In this part of the P&D Phase, the remaining production or deployment of the product is completed, leading to Full Operational Capability or Full Deployment.

(14) Operations and Support (O&S) Phase

(a) Purpose. The purpose of the O&S Phase is to execute the product support strategy, satisfy materiel readiness and operational support performance requirements, and sustain the system over its life cycle (to include disposal). The O&S Phase begins after the production or deployment decision and is based on an MDA-approved LCSP. Enclosure 6 includes a more detailed discussion of sustainment planning; Enclosure 7 addresses planning for human systems integration.

(b) Phase Description. The phase has two major efforts, Sustainment and Disposal. The LCSP, prepared by the Program Manager and approved by the MDA, is the basis for the activities conducted during this phase.

1. Sustainment. During this phase, the Program Manager will deploy the product support package and monitor its performance according to the LCSP. The LCSP may include time-phased transitions between commercial, organic, and partnered product support providers. The Program Manager will ensure resources are programmed and necessary IP deliverables and associated license rights, tools, equipment, and facilities are acquired to support each of the levels of maintenance that will provide product support; and will establish necessary organic depot maintenance capability in compliance with statute and the LCSP.

a. A successful program meets the sustainment performance requirements, remains affordable, and continues to seek cost reductions by applying Should Cost management and other techniques throughout the O&S Phase. Doing so requires close coordination with the war-fighting sponsor (i.e., user), resource sponsors, and materiel enterprise stake holders, along with effective management of support arrangements and contracts. During O&S, the Program Manager will measure, assess, and report system readiness using sustainment metrics and

implement corrective actions for trends diverging from the required performance outcomes defined in the APB and LCSP.

b. Over the system life cycle, operational needs, technology advances, evolving threats, process improvements, fiscal constraints, plans for follow-on systems, or a combination of these influences and others may warrant revisions to the LCSP. When revising the LCSP, the Program Manager will revalidate the supportability analyses and review the most current product support requirements, senior leader guidance, and fiscal assumptions to evaluate product support changes or alternatives and determine best value.

2. Disposal. At the end of its useful life, a system will be demilitarized and disposed of in accordance with all legal and regulatory requirements and policy relating to safety (including explosives safety), security, and the environment.

e. Additional Procedures and Guidance

(1) The enclosures to this instruction contain additional acquisition policy and procedures that guide program planning.

(a) Enclosure 1 details the programmatic requirements established by statute or regulation. It defines acquisition program categories and compliance requirements for those categories.

(b) Enclosures 2 through 10 and Enclosure 13 provide specific policy and procedures applicable in various functional areas across the life cycle of the acquired system.

(c) Enclosure 11 provides specific policy applicable to programs containing information technology.

(d) Reference (cw) provides specific policy and procedures applicable to Defense Business Systems.

(e) Enclosure 12 provides specific policy and procedures applicable to satisfying urgent needs in less than 2 years.

(2) Consistent with program requirements and subparagraphs 4b and 4c of this instruction, MDAs may tailor the information requirements and procedures in this section of the instruction and in Enclosures 1 through 14. As stated in paragraph 4c, some exceptions to regulatory policy may require coordination with the cognizant authority. Statutory requirements will not be waived unless permitted by the statute.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on the Directives Division Website at http://www.esd.whs.mil/DD/.

7. SUMMARY OF CHANGE 4. This change reassigns the office of primary responsibility for this instruction to the Under Secretary of Defense for Acquisition and Sustainment in accordance with the July 13, 2018 Deputy Secretary of Defense Memorandum (Reference (cx)).

8. EFFECTIVE DATE. This instruction is effective January 7, 2015.

Frank Kendall Under Secretary of Defense for Acquisition, Technology, and Logistics	J. Michael Gilmore Director, Operational Test and Evaluation	Terry Halvorsen Acting DoD Chief Information Officer

References

Enclosures

1. Acquisition Program Categories and Compliance Requirements
2. Program Management
3. Systems Engineering
4. Developmental Test and Evaluation (DT&E)
5. Operational and Live Fire Test and Evaluation (OT&E and LFT&E)
6. Life-Cycle Sustainment
7. Human Systems Integration (HSI)
8. Affordability Analysis and Investment Constraints
9. Analysis of Alternatives (AoA)
10. Cost Estimating and Reporting
11. Requirements Applicable to All Programs Containing Information Technology (IT)
12. Urgent Capability Acquisition
13. Cybersecurity in the Defense Acquisition System

Glossary

TABLE OF CONTENTS

PURPOSE 1
APPLICABILITY 1
POLICY 1
RESPONSIBILITIES 2
Defense Acquisition Executive (DAE) 2
MDA 2
Heads of the DoD Components 2
Secretaries of the Military Departments 2
Chiefs of the Military Services 2
PROCEDURES 3
Overview 3
Relationship Between Defense Acquisition, Requirements, and Budgeting Processes 5
Generic and DoD-Specific Acquisition Program Models, Decision Points, and Phase Activities. 6
Model 1: Hardware Intensive Program 10
Model 2: Defense Unique Software Intensive Program 10
Model 3: Incrementally Deployed Software Intensive Program 12
Model 4: Accelerated Acquisition Program. 13
Models 5 and 6: Hybrid Acquisition Programs 13
Risk Management in Hybrid Models 15
Acquisition Process Decision Points and Phase Content 15
Materiel Development Decision 16
Materiel Solution Analysis Phase 16
Milestone A 17
TMRR Phase 19
CDD Validation and CSBs 21
Development RFP Release Decision Point 22
PDR 24
Milestone B 24
EMD Phase 25
Milestone C 27
Production and Deployment (P&D) Phase 28
Full-Rate Production Decision or Full Deployment Decision 28
Full-Rate Production or Full Deployment 29
Operations and Support (O&S) Phase 29
Additional Procedures and Guidance 30
RELEASABILITY 30
SUMMARY OF CHANGE 4 31
EFFECTIVE DATE 31

REFERENCES 39

ENCLOSURE 1: ACQUISITION PROGRAM CATEGORIES AND COMPLIANCE REQUIREMENTS 44

PURPOSE 44
ACATs 44
Categories 44
Designation of Programs That Qualify as Both a Major Automated Information System (MAIS) Program and a Major Defense Acquisition Program (MDAP) 44
Program Reclassification 44
ACQUISITION PROGRAM INFORMATION REQUIREMENTS AT MILESTONES AND OTHER DECISION POINTS 46
APBs AND BASELINE BREACHES 59
REPORTING REQUIREMENTS 61
CCA COMPLIANCE 74

ENCLOSURE 2: PROGRAM MANAGEMENT 75
PURPOSE 75
ACQUISITION CHAIN OF COMMAND 75
ASSIGNMENT OF PEOs 75
ASSIGNMENT OF PROGRAM MANAGERS 76
PROGRAM OFFICE STRUCTURE AND ORGANIZATIONS 78
Program Office Structure 78
Joint Program Office Organization 78
PROGRAM MANAGEMENT RESPONSIBILITIES 78
Acquisition Strategies 79
Program Baseline Development and Management 80
Earned Value Management (EVM) 80
Risk Management 81
Cost Baseline Control and Use of “Should Cost” Management 82
INTERNATIONAL ACQUISITION AND EXPORTABILITY 82
International Acquisition and Exportability Considerations 82
International Cooperative Program Management 82
Waivers 83
INDUSTRIAL BASE ANALYSIS AND CONSIDERATIONS 83
LIFE-CYCLE MANAGEMENT OF INFORMATION AND DATA PROTECTION 84

ENCLOSURE 3: SYSTEMS ENGINEERING 85
PURPOSE 85
SYSTEMS ENGINEERING PLAN 85
DEVELOPMENT PLANNING 86
SYSTEMS ENGINEERING TRADE-OFF ANALYSES 86
TECHNICAL RISK AND OPPORTUNITY MANAGEMENT 86
TECHNICAL PERFORMANCE MEASURES AND METRICS 87
TECHNICAL REVIEWS 87
PDR 87
Critical Design Review (CDR) 87
CONFIGURATION MANAGEMENT 88
MODELING AND SIMULATION 88
MANUFACTURING AND PRODUCIBILITY 88

SOFTWARE 88
RELIABILITY AND MAINTAINABILITY (R&M) 89
PROGRAM PROTECTION 89
PPP 90
Countermeasures 90
MODULAR OPEN SYSTEMS APPROACH 90
CORROSION PREVENTION AND CONTROL 91
ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH (ESOH) 91
PESHE 91
NEPA/ E.O. 12114 91
Mishap Investigation Support 92
INSENSITIVE MUNITIONS 92
ITEM UNIQUE IDENTIFICATION. 92
SPECTRUM SUPPORTABILITY 92
PROGRAM SUPPORT ASSESSMENTS (PSAs) 92

ENCLOSURE 4: DEVELOPMENTAL TEST AND EVALUATION (DT&E) 94
PURPOSE 94
OVERVIEW 94
T&E MANAGEMENT 96
DT&E ACTIVITIES 96
DT&E PLANNING CONSIDERATIONS 97
DT&E EXECUTION, EVALUATION, AND REPORTING 100
DT&E Execution 100
DASD(DT&E) Program Assessments 100
DT&E Reports and Data 101

ENCLOSURE 5: OPERATIONAL AND LIVE FIRE TEST AND EVALUATION (OT&E AND LFT&E) 102
OVERVIEW 102
APPLICABILITY 102
DOT&E OVERSIGHT LIST 103
T&E PROGRAM MANAGEMENT 103
Early Engagement 103
Lead Operational Test Agency (OTA) 104
Required Documentation 104
T&E PROGRAM PLANNING 104
OT&E ACTIVITIES 106
Operational Assessments (OAs) 106
RFPs 107
OT&E for Reliability and Maintainability 107
Use of Modeling and Simulation 107
OT&E FOR SOFTWARE 108
CYBERSECURITY 109
LFT&E 109
1RESOURCES AND SCHEDULE 110

OPERATIONAL AND LIVE FIRE T&E EXECUTION 111
Planning Test Events 111
Conducting Test Events 113
Data Management, Evaluation, and Reporting 114
OPERATIONAL TEST READINESS 115
CERTIFICATIONS 115
TEMP EVOLUTION THROUGH THE ACQUISITION MILESTONES 115

ENCLOSURE 6: LIFE-CYCLE SUSTAINMENT 116
PURPOSE 116
SUSTAINMENT ACROSS THE LIFE CYCLE 116
LIFE-CYCLE SUSTAINMENT PLAN (LCSP) 118
SUSTAINMENT METRICS 120
Materiel Reliability 120
O&S Cost 121
Mean Down Time 121
Other Metrics 121
PRODUCT SUPPORT REVIEWS 121

ENCLOSURE 7: HUMAN SYSTEMS INTEGRATION (HSI) 122
PURPOSE 122
GENERAL 122
HSI PLANNING 122
Human Factors Engineering 122
Personnel 122
Habitability 122
Manpower 123
Training 123
Safety and Occupational Health 123
Force Protection and Survivability 123

ENCLOSURE 8: AFFORDABILITY ANALYSIS AND INVESTMENT CONSTRAINTS 124
PURPOSE 124
OVERVIEW 124
LIFE- CYCLE AFFORDABILITY 125
A Product Life Cycle, Component Portfolio Analysis (30 to 40 Years Nominal) 125
Future Budget 126
Time Horizon 126
Consistency 126
Fiscal Guidance 126
Inflators 126
Portfolios 126
Other Portfolio Plans 126
Affordability Analysis Updates 126
Affordability Analysis Output Format 126
Data Format 127

Data Requirements for Programs 127
Timing of Affordability Analysis 127
Importance of AoAs to Affordability 127
Affordability Constraints: Goals and Caps 127
At MDD 128
At Milestone A 128
At the Development RFP Release Decision Point, Milestone B, and Beyond 128
Monitoring and Reporting 128
LOWER ACAT PROGRAMS 128

ENCLOSURE 9: ANALYSIS OF ALTERNATIVES (AOA) 129
PURPOSE 129
AOA PROCEDURES 129

ENCLOSURE 10: COST ESTIMATING AND REPORTING 131
PURPOSE 131
COST ESTIMATION 131
COST ANALYSIS REQUIREMENTS DESCRIPTION (CARD) 134
DATA TO SUPPORT COST ESTIMATING 134
DCAPE PROCEDURES 135
MULTI-YEAR PROCUREMENT—COST ANALYSIS REQUIREMENTS 136
General 136
CAPE Role and Requirements 137
Additional Requirements 137

ENCLOSURE 11: REQUIREMENTS APPLICABLE TO ALL PROGRAMS CONTAINING INFORMATION TECHNOLOGY (IT) 138
PURPOSE 138
APPLICABILITY 138
CLINGER-COHEN ACT (CCA) COMPLIANCE 138
POST IMPLEMENTATION REVIEW (PIR) 139
DOD INFORMATION ENTERPRISE ARCHITECTURE 139
CYBERSECURITY 140
Cybersecurity Risk Management Framework (RMF) 140
Cybersecurity Strategy 140
TRUSTED SYSTEMS AND NETWORKS (TSN) 140
LIMITED DEPLOYMENT FOR A MAJOR AUTOMATED INFORMATION SYSTEM (MAIS) PROGRAM 141
CLOUD COMPUTING 141
DOD ENTERPRISE SOFTWARE INITIATIVE (ESI) 141
DOD DATA CENTER CONSOLIDATION 141
IT, INCLUDING NSS, INTEROPERABILITY 141
DATA PROTECTION 142
SECTION 508 - ACCESSIBILITY OF ELECTRONIC AND INFORMATION TECHNOLOGY FOR INDIVIDUALS WITH DISABILITIES 142

ENCLOSURE 12: URGENT CAPABILITY ACQUISITION 143
PURPOSE 143
URGENT OPERATIONAL NEEDS AND OTHER QUICK REACTION CAPABILITIES 143
PROCEDURES 144
URGENT CAPABILITY ACQUISITION ACTIVITIES 145
Pre-Development 145
Development Milestone. Entry into Development is approved by the MDA 147
Development Activities 149
P&D Milestone 149
O&S 150
ADDITIONAL INFORMATION REQUIREMENTS 151

ENCLOSURE 13: CYBERSECURITY IN THE DEFENSE ACQUISITION SYSTEM 153
INTRODUCTION 153
Cyber Impact on Defense Acquisition 153
Program Manager Responsibilities 153
CYBERSECURITY RISKS 154
Government Program Organization 154
Contractor Organizations and Environments 154
Software and Hardware 154
System Interfaces 155
Enabling and Support Equipment, Systems, and Facilities 155
Fielded Systems 155
ACTIVITIES TO MITIGATE CYBERSECURITY RISKS 155
Safeguard Program Information Against Cyber-Attack 155
Design for Cyber Threat Environments 156
Manage Cybersecurity Impacts to Information Types and System Interfaces to the DoDIN 160
Protect the System Against Cyber Attacks From Enabling and Supporting Systems 160
Protect Fielded Systems 160
Independent Acquisition, Engineering, and Technical Assessments 161
PROTECTION PLANNING 161
Systems Engineering Plan (SEP) 161
PPP 161
TEMP 162
Risk Management Framework for DoD IT Security Plan and Cybersecurity Strategy 162
PROGRAM MANAGEMENT AND COMPONENT ACTIONS TO IMPLEMENT CYBERSECURITY AND RELATED PROGRAM SECURITY ACROSS THE MATERIEL LIFE CYCLE 162
Prior to Materiel Development Decisions 162
Materiel Solutions Analysis (MSA) Phase 163
Technology Maturation and Risk Reduction (TMRR) Phase 164
Engineering and Manufacturing Development (EMD) Phase 164
Production and Deployment Phase 165

Operations and Support Phase 166
RESOURCES FOR EXECUTING CYBERSECURITY AND RELATED PROGRAM SECURITY ACTIVITIES 166

GLOSSARY 170

TABLES

1. Description and Decision Authority for ACAT I – III Programs 45
2. Milestone and Phase Information Requirements 48
3. APBs 60
4. Statutory Program Breach and Change Definitions 61
5. Recurring Program Reports 63
6. Exceptions, Waivers, and Alternative Management and Reporting Requirements 65
7. CSDR System Requirements 71
8. EVM Application Requirements 72
9. EVM Reporting Requirements 73
10. CCA Compliance 74
11. Information Requirements Unique to the Urgent Capability Acquisition Process 152
12. Cybersecurity and Related Program Security Resources and Publications 167

FIGURES

3. Model 1: Hardware Intensive Program 10
4. Model 2: Defense Unique Software Intensive Program 11
5. Model 3: Incrementally Deployed Software Intensive Program 12
6. Model 4: Accelerated Acquisition Program 13
7. Model 5: Hybrid Program A (Hardware Dominant) 14
8. Model 6: Hybrid Program B (Software Dominant) 15
9. Operational or Major Live Fire Test Event: Planning, Approval, Execution, and Reporting 111
10. Urgent Capability Acquisitions 145

REFERENCES

(a) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
(b) Interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 26, 2013 (hereby cancelled)
(c) Office of Management and Budget Circular A-11, "Preparing, Submitting, and Executing the Budget," current edition
(d) Public Law 114-92, "National Defense Authorization Act for Fiscal Year 2016"
(e) Chairman of the Joint Chiefs of Staff Instruction 3170.01I, "Joint Capabilities Integration and Development System," January 23, 2015
(f) Assistant Secretary of Defense for Research and Engineering Guide, "Technology Readiness Assessment (TRA) Guidance," April 2011, as amended[1]
(g) Public Law 110-417, "The Duncan Hunter National Defense Authorization Act for Fiscal Year 2009," October 14, 2008
(h) Title 10, United States Code
(i) DoD Instruction 5000.74, "Defense Acquisition of Services," January 5, 2016
(j) Title 15, United States Code
(k) Public Law 109-364, "John Warner National Defense Authorization Act for Fiscal Year 2007," October 17, 2006
(l) Public Law 112-239, "National Defense Authorization Act for Fiscal Year 2013," January 2, 2013
(m) Public Law 111-383, "Ike Skelton National Defense Authorization Act for Fiscal Year 2011," January 7, 2011
(n) Public Law 101-576, "Chief Financial Officers Act of 1990," November 15, 1990
(o) Statement of Federal Financial Accounting Standards (SFFAS) No. 23, "Eliminating the Category National Defense Property, Plant, and Equipment," May 8, 2003
(p) Title 40, United States Code
(q) Public Law 106-398, "Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001," October 30, 2000
(r) Joint Capabilities Integration and Development System (JCIDS) Manual "Manual for the Operation of the Joint Capabilities Integration and Development System," current edition[2]
(s) Chairman of the Joint Chiefs of Staff Instruction 5123.01G, "Charter for Joint Requirements Oversight Council," February 12, 2015
(t) Defense Intelligence Agency Directive 5000.200, "Intelligence Threat Support for Major Defense Acquisition Programs," September 19, 2016[3]
(u) Defense Intelligence Agency Instruction 5000.002, "Intelligence Threat Support for Major Defense Acquisition Programs," September 19, 2016[4]
(v) Public Law 112-81, "National Defense Authorization Act for Fiscal Year 2012," December 31, 2011

---

[1] https://acc.dau.mil/CommunityBrowser.aspx?id=18545
[2] https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=1517681
[3] This is a controlled document. The office of primary responsibility is the Defense Intelligence Agency, (202) 231-0678
[4] This is a controlled document. The office of primary responsibility is the Defense Intelligence Agency, (202) 231-0678

(w) DoD Instruction 5000.73, "Cost Analysis Guidance and Procedures," June 9, 2015
(x) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(y) DoD Instruction 7041.03, "Economic Analysis for Decision-Making," September 9, 2015
(z) Public Law 102-538, "The National Telecommunications and Information Organization Act," October 27, 1992
(aa) Title 47, United States Code
(ab) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014
(ac) DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
(ad) DoD Instruction 8410.03, "Network Management (NM)," August 29, 2012, as amended
(ae) DoD Instruction 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property," September 3, 2015
(af) DoD Directive 5250.01, "Management of Intelligence Mission Data (IMD) in DoD Acquisition," January 22, 2013
(ag) Section 4321, Title 42, United States Code
(ah) Executive Order 12114, "Environmental Effects Abroad of Major Federal Actions," January 4, 1979
(ai) DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015
(aj) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, as amended
(ak) Federal Acquisition Regulation, current edition
(al) Defense Federal Acquisition Regulation Supplement, current edition
(am) DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009
(an) Public Law 111-23, "Weapon Systems Acquisition Reform Act of 2009," May 22, 2009
(ao) DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended[5]
(ap) DoD Instruction 4630.09, "Wireless Communications Waveform Development and Management," July 15, 2015
(aq) Public Law 109-163, "National Defense Authorization Act for Fiscal Year 2006," January 6, 2006
(ar) Memorandum of Agreement between the Director of National Intelligence and the Secretary of Defense concerning the Management of Acquisition Programs Executed at the Department of Defense Intelligence Community Elements, March 25, 2008[6]
(as) Intelligence Community Policy Guidance 801.1, "Acquisition," July 12, 2007[7]
(at) DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual," November 4, 2011
(au) American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) 748, March 2013

[5] This is a controlled document. The office of primary responsibility is Under Secretary of Defense (Intelligence), USDI.Pubs@osd.mil. Access requires a DoD PKI Certificate.
[6] www.fas.org/irp/dni/moa.pdf
[7] http://www.dni.gov/files/documents/ICPG/ICPG_801_1.pdf

(av) Data Item Management-81861, "Data Item Description: Integrated Program Management Report (IPMR)," June 20, 2012
(aw) Title 44, United States Code
(ax) DoD Instruction 5000.66, "Operation of the Defense Acquisition, Technology, and Logistics Workforce Education, Training, and Career Development Program," July 27, 2017
(ay) Under Secretary of Defense for Acquisition, Technology, and Logistics Policy Memorandum, "Key Leadership Positions and Qualification Criteria," November 8, 2013
(az) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014
(ba) DoD Instruction 2010.06, "Materiel Interoperability and Standardization with Allies and Coalition Partners," July 29, 2009
(bb) Defense Security Cooperation Agency Manual, "Security Assistance Management Manual (SAMM)," current version[8]
(bc) DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
(bd) Military-Standard 882E, "DoD Standard Practice for System Safety," May 11, 2012
(bf) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, as amended
(bg) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
(bh) DoD Instruction 5000.61, "DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)," December 9, 2009
(bi) DoD Instruction 4151.22, "Condition Based Maintenance Plus (CBM+) for Materiel Maintenance," October 16, 2012
(bj) Public Law 113-66, "National Defense Authorization Act for Fiscal Year 2014," December 26, 2013
(bk) DoD Manual 4160.28, Volume 1, "Defense Demilitarization: Program Administration," June 7, 2011
(bl) DoD Instruction 5000.67, "Prevention and Mitigation of Corrosion on DoD Military Equipment and Infrastructure," February 1, 2010
(bm) DoD Instruction 1100.22, "Policy and Procedures for Determining Workforce Mix," April 12, 2010
(bn) DoD Instruction 7041.04, "Estimating and Comparing the Full Costs of Civilian and Active Duty Military Manpower and Contract Support," July 3, 2013
(bo) DoD Directive 1322.18, "Military Training," January 13, 2009, as amended
(bp) DoD Directive 5105.84, "Director of Cost Assessment and Program Evaluation (DCAPE)," May 11, 2012
(bq) Office of the Secretary of Defense, Cost Assessment and Program Evaluation, "Operating and Support Cost-Estimating Guide," March 2014
(br) Global Information Grid (GIG) Technical Guidance Federation (GTGF)[9]
(bt) Office of Management and Budget Memorandum M-04-08, "Maximizing Use of SmartBuy and Avoiding Duplication of Agency Activities with the President's 24 E-Gov Initiatives," February 25, 2004

[8] http://www.samm.dsca.mil/
[9] http://www.disa.mil/Services/Enterprise-Engineering/IT-Standards

(bu) Office of Management and Budget Memorandum M-04-16, "Software Acquisition," July 1, 2004
(bv) Office of Management and Budget Memorandum M-05-25, "SmartBUY Agreement with Oracle," August 25, 2005
(bw) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
(bx) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(by) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015
(bz) DoD Instruction 3200.12, "DoD Scientific and Technical Information Program (STIP)," August 22, 2013
(ca) Section 794d of Title 29, United States Code
(cb) DoD Manual 8400.01-M, "Procedures for Ensuring the Accessibility of Electronic and Information Technology (E&IT) Procured by DoD Organizations," June 3, 2011
(cc) DoD Directive 5000.71, "Rapid Fulfillment of Combatant Commander Urgent Operational Needs," August 24, 2012
(cd) Public Law 107-314, "Bob Stump National Defense Authorization Act for Fiscal Year 2003," December 2, 2002
(ce) Defense Acquisition University Website[10]
(cf) Defense Acquisition University Glossary[11]
(cg) Public Law 113-291, "Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015," December 19, 2014
(ch) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Change to Major Defense Acquisition Program Milestone A Requirements," January 31, 2016[12]
(ci) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Change to Major Defense Acquisition Program Milestone B Requirements," January 31, 2016[13]
(cj) Integrated Program Management Report Implementation Guide, February 5, 2016[14]
(ck) DoD Instruction 4140.67, "DoD Counterfeit Prevention Policy," April 26, 2013
(cl) Directive Type Memo 17-001, "Cybersecurity in the Defense Acquisition System," January 11, 2017 (hereby cancelled)
(cm) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005, as amended
(cn) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
(co) DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010
(cp) Part 236 of Title 32, Code of Federal Regulations
(cq) Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," February 13, 2015

[10] http://www.dau.mil/default.aspx
[11] https://dap.dau.mil/glossary/Pages/Default.aspx
[12] https://ebiz.acq.osd.mil/DABCalendar/Home/Document/31 (access requires Common Access Card (CAC))
[13] https://ebiz.acq.osd.mil/DABCalendar/Home/Document/32 (access requires CAC)
[14] http://www.acq.osd.mil/evm/docs/IPMR%20Implementation%20Guide.pdf

(cr) Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, "Department of Defense Cybersecurity Test and Evaluation Guidebook," July 1, 2015
(cs) Director, Operational Test and Evaluation, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," August 1, 2014
(ct) Office of the Deputy Assistant Secretary of Defense for Systems Engineering, "Guidance to Stakeholders for Implementing Defense Federal Acquisition Supplement Clause 252.204-7012," August 2015
(cu) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016
(cv) Office of the Deputy Assistant Secretary of Defense for Systems Engineering, "Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs," June 2015
(cw) DoD Instruction 5000.75, "Business Systems Requirements and Acquisition," February 2, 2017
(cx) Deputy Secretary of Defense Memorandum, "Establishment of the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment," July 13, 2018

ENCLOSURE 1

ACQUISITION PROGRAM CATEGORIES AND COMPLIANCE REQUIREMENTS

1. PURPOSE. This enclosure:

a. Provides the definitions and dollar thresholds of acquisition categories (ACATs) and prescribes the policy for assignment of the cognizant MDA.

b. Lists the information requirements associated with the ACATs in tabular format.

c. Provides the policy and procedure applicable to acquisition program baselines and acquisition program reporting.

2. ACATs

a. Categories. An acquisition program will be categorized based on the criteria in Table 1 of this enclosure. Table 1 contains the description and decision authority for ACAT I through ACAT III programs. The Defense Acquisition Executive (DAE) or designee will review potential ACAT I and IA materiel solutions; the Component Acquisition Executive (CAE) or the individual designated by the CAE will review potential ACAT II and ACAT III materiel solutions.

b. Designation of Programs That Qualify as Both a Major Automated Information System (MAIS) Program and a Major Defense Acquisition Program (MDAP). At the DAE's discretion, a program that meets the definitions of both a MAIS program and an MDAP may be treated as an MDAP. Programs will comply with the statutory and regulatory requirements associated with the chosen designation. The DAE's determination will be documented in an ADM for the program.

c. Program Reclassification

(1) The CAE will notify the DAE when an increase or estimated increase in program cost or a change in acquisition strategy will result in a possible reclassification of a formerly lower ACAT program as an ACAT I or IA program. ACAT changes will be reported as soon as the DoD Component anticipates that the program's cost is within 10 percent of the minimum cost threshold of the next ACAT level. ACAT reclassification will occur upon designation by the DAE.

(2) The CAE may request reclassification of an ACAT I or IA program to a lower category. The request will identify the reasons for the reduction in category level. The category reduction will become effective upon approval of the request by the DAE.

Table 1. Description and Decision Authority for ACAT I – III Programs

ACAT	Reason for ACAT Designation	Decision Authority
ACAT I	• MDAP (10 U.S.C. 2430 (Reference (h))) o Dollar value for all increments of the program: estimated by the DAE to require an eventual total expenditure for research, development, and test and evaluation (RDT&E) of more than $480 million in Fiscal Year (FY) 2014 constant dollars or, for procurement, of more than $2.79 billion in FY 2014 constant dollars o MDA designation • MDA designation as special interest[1]	ACAT ID: DAE or as delegated ACAT IC: Head of the DoD Component or, if delegated, the CAE
ACAT IA[2, 3]	• MAIS (10 U.S.C. 2445a (Reference (h))): A DoD acquisition program for an Automated Information System[4] (AIS) (either as a product or a service[5]) that is either: o Designated by the MDA as a MAIS program; or o Estimated to exceed: ▪ $40 million in FY 2014 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, and sustainment, and incurred in any single fiscal year; or ▪ $165 million in FY 2014 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred from the beginning of the Materiel Solution Analysis Phase through deployment at all sites; or ▪ $520 million in FY 2014 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the Materiel Solution Analysis Phase through sustainment for the estimated useful life of the system. • MDA designation as special interest[1]	ACAT IAM: DAE or as delegated ACAT IAC: Head of the DoD Component or, if delegated, the CAE
ACAT II	• Does not meet criteria for ACAT I or IA • Major system (10 U.S.C. 2302d (Reference (h))) o Dollar value: estimated by the DoD Component head to require an eventual total expenditure for RDT&E of more than $185 million in FY 2014 constant dollars, or for procurement of more than $835 million in FY 2014 constant dollars o MDA designation[5] (10 U.S.C. 2302 (Reference (h)))	CAE or the individual designated by the CAE[6]
ACAT III	• Does not meet criteria for ACAT II or above • An AIS program that is not a MAIS program	Designated by the CAE[6]

1. The Special Interest designation is typically based on one or more of the following factors: technological complexity; congressional interest; a large commitment of resources; or the program is critical to the achievement of a capability or set of capabilities, part of a system of systems, or a joint program. Programs that already meet the MDAP and MAIS thresholds cannot be designated as Special Interest.

2. When a MAIS program also meets the definition of an MDAP, the DAE will be the MDA unless delegated to a DoD Component or other official. The DAE will designate the program as either a MAIS or an MDAP, and the Program Manager will manage the program consistent with the designation.

3. The DAE will designate MAIS programs as ACAT IAM or ACAT IAC. MAIS programs will not be designated as ACAT II.

4. AIS: A system of computer hardware, computer software, data or telecommunications that performs functions such as collecting, processing, storing, transmitting, and displaying information. Excluded are computer resources, both hardware and software, that are an integral part of a weapon or weapon system; used for highly sensitive classified programs (as determined by the Secretary of Defense); used for other highly sensitive information technology (IT) programs (as determined by the DoD CIO; or determined by the DAE or designee to be better overseen as a non-AIS program (e.g., a program with a low ratio of RDT&E funding to total program acquisition costs or that requires significant hardware development).

5. When determined by the USD (AT&L) (or designee), IT services programs that achieve the MAIS threshold will follow the procedures applicable to MAIS programs specified in this instruction. Additionally, regardless of MAIS status, software that is acquired as a service will be managed under this Instruction. IT services that are designated ACAT III or lower AIS programs will be managed under this Instruction. All other acquisitions of services will comply with DoD Instruction 5000.74 (Reference (i)).

6. As delegated by the Secretary of Defense or Secretary of the Military Department.

(3) The DAE may reclassify an acquisition program at any time. The reclassification decision will be documented in an ADM.

3. ACQUISITION PROGRAM INFORMATION REQUIREMENTS AT MILESTONES AND OTHER DECISION POINTS

a. Table 2 lists the statutory and regulatory requirements at each of the milestones and other decision points during the acquisition process. In consultation with the appropriate stakeholders, program managers may propose for MDA approval, tailoring of Regulatory program information. MDAs will document all information tailoring decisions.

b. Each row identifies an information requirement and the source of the requirement. (Sources may refer to United States Code (U.S.C.), Public Law (P.L.), an Executive Order (E.O.), DoD Instructions (DoDIs), Directives (DoDDs), or other types of documentation. When available, the source will include paragraph (Para.), section (Sec.), or enclosure (Enc.) numbers and the reference (Ref.) identifier from the list of references in this instruction. STATUTORY items and sources appear in ALL CAPS; Regulatory items and sources appear in normal text. Requirements are in alphabetical order.

(1) A dot (●) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission of information. Moving right across a row, a checkmark (✓) indicates the requirement for updated information, and another dot indicates submission of new information.

(2) Notes accompany each row to explain the requirement, limit or extend the requirement's applicability to program type and/or life-cycle event, or refer the reader to more detailed direction.

c. Labels for the "Life-Cycle Event" columns represent the following events:

(1) "MDD"—Materiel Development Decision.

(2) "MS A"—Milestone A Decision Review.

(3) "CDD Val"—Capability Development Document Validation.

(4) "Dev RFP Rel"—The Development RFP Release Decision Point conducted before Milestone B to authorize release of the RFP for the next phase.

(5) "MS B"—Milestone B Decision Review.

(6) "MS C"—Milestone C Decision Review.

(7) "FRP/FD Dec"—The Full-Rate Production (FRP) Decision or the Full Deployment (FD) Decision.

(8) "Other"—An event other than the events listed above; the event will be identified in the notes associated with the row.

d. Documentation for the identified events will be submitted at least 45 calendar days before the planned review.

e. Information requirements that are finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless substantive changes have occurred.

f. Final milestone documents for programs reviewed at the OSD level will be submitted to the Acquisition Information Repository within 5 business days of document approval.

g. In Table 2, when applied to requirements associated with the Development RFP Release Decision Point, the modifier "draft" will mean a Program Manager-, Program Executive Officer (PEO)-, and CAE-approved draft subject to change based on results of the source selection process and pre-Milestone B Component and OSD staff coordination.

h. The Program Manager may submit a document prepared to satisfy the information requirements of multiple programs (instead of a program-specific document). Such substitution will require written permission from the approving authority.

i. When there is a logical relationship between required documents, e.g., the Acquisition Strategy and the Life-Cycle Sustainment Plan, and consequent coordination can be streamlined, the MDA may approve combining requirements.

Table 2. Milestone and Phase Information Requirements

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[6]	MS C	FRP/FD Dec	OTHER		
2366a WRITTEN DETERMINATION	•					•							10 U.S.C. 2366a (Ref. (h)) This instruction	MDA
STATUTORY for MDAPs and major subprograms of MDAPs before Milestone A approval. By this instruction, the MDA does not have authority to delegate this requirement. Specific criteria for the WRITTEN DETERMINATION are in the source statute; implementation details are in the current version of USD(AT&L) Memorandum, "Change to Major Defense Acquisition Program Milestone A Requirements" (Reference (ch)).														
2366b CERTIFICATION AND DETERMINATION	•								•	•			10 U.S.C. 2366b (Ref. (h)) This instruction	MDA
STATUTORY for MDAPs before Milestone B approval. The MDA does not have authority to delegate this requirement. The certification and determination will be submitted to the congressional defense committees with the first Selected Acquisition Report (SAR) submitted after completion of the certification. Specific criteria for the CERTIFICATION AND DETERMINATION are in the source statute; implementation details are in the current version of USD(AT&L) Memorandum, "Change to Major Defense Acquisition Program Milestone B Requirements" (Reference (ci)). A memorandum documenting the certification and determination elements is a Regulatory requirement at Milestone C if "C" is program initiation.														
Acquisition Decision Memorandum (ADM)	•	•	•	•	•	•		•	•	•	•	•	This instruction	MDA
Regulatory. Documents MDA decisions and direction.														
ACQUISITION PROGRAM BASELINE (APB)	•	•	•	•				•	✓	✓	✓	✓	10 U.S.C. 2435 (Ref. (h)) 10 U.S.C. 2433a (Ref. (h)) DoDD 5000.01 (Ref. (a))	MDA
STATUTORY for MDAPs at Milestones B and C and the FRP decision; a Regulatory requirement at all other Program Type/Event combinations, including the required draft at Development RFP Release. For the APB, the draft due at RFP Release does not require CAE approval. The APB is not approved by the MDA until Milestone B, however. See section 4 in this enclosure for requirements at other than the identified decision points.														

Table Notes:

1. A dot (•) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[5]	MS C	FRP/FD Dec	OTHER		
ACQUISITION STRATEGY	•	•	•	•		•		•	✓	✓	✓		10 U.S.C. 2431a (Ref. (h)) Para. 6a of Enc. 2 of this instruction	MDA

STATUTORY for MDAPs, MAIS programs, and major systems; Regulatory for other programs. The Acquisition Strategy includes STATUTORY and Regulatory information. Major changes to the plan reflected in the Acquisition Strategy require MDA approval. If the MDA revises the strategy, the MDA must notify the congressional defense committees consistent with Table 6. The MDA must review and approve the strategy when there has been a significant change to the cost, schedule, or performance of the program (or system) or there has been a critical change to the cost of the program (or system). The strategy may also be reviewed and approved at any time considered relevant by the MDA. The following STATUTORY requirements will be satisfied in the Acquisition Strategy:

- ACQUISITION APPROACH : STATUTORY; describe the top-level business and technical management approach in sufficient detail to allow the MDA to assess (1) the viability of the approach; (2) the method of implementing laws and policies; and (3) program objectives. Provide a clear explanation of how the strategy is designed to be implemented within the available resources of time, funding, and management capacity. Discuss the tailoring that will address program requirements and constraints. Where appropriate, the strategy should consider the delivery of required capability in increments, each dependent on available, mature technology, and recognizing up front the need for future capability improvements. SOURCE: 10 U.S.C. 2431a (Ref. (h))
- BENEFIT ANALYSIS AND DETERMINATION: STATUTORY; applies to bundled acquisitions only. Includes MARKET RESEARCH to determine whether consolidation of the requirements is necessary and justified. Required at Milestone C if there was no Milestone B; an update is not required at the FRP/FD decision point. 15 U.S.C. 632 (Reference (j)) defines a bundled contract as a contract that is entered into to meet requirements that are consolidated in a bundling of contract requirements. The term "bundling of contract requirements" means consolidating two or more procurement requirements for goods or services previously provided or performed under separate smaller contracts into a solicitation of offers for a single contract that is likely to be unsuitable for award to a small-business concern. SOURCE(S): 15 U.S.C. 644(e) (Ref. (j)), 15 U.S.C. 657q (Ref. (j))
- BUSINESS STRATEGY: STATUTORY; paragraph 5d(4)(f)1 in this instruction identifies the minimum set of elements to describe. SOURCE(S): 10 U.S.C. 2431a (Ref. (h)), 10 U.S.C. 2337 (Ref. (h))
- CONTRACTING STRATEGY: STATUTORY; discuss the planned contract type and how it relates to risk management in each acquisition phase; whether risk management enables the use of fixed-price elements in subsequent contracts; market research; and small business participation. Include the following sub-elements. SOURCE(S): 10 U.S.C.2431a (Ref. (h)), 10 U.S.C. 2377 (Ref. (h)), 15 U.S.C. 644(e)(2) (Ref. (j))
  - CONTRACT-TYPE DETERMINATION: STATUTORY. Satisfied when the MDA approves the Acquisition Strategy with specified contract types. Only required for MDAPs at Development RFP Release and Milestones B and C. The MDA for an MDAP may conditionally approve the contract type selected for a development program at the Development RFP Release Decision Point, and give final approval at the time of Milestone B approval. The development contract type must be consistent with the level of program risk and may be either a fixed price or cost type contract. If selecting a cost-type contract, the MDA must comply with the conditions and reporting requirements listed in Table 6 in this enclosure. The DoD MAY NOT enter into cost-type contracts for production of an MDAP unless compliant with the conditions and notifications listed in Table 6. SOURCE(S): SEC. 818, P.L. 109-364 (Ref. (k)), SEC. 811, P.L. 112-239 (Ref. (l))
  - TERMINATION LIABILITY ESTIMATE: STATUTORY. Only for MDAPs. Must be documented in the ACQUISITION STRATEGY for any contract for the development or production of an MDAP for which potential termination liability could reasonably be expected to exceed $100 million. Updates may therefore be required at other than the marked events. The estimate must include how such termination liability is likely to increase or decrease over the period of performance. The Program Manager must consider the estimate before making recommendations on decisions to enter into or terminate such contracts. SOURCE(S): SEC. 812, P.L. 112–239 (Ref. (l))
- COOPERATIVE OPPORTUNITIES: STATUTORY. Only due at the first program milestone review. The requirement to discuss opportunities for cooperative research and development will be satisfied via the International Involvement section in the Acquisition Strategy outline and will include consideration of foreign military sales. For programs responding to urgent needs, proven capabilities will be assessed during the COURSE OF ACTION ANALYSIS. SOURCE(S) : 10 U.S.C. 2350a (Ref. (h))
- GENERAL EQUIPMENT VALUATION: STATUTORY; a program description that identifies contract-deliverable military equipment, non-military equipment, and other deliverable items; includes plan(s) to ensure that all deliverable equipment requiring capitalization is serially identified and valued. Only required at Milestone C; updated as necessary for the FRP/FD Decision. The capitalization thresholds are unit costs at or above $1 million for Air Force and Navy general fund assets, and unit costs at or above $250 thousand for all internal use software and for other equipment assets for all other general and working capital funds. SOURCE(S): P.L. 101-576 (Ref. (n)), Statement of Federal Financial Accounting Standards 23 (Ref. (o))
- INDUSTRIAL BASE CAPABILITIES CONSIDERATIONS: STATUTORY for MDAPs; Regulatory for others. Summarizes the results of the industrial base capabilities' analysis. SOURCE(S): 10 U.S.C. 2440 (Ref. (h))

(continued, next page…)

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[6]	MS C	FRP/FD Dec	OTHER		
ACQUISITION STRATEGY	•	•	•	•		•		•	✓	✓	✓		10 U.S.C. 2431a (Ref. (h)) Para. 6a of Enc. 2 of this instruction	MDA
ACQUISITION STRATEGY, continued														
• INTELLECTUAL PROPERTY (IP) STRATEGY: STATUTORY for major weapon systems and subsystems; Regulatory for other program types. The IP Strategy must be updated as appropriate to support and account for evolving IP considerations associated with the award and administration of all contracts throughout the system life cycle. Becomes part of the Life-Cycle Sustainment Plan (LCSP) during Operations and Support (O&S). For programs responding to urgent needs, due at the Development Milestone. SOURCE(S): 10 U.S.C. 2320 (Ref. (h)), Para. 6a(4) of Enclosure 2 of this instruction														
• MARKET RESEARCH: STATUTORY. A stand-alone, Regulatory requirement at MDD. STATUTORY updates (as part of the ACQUISITION STRATEGY) required at Milestone A and the Development RFP release point; not required thereafter. Conducted to reduce the duplication of existing technologies and products, and to understand potential materiel solutions, technology maturity, and potential sources, to assure maximum participation of small business concerns, and possible strategies to acquire them. For programs responding to urgent needs, included in the Course of Action Approach at the Development Milestone. SOURCE(S): 10 U.S.C. 2377 (Ref. (h)), 15 U.S.C. 644(e)(2) (Ref. (j)), This instruction														
• MODULAR OPEN SYSTEMS APPROACH: STATUTORY. Identify how a modular open systems approach will or will not be used. SOURCE(S): SEC. 801, P.L. 113-291 (Ref. (cg)).														
• MULTI-YEAR PROCUREMENT: STATUTORY; when appropriate, include a summary discussion of multi-year procurement (further discussed in section 6 of Enclosure 10). SOURCE(S): 10 U.S.C. 2306b (Ref. (h)).														
• RISK MANAGEMENT: STATUTORY; include a comprehensive approach to risk management and mitigation. Planning will be consistent with the discussion in paragraphs 6a and 6d in Enclosure 2, and the competitive prototyping discussion in paragraph 5d(4)(b)2 in the basic instruction. If prototyping is not used, explain why. SOURCE(S): 10 U.S.C. 2431a and 10 U.S.C. 2431b (Ref. (h))														
• SMALL BUSINESS INNOVATION RESEARCH (SBIR)/SMALL BUSINESS TECHNOLOGY TRANSFER (STTR) PROGRAM TECHNOLOGIES: STATUTORY. Program managers will establish goals for applying SBIR and STTR technologies in programs of record and incentivize primes to meet those goals. For contracts with a value at or above $100 million, program managers will establish goals for the transition of Phase III technologies in subcontracting plans and require primes to report the number and dollar amount of Phase III SBIR or STTR contracts. Not required at Milestone B. SOURCE(S): 15 U.S.C. 638 (Ref. (j))														
Affordability Analysis	•	•	•	•	•	✓		✓	✓	✓	✓		Sec. 3 of Enc. 8 of this instruction	MDA
Regulatory. Prior to the MDD, the analysis will yield tentative cost goals and inventory goals; for Milestone A, the analysis will yield affordability goals; and for the Development RFP Release Decision Point, Milestone B, and beyond, the analysis will yield binding affordability caps.														
ANALYSIS OF A DLTERNATIVES (AoA)	•	•	•	•		•		✓		✓		✓	40 U.S.C. 11312 (Ref. (p)) SEC. 811, P.L. 106-398 (Ref. (q)) 10 U.S.C. 2366a (Ref. (h))	MDA (DCAPE assesses AoAs for ACAT ID/IAM only)
STATUTORY for MDAPs, MAIS programs, and all AIS programs, including National Security Systems (NSSs), at Milestone A. STATUTORY updates required through Milestone C (or Milestone B if there is no Milestone C) for MAIS programs, and all AIS programs. Regulatory for all other specified Program Type/Event combinations. A DoD Component is responsible for conduct and approval of the AoA. The distinct assessment and approval roles of DCAPE and the MDA associated with the AoA and the selection of the materiel solution(s) are detailed in section 2 of Enclosure 9 of this instruction.														

Table Notes:

1. A dot (•) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[5]	MS C	FRP/FD Dec	OTHER		
AoA Study Guidance and AoA Study Plan	•	•	•	•	•								Para. 5d(1)(b) of this instruction	DCAPE or DoD Component Equivalent
Regulatory requirements to guide the AoA. AoA Study Guidance informs the preparation of the AoA Study Plan. The AoA Study Guidance must be provided to DoD Component(s) for development of the AoA Study Plan prior to the MDD. Consistent with the AoA Study Guidance, the lead DoD Component will prepare the AoA Study Plan and present it at the MDD.														
BANDWIDTH REQUIREMENTS REVIEW	•	•	•	•				•	✓	✓			SEC. 1047, P.L. 110-417 (Ref. (g)) This Instruction	DoD CIO
STATUTORY for MDAPs and major weapon systems; Regulatory for all other programs. Bandwidth requirements data will be documented in the Information Support Plan (ISP). If the ISP is waived for a program, conformance with bandwidth review will be based on data provided in the Capability Development Document (CDD), consistent with Net-Ready Key Performance Parameter (NR-KPP) guidance in Appendix E to Enclosure D of the Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS) (Reference (r)) and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5123.01G (Reference (s)).														
Capability Development Document (CDD)	•	•	•	•		•	✓	✓		✓		✓	CJCSI 3170.01 (Ref.(d)) JCIDS Manual (Ref. (r))	JROC, JCB, or Component Validation
Regulatory. A draft CDD is required at Milestone A; a validated CDD is required at the Development RFP Release Decision Point and informs Milestone B. If there are no changes, a revalidated CDD may be submitted for the Capability Production Document (CPD) required at Milestone C. An equivalent DoD Component-validated requirements document will satisfy this requirement for certain information systems. For approval authorities, JROC is Joint Requirements Oversight Council; JCB is Joint Capabilities Board.														
Capability Production Document (CPD)	•	•	•	•						•			CJCSI 3170.01 (Ref.(d)) JCIDS Manual (Ref. (r))	JROC, JCB, or Component Validation
Regulatory. If there are no changes, a revalidated CDD may satisfy this information requirement. An equivalent DoD Component-validated requirements document will satisfy this requirement for certain information systems; the equivalent documents are finalized after Milestone B, to support deployment.														
CLINGER-COHEN ACT (CCA) COMPLIANCE	•	•	•	•		•			•	•	•		SUBTITLE III, TITLE 40 (Ref. (p)) SEC. 811, P.L. 106-398 (Ref. (q))	MDA and Component CIO or designee
STATUTORY for all programs that acquire information technology (IT); Regulatory for other programs. See section 3 in Enclosure 11 for amplifying guidance. A summary of required actions is in Table 10 in this enclosure. The Program Manager will report CCA compliance to the MDA and the Component CIO or designee. For IT programs employing an incremental development model (i.e., Model 3), the Program Manager will report CCA compliance at each Limited Deployment Decision Point.														

Table Notes:

1. A dot (•) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[5]	MS C	FRP/FD Dec	OTHER		
Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP)	•	•	•	•		•		✓		✓			JCIDS Manual (Ref. (r))	DoD Component
Regulatory. The CONOPS/OMS/MP is a Component approved acquisition document that is derived from and consistent with the validated/approved capability requirements document. The CONOPS/OMS/MP describes the operational tasks, events, durations, frequency, and environment in which the materiel solution is expected to perform each mission and each phase of the mission. The CONOPS/OMS/MP will be provided to the MDA at the specified decision events and normally provided to industry as part of the RFP.														
CORE LOGISTICS DETERMINATION / CORE LOGISTICS AND SUSTAINING WORKLOADS ESTIMATE	•		•	•		•		•	✓	•			10 U.S.C. 2464 (Ref. (h)) 10 U.S.C. 2366a & 2366b (Ref. (h)) SEC. 801, P.L. 112-81 (Ref. (v)) Para. 3d(2) of Enc. 6 of this instruction	MDA/DoD Component
STATUTORY. Only the CORE LOGISTICS DETERMINATION is required at Milestone A. Required at Milestone C if there was no Milestone B. Documented in the LCSP. Not required for AIS programs.														
Cost Analysis Requirements Description (CARD)	•	•				•		✓	•	✓	✓	✓	Sec. 3 of Enc. 10 of this instruction DoDI 5000.73 (Ref. (w))	DoD Component
Regulatory. Due any time an INDEPENDENT COST ESTIMATE (ICE) or an ECONOMIC ANALYSIS is required. Procedures are specified in section 3 of Enclosure 10 of this instruction. The DoD Component, with CAPE concurrence, will determine the CARD requirements for ACAT II and below programs.														
CYBERSECURITY STRATEGY	•	•	•	•		•		✓	✓	✓	✓		SEC. 811, P.L. 106-398 (Ref. (q)) 40 U.S.C. 11312 (Ref. (p)) DoDI 8500.01 (Ref. (x))	DoD CIO; Component CIO
STATUTORY for mission critical or mission essential IT systems. Regulatory for all other programs containing IT, including NSS. See section 6 of Enclosure 11 and Enclosure 14. The CYBERSECURITY STRATEGY is an appendix to the Program Protection Plan (PPP). A draft[4] update is due for the Development RFP Release and is approved at Milestone B. May include the approved DoD Risk Management Framework Security Plan for urgent needs. The DoD CIO is approval authority for ACAT ID and all ACAT IA programs; the Component CIO is approval authority for all other ACATs.														
Defense Intelligence Threat Library (Threat Modules)	•	•	•	•								•	DIA Directive 5000.200 (Ref. (t)) DIA Instruction 5000.002 (Ref. (u))	Validated by Defense Intelligence Agency (DIA)
Regulatory. Threat Modules are produced by the Defense Intelligence Community and are required to be updated every 2 years, independent of acquisition decision events. Threat Modules serve as the analytical foundation for Validated On-line Life-cycle Threat (VOLT) Reports and maintain projections of technology and adversary capability trends over the next 20 years.														

Table Notes:

1. A dot (•) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[5]	MS C	FRP/FD Dec	OTHER		
Development RFP Release Cost Assessment	●	●						●					Para. 2a(5) of Enc. 10 of this instruction	CAPE
Regulatory. Requirements and procedures for this assessment are specified in paragraph 2a(5) in Enclosure 10 of this instruction.														
DoD Component Cost Estimate	●	●				●			●	●	●	●	Para. 5d(3)(b)2b of this instruction Sec. 2 of Enc. 10 of this instruction	DoD Component
Regulatory. See the direction in section 2 of Enclosure 10 of this instruction. The DoD Component will determine the cost estimating requirements for ACAT II and below programs.														
DoD Component Cost Position	●	●				●			●	●	●	●	Para. 2e of Enc. 10 of this instruction	DoD Component
Regulatory. Mandatory for MDAPs and MAIS programs; documented DoD Component Cost Position must be signed by the appropriate DoD Component Deputy Assistant Secretary for Cost and Economics.														
DoD Component Live Fire Test and Evaluation (LFT&E) Report	●		●	●							●	●	This instruction	CAE
Regulatory. Programs on the DOT&E Oversight List for LFT&E oversight only; due upon completion of LFT&E.														
DOT&E REPORT ON INITIAL OPERATIONAL TEST AND EVALUATION (IOT&E)	●	●	●	●							●		10 U.S.C. 2399 (Ref. (h)) 10 U.S.C. 139 (Ref. (h))	DOT&E
STATUTORY; required for DOT&E Oversight List programs only. The DOT&E publishes an online list of programs under operational test and evaluation (OT&E) and LFT&E oversight at https://extranet.dote.osd.mil/oversight/ (requires login with a Common Access Card). A final decision to proceed beyond Low-Rate Initial Production (LRIP) or beyond Limited Deployment may not be made until the DOT&E has submitted the IOT&E Report to the Secretary of Defense, and the congressional defense committees have received that report. If DoD decides to proceed to operational use of the program or to make procurement funds available for the program before the MDA's FRP/FD decision, the DOT&E's report will be submitted as soon as practicable after the DoD decision to proceed.														
ECONOMIC ANALYSIS		●				●		●	●		●	●	SEC. 811, P.L. 106-398 (Ref. (q)) DoDI 7041.03 (Ref. (y))	DoD Component
STATUTORY for MAIS. May be combined with the AoA at Milestone A. Also required at any review that is the equivalent of Milestone B or the FD Decision.														

Table Notes:

1. A dot (●) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[5]	MS C	FRP/FD Dec	OTHER		
Exit Criteria	•	•	•	•		•		•	✓	•			This instruction	MDA
Regulatory. Exit criteria are specific events and accomplishments that must be achieved before a program can proceed to the designated acquisition phase covered by the criteria. Documented in the ADM.														
FREQUENCY ALLOCATION APPLICATION (DD FORM 1494)	•	•	•	•		•			•	•			SEC. 104, P.L. 102-538 (Ref. (z)) 47 U.S.C. 305, 901-904 (Ref. (aa))	National Telecommunications and Information Administration
STATUTORY for all systems/equipment that use the electromagnetic spectrum while operating in the United States and its possessions. The DD Form 1494, Application for Equipment Frequency Allocation, is available from http://www.dtic.mil/whs/directives/forms/dd/ddforms1000-1499.htm. The STATUTORY requirement for milestone decisions is met when DD Form 1494 is submitted by the Program Manager to the appropriate reviewing and approving agencies.														
Full Funding Certification Memorandum	•	•				•			•	•	•		Para. 2f of Enc. 10 of this instruction	MDA/CAPE
Regulatory. See paragraph 2f of Enclosure 10 to this instruction. Must be signed by the CAE and the Component Chief Financial Officer.														
INDEPENDENT COST ESTIMATE (ICE)	•	•				•			•	•	•	•	10 U.S.C. 2434 (Ref. (h)) 10 U.S.C. 2334 (Ref. (h))	DCAPE or DoD Component
STATUTORY. Section 2 in Enclosure 10 provides detailed instructions for MDAPs and MAIS programs. The Milestone C requirement only applies when the milestone decision authorizes LRIP. The DCAPE will be the approval authority for ACAT ID and IAM programs; the Component will approve ACAT IC programs following review by DCAPE.														
INDEPENDENT LOGISTICS ASSESSMENT (ILA)	•								•	•	•	✓	SEC. 832, P.L. 112-81 (Ref. (v)) Sec. 5 of Enc. 6 of this instruction	CAE
STATUTORY for weapon system MDAPs only. For the FRP, the assessment is required if the decision is more than 4 years after Milestone C. Assessments after FRP will be accomplished at a minimum interval of every 5 years after Initial Operational Capability (IOC).														
Information Support Plan (ISP)	•	•	•	•				•		✓		✓	DoDI 8330.01 (Ref. (ab)) DoDI 8320.02 (Ref. (ac)) DoDI 8410.03 (Ref. (ad))	DoD Component or as delegated
Regulatory. Applicable to all IT, including NSS. A draft[4] is due for Development RFP Release; approved at Milestone B. Unless waived, updated at the Critical Design Review. The ISP of record is due prior to Milestone C; an updated ISP of record may be required during O&S. Enter data on-line at https://gtg.csd.disa.mil/; requires an account and login with a Common Access Card.														

Table Notes:

1. A dot (•) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[5]	MS C	FRP/FD Dec	OTHER		
Information Technology (IT) and National Security System (NSS) Interoperability Certification	•	•	•	•							•		DoDI 8330.01 (Ref. (ab))	JITC or DoD Component
Regulatory. Applicable to all IT, including NSS. Testing completed before or during OT&E. The Joint Interoperability Test Command (JITC) certifies interoperability of IT with joint, multinational, and/or interagency interoperability requirements. DoD Components certify all other IT. Certification must occur prior to deployment.														
Initial Capabilities Document (ICD)	•	•	•	•	•								CJCSI 3170.01 (Ref. (d)) JCIDS Manual (Ref. (r))	JROC, JCB, or Component Validation
Regulatory. The ICD is the fundamental requirements document establishing validated capability requirements; required for the MDD.														
Item Unique Identification Implementation Plan	•	•	•	•		•		✓	✓	✓			DoDI 8320.04 (Ref. (ae))	CAE or as delegated
Regulatory. Design considerations related to unique identification are included in the Systems Engineering Plan (SEP).														
Life-Cycle Mission Data Plan	•	•	•	•		•		✓	✓	✓	✓		DoDD 5250.01 (Ref. (af))	DoD Component
Regulatory; only required if the system is dependent on Intelligence Mission Data. A draft[4] update is due for Development RFP Release; approved at Milestone B.														
Life-Cycle Sustainment Plan (LCSP)	•	•	•	•		•		✓	✓	✓	✓	✓	Sec. 3 in Enc. 6 of this instruction	MDA or designee
Regulatory. A draft[4] update is due for Development RFP Release; approved at Milestone B. The LCSP is reviewed by the CAE at least every 5 years after a system's IOC. See Enclosure 6 of this instruction for details about the LCSP.														
LFT&E REPORT	•		•	•							•	•	10 U.S.C. 2366 (Ref. (h))	DOT&E
STATUTORY; Programs on the DOT&E Oversight List for LFT&E oversight only. Report is due as soon as practicable after testing is concluded. See related SURVIVABILITY AND LIVE FIRE TESTING STATUS REPORT in Table 6 in this enclosure.														
LOW-RATE INITIAL PRODUCTION (LRIP) QUANTITY	•		•	•				•	✓				10 U.S.C. 2400 (Ref. (h)) Para. 5d(6)(e) of this instruction	MDA
STATUTORY for MDAPs and ACAT II programs; Regulatory for other programs. A preliminary quantity is determined at the Development RFP Release Decision Point; the final LRIP quantity is determined at Milestone B. The LRIP quantity will be documented in the ADM. For programs on the DOT&E Oversight List, LRIP quantities must equal or exceed the numbers required for testing as identified in the approved Test and Evaluation Master Plan (TEMP).														

Table Notes:

1. A dot (•) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[5]	MS C	FRP/FD Dec	OTHER		
Operational Test Agency (OTA) Report of OT&E Results	•	•	•	•							•	•	This instruction	OTA
Regulatory. Required earlier than the FRP/FD decision if early operational assessments or operational assessments are conducted.														
OPERATIONAL TEST PLAN (OTP)	•	•	•	•								•	10 U.S.C. 2399 (Ref. (h)) Para. 3e of Enc. 5 of this instruction	DOT&E or Component equivalent
STATUTORY/Regulatory. An OTP, approved before the start of OT&E, is mandatory for all programs. Approval by DOT&E is a STATUTORY requirement for programs on the DOT&E Oversight list. DoD Component-equivalent approval is a Regulatory requirement for all other programs.														
PESHE AND NEPA/E.O. 12114 COMPLIANCE SCHEDULE	•	•	•	•					•	✓	✓		42 U.S.C. 4321-4347 (Ref. (ag)) E.O. 12114 (Ref. (ah))	CAE or as delegated
STATUTORY. The Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and National Environmental Policy Act (NEPA) / Executive Order (E.O.) 12114 Compliance Schedule is approved by the CAE. Related design considerations must be included in the SEP; related operations or sustainment considerations after Milestone C will be included in the LCSP. Not required for software programs with no hardware component.														
POST IMPLEMENTATION REVIEW (PIR)	•	•	•	•								•	40 U.S.C. 11313 (Ref. (p))	Functional sponsor
STATUTORY. Responds to statute that requires Federal Agencies to compare actual program results with established performance objectives. The PIR is a process that aggregates information needed to successfully evaluate the degree to which a capability has been achieved. The preparation of the TEMP and the MDA's decision to proceed with FRP satisfy the requirement for weapons systems. DoD Components will plan, conduct, and document the required review for IT systems and NSS post IOC (see section 4 in Enclosure 11 of this instruction). Approval by the Functional Sponsor will require coordination with the Component CIO.														
PRESERVATION AND STORAGE OF UNIQUE TOOLING PLAN	•									•		✓	SEC. 815, P.L. 110-417 (Ref. (g))	MDA
STATUTORY. Part of the LCSP. The MDA must approve the plan prior to Milestone C approval; updated only as necessary, thereafter. The plan must identify any contract clauses, facilities, and funding required to preserve and to store the unique tooling associated with the production of the MDAP hardware through the end of the service life of the end item. See paragraph 3d(3) in Enclosure 6 for details.														

Table Notes:

1. A dot (•) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[5]	MS C	FRP/FD Dec	OTHER		
Program Protection Plan (PPP)	•	•	•	•		•		✓	✓	✓	✓		DoDI 5200.39 (Ref. (ai)) DoDI 5200.44 (Ref. (aj) Para. 13a in Enc. 3, this instruction	MDA
Regulatory. A draft[4] update is due for the Development RFP Release decision and is approved at Milestone B. The PPP includes appropriate appendixes or links to required information. See section 13 in Enclosure 3 of this instruction.														
REPLACED SYSTEM SUSTAINMENT PLAN	•					•			•				10 U.S.C. 2437 (Ref. (h))	DoD Component
STATUTORY. May be submitted as early as Milestone A, but no later than Milestone B. Required when an MDAP replaces an existing system and the capability of the old system remains necessary and relevant during fielding of and transition to the new system. The plan must provide for the appropriate level of budgeting for sustainment of the old system, the schedule for developing and fielding the new system, and an analysis of the ability of the existing system to maintain mission capability against relevant threats.														
Request for Proposal (RFP)	•	•	•	•		•		•		•	•		Federal Acquisition Regulation Subpart 15.203 (Ref. (ak))	MDA is release authority
Regulatory. RFPs are issued as necessary; they include specifications and statement of work. See also Defense Federal Acquisition Regulation Supplement subpart 201.170 (Reference (al)) for the requirement for peer reviews.														
Should Cost Target	•	•	•	•		•		•	•	•	•		Para. 5d(3)(b)1 of this instruction	MDA
Regulatory. "Should Cost" is a regulatory tool designed to proactively target cost reduction and drive productivity improvement into programs. Paragraph 6e in Enclosure 2 of this instruction provides additional detail on "Should Cost."														
Spectrum Supportability Risk Assessment	•	•	•	•		•			•	•		•	DoDI 4650.01 (Ref. (am))	Component CIO or designee
Regulatory. Applicable to all systems/equipment that use the electromagnetic spectrum in the United States and in other host nations. Due at milestone reviews and prior to requesting authorization to operate (for other than testing) in the United States or in host nations.														
Systems Engineering Plan (SEP)	•	•	•	•		•		✓	✓	✓			Sec. 2 of Enc. 3 of this instruction	MDA
Regulatory. A draft[4] update is due for the Development RFP Release Decision Point; approved at Milestone B. (SEP outline provided at http://www.acq.osd.mil/se/pg/guidance.html)														

Table Notes:

1. A dot (•) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

Table 2. Milestone and Phase Information Requirements, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE[1]				LIFE-CYCLE EVENT[1,2,3]								SOURCE	APPROVAL AUTHORITY
	MDAP	MAIS	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B[5]	MS C	FRP/FD Dec	OTHER		
TECHNOLOGY READINESS ASSESSMENT (TRA)	•							•	✓	•			10 U.S.C. 2366b (Ref. (h)) 10 U.S.C. 138 (Ref. (h))	ASD(R&E)
STATUTORY. A preliminary assessment is due for the Development RFP Release Decision Point. The Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), in consultation with the Deputy Assistant Secretary of Defense (Developmental Test and Evaluation) (DASD(DT&E)), will conduct an independent review and assessment of the TRA conducted by the Program Manager and other factors to determine whether the technology in the program has been demonstrated in a relevant environment. The assessment informs the 2366b CERTIFICATION AND DETERMINATION before Milestone B (in accordance with 10 U.S.C. 2366b (Reference (h)). The TRA at Milestone C is a Regulatory requirement when Milestone C is Program Initiation.														
Technology Targeting Risk Assessment	•	•	•	•		•							This instruction DIA Directive 5000.200 (Ref. (t)) DIA Instruction 5000.002 (Ref. (u))	Validation by DIA or DoD Component
Regulatory. Prepared by the DoD Component and coordinated with the DoD Component Intelligence analytical centers per DoDI O-5240.24 (Reference (ao)) and DoDI 5200.39 (Reference (ai)). Forms the analytic foundation for Counterintelligence assessments in the associated PPP. DIA will validate the report for ACAT ID and IAM; for ACAT IC, IAC, and below, the DoD Component will be the validation authority.														
Test and Evaluation Master Plan (TEMP)	•	•	•	•		•		✓	✓	✓	✓		Enclosures 4 and 5 of this instruction	See Notes for this row.
Regulatory. A draft[4] update is due for the Development RFP Release Decision Point; approved at Milestone B. DOT&E will approve the operational test (OT) and LFT&E portions of the TEMP for DOT&E Oversight programs (10 U.S.C. 2399 (Reference (h))); the DoD Component OT authority will approve the OT portion of the TEMP for all other programs. The DASD(DT&E) will review the DT&E plans in the TEMP for each MDAP (10 U.S.C. 138 & 139b, Reference (h))) and provide a recommendation to the MDA. The MDA (or designee) will be the approval authority for the DT&E Plans in the TEMP. TEMP outline guidance for OT&E is located at http://www.dote.osd.mil/temp-guidebook/index.html.														
Validated On-line Life-cycle Threat (VOLT) Report	•	•	•	•	•	✓		✓		✓	✓		This instruction DIA Directive 5000.200 (Ref. (t)) DIA Instruction 5000.002 (Ref. (u))	DIA or DoD Component
Regulatory. MDAP and MAIS programs require a unique, system-specific VOLT Report to support capability development and program manager assessments of mission needs and capability gaps against likely threat capabilities at IOC. VOLT Reports are required for all other programs unless waived by the MDA. Programs on the DOT&E Oversight List require a unique, system-specific VOLT, unless waived by both the MDA and the DOT&E. DoD Components produce a VOLT. DIA validates the VOLT for ACAT ID or IAM programs; the DoD Component validates the VOLT for ACAT IC or IAC programs and below.														
Waveform Assessment Application	•	•	•	•					•	✓			DoDI 4630.09 (Ref. (ap))	DoD CIO
Regulatory. Application to the DoD CIO for approval of the development or modification of waveforms. Required at Milestone C if a waveform is added or modified after Milestone B.														

Table Notes:

1. A dot (•) in a cell indicates the specific applicability of the requirement to program type and life-cycle event, and represents the initial submission requirement. Moving right across a row, a checkmark (✓) indicates the requirement for updated information.
2. All of the "Life-Cycle Events" will not necessarily apply to all "Program Types."
3. Unless otherwise specified when discussed in this instruction, documentation for identified events will be submitted no later than 45 calendar days before the planned review.
4. Requires a Program Manager-, PEO-, and CAE-approved draft.
5. Information requirements that have been finalized and approved by the responsible authority in support of the Development RFP Release Decision Point do not have to be re-submitted prior to Milestone B unless changes have occurred. In that case, updated documents will be provided.
6. Incrementally Deployed Software Intensive Programs (Model #3) do not have a Milestone C and consequently are not required to satisfy the Table 2 requirements associated with that milestone.

4. APBs AND BASELINE BREACHES

a. The APB will describe the approved program. The APB represents the formal commitment of the Component and the acquisition chain of command to the MDA. Deviations from the approved APB will be immediately reported to the MDA. Deviations are specified default thresholds for schedule and cost of:

(1) Objective schedule value plus 6 months.

(2) Objective cost value plus ten percent.

b. Table 3 in this enclosure provides acquisition program baseline policy, addressing Original Baselines, Current Baselines, Baseline Deviations, and Subprograms.

c. Table 4 in this enclosure provides the statutory breach and change definitions for programs requiring APBs.

(1) The MDAP definitions for significant and critical unit cost breaches are based on unit cost growth as defined in 10 U.S.C. 2433 (Reference (h)).

(2) The MAIS program definitions for significant and critical changes are based on schedule, cost, or expected performance of the program as defined in 10 U.S.C. 2445c (Reference (h)). The section 2445c critical change definition also applies to programs that are designated as Pre-MAIS programs, and to any other AIS that are prior to a formal acquisition decision and are expected to exceed the MAIS program thresholds in Table 1, as prescribed by 10 U.S.C. 2445a.

d. The reporting requirements associated with breaches and changes are detailed in Table 6, this enclosure.

Table 3. APBs

Original Baseline Description, Original APB, or Original Estimate	For all programs: • The first APB is approved by the MDA prior to a program entering Engineering and Manufacturing Development, or at program initiation, whichever occurs later. • Serves as the current baseline description until a revised APB is approved. • Incorporates the KPPs from the CDD or CPD (if program initiation is at Milestone C). For MDAPs: • The cost/unit cost estimate parameters may be revised under 10 U.S.C. 2435 (Reference (h)) only if a breach occurs that exceeds the critical cost growth threshold for the program under 10 U.S.C. 2433 (Reference (h)). For MAIS Programs: • The Original Estimate is the initial schedule, performance, cost baseline submitted to Congress in a MAIS Annual Report (MAR), and can only be revised under 10 U.S.C. 2445c (Reference (h)) following a Critical Change Report to Congress. ▪ The Original Estimate is created from the objective schedule and cost values, and the performance threshold values in the first APB approved by the MDA. ▪ The statutory term, "development cost," will be treated the same as "total acquisition cost."
Current Baseline Description or Current APB	• May be revised only: ▪ At milestone and FRP and FD decisions; ▪ As a result of a major program restructure that is fully funded and approved by the MDA; ▪ As a result of a program deviation (breach); or ▪ At the MDA's discretion if fact of life program changes are so significant that managing to the existing baseline is not practical. • Circumstances authorizing changes are limited; revisions to the current baseline estimate/APB are not automatically authorized for program changes to cost, schedule, or performance parameters. • Revisions to the current APB will not be authorized unless there is a significant change in program parameters. • A revision to the current APB will not be authorized if proposed merely to avoid a reportable breach. • The MDA determines whether to revise the APB.
Deviations	• The Program Manager will immediately notify the MDA when the Program Manager becomes aware of an impending deviation from any parameter (cost, schedule, performance, etc.). • Within 30 business days of occurrence of the deviation, the Program Manager will submit a Program Deviation Report that informs the MDA of the reason for the deviation and planned actions. • Within 90 business days of occurrence of the deviation: ▪ The Program Manager will bring the program back within APB parameters; or ▪ The Program Manager will submit information to the OIPT to inform a recommendation to the MDA on whether it is appropriate to approve a revision to an APB. • The MDA will decide, after considering the recommendation resulting from the OIPT or equivalent Component-level review, whether it is appropriate to approve a revision to an APB.
Subprograms (10 U.S.C. 2430a (Reference (h))	When an MDAP requires the delivery of two or more categories of end items that differ significantly in form and function, or the delivery of satellites in two or more increments or blocks, subprograms may be established for baselining and reporting purposes. Once one subprogram is designated, all remaining elements (increments or components) of the program will also be appropriately organized into one or more other subprograms.

Table 4. Statutory Program Breach and Change Definitions

Significant Nunn-McCurdy Unit Cost Breaches (10 U.S.C. 2433 and 2433a (Reference (h))) Applicable to MDAPs only	• The cost growth threshold, as it relates to the current APB, is defined to be an increase of at least 15 percent over the program acquisition unit cost (PAUC) or average procurement unit cost (APUC) for the current program as shown in the current Baseline Estimate. • The cost growth threshold, as it relates to the original APB, is defined to be an increase of at least 30 percent over the PAUC or APUC for the original program as shown in the original Baseline Estimate. • Only the current APB will be revised.
Critical Nunn-McCurdy Unit Cost Breaches (10 U.S.C. 2433 (Reference (h))) Applicable to MDAPs only	• The cost growth threshold, as it relates to the current APB, is defined to be an increase of at least 25 percent over the PAUC or APUC for the program or subprogram as shown in the current Baseline Estimate/APB. • The cost growth threshold, as it relates to the original APB, is defined to be an increase of at least 50 percent over the PAUC or APUC for the program or subprogram as shown in the original Baseline Estimate/APB for the program or subprogram. • If the program or subprogram is certified rather than terminated, the most recent major milestone must be rescinded and a new milestone is required after certification. The program establishes a revised original Baseline Estimate/APB that reflects MDA certification and approval.
Significant Change (10 U.S.C. 2445c (Reference (h))) Applicable to MAIS programs only	As it relates to the original estimate (see definition in Table 3, this enclosure): • A schedule change that will cause a delay of more than 6 months but less than 1 year; • An increase in the estimated development cost or full life-cycle cost for the program by at least 15 percent, but less than 25 percent; or • A significant, adverse change in the expected performance of the MAIS to be acquired.
Critical Change (10 U.S.C. 2445c (Reference (h))) Applicable to MAIS programs and other major IT investment programs only	As it relates to the original estimate (see definition in Table 3, this enclosure): • A schedule change will cause a delay of 1 year or more; • The estimated development cost or full life-cycle cost for the program has increased 25 percent or more; or • A change in expected performance will undermine the ability of the system to perform the functions anticipated (i.e., the expected failure to meet a threshold KPP). • If a MAIS program is already baselined and the MAR shows a Milestone C event, and a Milestone C is not conducted, a critical change will occur.
Cost or Schedule Growth Notification for 2366b Certified Programs (10 U.S.C. 2366b (Reference (h))) Applicable to MDAPs only	• The Program Manager for an MDAP that has received Milestone B certification will immediately notify the MDA of any changes to the program or a designated major subprogram of such program that alter the substantive basis for the certification of the milestone decision.

5. REPORTING REQUIREMENTS

a. Tables 5 through 9 of this enclosure summarize STATUTORY and Regulatory reporting requirements, and specify when the reports are due.

(1) Table 5 presents recurring reporting requirements.

(2) Table 6 lists the reporting requirements established for exceptions, waivers, and alternative reporting.

(3) Table 7 summarizes Cost and Software Data Reporting (CSDR) System requirements.

(4) Tables 8 and 9 summarize Earned Value Management (EVM) reporting requirements.

b. In Tables 5 and 6 of this enclosure, each row identifies an information requirement and the source of the requirement. STATUTORY items and sources appear in ALL CAPS; Regulatory items and sources appear in normal text. A dot (●) in a cell indicates the applicability of the requirement to the program type for that column.

(1) Table 5 summarizes STATUTORY and Regulatory recurring reporting requirements, and specifies when the reports are due.

Table 5. Recurring Program Report

INFORMATION REQUIREMENT	PROGRAM TYPE				WHEN REQUIRED	SOURCE	REPORTING PROCEDURE
	MDAP	MAIS	ACAT II	ACAT ≤ III			
Defense Acquisition Executive Summary (DAES)	•	•			▪ For MDAPs, quarterly after initial Selected Acquisition Report (SAR) submission. ▪ For MAIS, quarterly after the program is baselined. ▪ Active programs that are 75 percent or more delivered through the production phase (or 75 percent expended if RDT&E only) will submit only a Unit Cost Reporting DAES pursuant to 10 U.S.C. 2433 (Reference (h)). ▪ For MDAPs, the DAES reporting requirement ceases after a termination SAR is submitted (90 percent of items delivered or 90 percent of funds are expended). ▪ For MAIS, DAES reporting ceases after FD is declared and a Close-out DAES is submitted.	This instruction	Program Manager
	Regulatory. Identifies program issues that may impact program cost, schedule, or performance. The DAES provides a mechanism for the Department to meet Unit Cost Reporting requirements (see page 65 of this instruction) for MDAPs. Programs should begin input of basic program information, cost estimates, and any budget data into the automated DAES module of the Defense Automated Management Information Retrieval system upon submission of the Program Objective Memorandum or Budget Estimate Submission.						
MAIS ANNUAL REPORT (MAR) TO CONGRESS		•			▪ Annually for each MAIS program and each other major IT investment program for which funds are requested by the President in the budget. ▪ This reporting requirement applies to baselined and unbaselined MAIS. ▪ Due 45 business days after the President's Budget is submitted to Congress. ▪ Requirement terminates after FD is declared and a Close-out MAR is submitted. ▪ For a MAIS that is not a national security system, if a baseline change results in a projected FD decision beyond 5 years after program initiation, the MAR must include a written determination that justifies the longer period.	10 U.S.C. 2445b (Ref. (h))	- Program Manager to Senior Officials (CAE, USD(AT&L)) - USD(AT&L) to Congress
	STATUTORY. The MAR is the basis for the quarterly reports and reports on program changes required by 10 U.S.C. 2445c (Reference (h)). IT programs employing an incremental development model (i.e., Model 3) will initiate MAR reporting for each program increment and will identify the limited deployment associated with delivery of approximately 50% of that increment's capability as a significant/breachable event.						
MAIS QUARTERLY REPORT (MQR)		•			▪ Quarterly following the initial submission of a baselined MAR and not later than 5 years after Milestone A or MDA approval of the preferred alternative. ▪ MAIS Quarterly Report reporting ceases after FD is declared and a Close-out MAIS Quarterly Report is submitted.	10 U.S.C. 2445c (Ref. (h))	Program Manager to Senior Officials (CAE, USD(AT&L)) USD(AT&L) to Congress
	STATUTORY. This report will identify any projected variance from the Original Estimate (see Table 3 for a description of the Original Estimate). Reported via the electronic DAES submission process.						
Note: A dot (•) in a cell indicates the specific applicability of the requirement to program type.							

Table 5. Recurring Program Report, Continued

INFORMATION REQUIREMENT	PROGRAM TYPE				WHEN REQUIRED	SOURCE	REPORTING PROCEDURE
	MDAP	MAIS	ACAT II	ACAT ≤ III			
SELECTED ACQUISITION REPORT (SAR)	•				▪ Program initiation (normally Milestone B except for some ship programs) or MDAP designation. ▪ Annually (as of December) for all programs and quarterly (as of March, June, and September) on an exception basis when there is: (1) a 6-month or more schedule slip in the current estimate since the prior SAR; or (2) a unit cost increase of 15 percent or more to the current APB objective or 30 percent or more to the original APB objective. ▪ SAR rebaselining after a major milestone decision (i.e., Milestone C or Milestones B and C for some ship programs). ▪ SAR reporting requirement ceases after 90 percent of items are delivered or 90 percent of planned expenditures under the program or subprogram have been made.	10 U.S.C. 2432 (Ref. (h)) 10 U.S.C. 2433 (Ref. (h)) 10 U.S.C. 2430 (Ref. (h))	Submitted by Program Manager to CAE, USD(AT&L) Submitted by USD(AT&L) to Congress
	STATUTORY. Provides the status of total program cost, schedule, and performance to Congress; provides program unit cost and unit cost breach information for a specific program. • The first SAR after the MDA's 10 U.S.C. 2366b CERTIFICATION AND DETERMINATION (see Table 2) will include the certification and determination. • Every SAR must include certification by the Secretary of the Military Department and the Chief of the armed force that program requirements are stable and funding is adequate to meet program cost, schedule, and performance objectives, and the Secretary and Chief must identify and report in the SAR any increased program risk since the last report.						
UNIT COST REPORT (UCR)	•				▪ Quarterly after initial SAR submission. ▪ Unit Cost Reporting ceases after a termination SAR is submitted (90 percent of items delivered or 90 percent of funds are expended).	10 U.S.C. 2433 (Ref. (h))	Program Manager; CAE, USD(AT&L) (see Note, this row)
	STATUTORY. Reported via the DAES submission process. The Program Manager provides the report quarterly to USD(AT&L) for the 3 quarters excluding the quarter with the annual SAR submission. The USD(AT&L) provides the report to Congress annually (included in SAR submission).						

Note: A dot (•) in a cell indicates the specific applicability of the requirement to program type.

(2) Table 6 summarizes STATUTORY and Regulatory requirements established for exceptions, waivers, and alternative management and reporting. The table specifies the conditions and point in time when each report is required.

Table 6. Exceptions, Waivers, and Alternative Management and Reporting Requirements

INFORMATION REQUIREMENT FOR WAIVER OR EXCEPTION	PROGRAM TYPE				WHEN REQUIRED	SOURCE	REPORTING PROCEDURE
	MDAP	MAIS	ACAT				
			II	≤ III			
ALTERNATE LFT&E PLAN	•		•	•	A DoD Component-approved final draft plan is due 45 calendar days prior to the Development RFP Release decision. The final plan is required at Milestone B or as soon as practicable after program initiation.	10 U.S.C. 2366 (Ref. (h))	Program Manager to DOT&E
	STATUTORY. Only required for programs on the DOT&E oversight list for LFT&E with or requesting a waiver from full-up, system-level testing.						
CONGRESSIONAL NOTIFICATION OF CONDUCTING DT&E WITHOUT AN APPROVED TEMP	•				Notification is required not later than 30 days after any decision is made for a lead DT&E Organization to conduct any developmental T&E activities for the MDAP without an approved TEMP.	SEC. 904, P.L. 112-239 (Ref. (l))	Program Manager to USD(AT&L) to Congress
	STATUTORY. The Program Manager will prepare the notification and submit to USD(AT&L). The notification must include a written explanation of the basis for the decision and a timeline for getting an approved plan in place. A copy of the notification will be provided to DOT&E.						
CONGRESSIONAL NOTIFICATION OF CORE LOGISTICS COMMERCIAL ITEM EXCEPTION	•	•	•	•	Due upon determination that the system or equipment is a commercial item.	10 U.S.C. 2464 (Ref. (h))	DAE to Congress
	STATUTORY. The commercial item exception notice must include the justification for the determination.						
CONGRESSIONAL NOTIFICATION OF CRITICAL COST BREACH	•				STATUTORY. Due within 45 calendar days of a Program Deviation Report	10 U.S.C. 2433 (Ref. (h)) 10 U.S.C. 2433a (Ref. (h))	Service Secretary to Congress
CONGRESSIONAL NOTIFICATION OF MAIS CANCELLATION OR SIGNIFICANT REDUCTION IN SCOPE		•			Due 60 calendar days prior to an MDA cancellation decision.	SEC. 806, P.L. 109-163 (Ref. (aq))	USD(AT&L) to Congress
	STATUTORY. Provides congressional notification of an MDA decision to cancel or significantly reduce the scope of a fielded or post-Milestone C MAIS program.						
Note: A dot (•) in a cell indicates the specific applicability of the requirement to program type.							

Table 6. Exceptions, Waivers, and Alternative Management and Reporting Requirements, Continued

INFORMATION REQUIREMENT FOR WAIVER OR EXCEPTION	PROGRAM TYPE				WHEN REQUIRED	SOURCE	REPORTING PROCEDURE
	MDAP	MAIS	ACAT				
			II	≤ III			
CONGRESSIONAL NOTIFICATION OF MDA REVISION OF THE ACQUISITION STRATEGY	•	•	•		STATUTORY. Notification reports an MDA-directed change to the program or system to the congressional defense committees.	10 U.S.C. 2431a (Ref. (h))	MDA to DAE to Congress
CONGRESSIONAL NOTIFICATION OF MDA WAIVER OF 10 U.S.C. 2366b REQUIREMENTS	•				Due no later than 30 calendar days after the waiver is authorized.	10 U.S.C. 2366b (Ref. (h))	Program Manager to MDA to Congress
	STATUTORY. The MDA may waive any of the 10 U.S.C. 2366b, Milestone B certification and determination requirements before Milestone B (except that the cost benefit analysis for some satellite systems described in subsection (a)(4) in 10 U.S.C. 2366b MAY NOT be waived) if the MDA determines that, but for such a waiver, the DoD would be unable to meet critical national security objectives. If the MDA authorizes a waiver: (1) The waiver, the determination, and the reasons for the determination will be submitted in writing to the congressional defense committees within 30 calendar days after the waiver is authorized. (2) The MDA will review the program not less often than annually to determine the extent to which the program otherwise satisfies the 10 U.S.C. 2366b Milestone B certification and determination components, until such time as the MDA determines that the program satisfies all of the certification and determination components. (3) Any budget request, budget justification material, budget display, reprogramming request, SAR, or other budget documentation or performance report submitted by the Secretary of Defense to the President regarding an MDAP receiving a waiver to 2366b certification will prominently and clearly indicate that such program has not fully satisfied the certification and determination requirements for Milestone B, until such time that the MDA makes a determination that the program has satisfied all such certification and determination requirements.						
CONGRESSIONAL NOTIFICATION OF MDAP SUBPROGRAM DESIGNATION(S)	•				Due not less than 30 calendar days before approval of a subprogram APB.	10 U.S.C. 2430a (Ref. (h))	DAE to Congress
	STATUTORY. Reports the DAE's determination that (1) different categories of end items in an MDAP, or (2) delivery increments or blocks of a satellite program warrant separate acquisition reporting and will be designated Major Subprograms. Table 3 in this enclosure provides additional policy regarding subprograms.						
CONGRESSIONAL NOTIFICATION OF PRESERVATION AND STORAGE OF UNIQUE PRODUCTION TOOLING WAIVER	•				Due before Milestone C or at any time before the end of the item's service life if the Secretary determines the waiver is in the best interest of the DoD.	SEC. 815 of P.L. 110-417 (Ref. (g))	DAE to Congress
	STATUTORY. Based on the Secretary's written determination that such a waiver is in the best interest of the Department of Defense.						
Note: A dot (•) in a cell indicates the specific applicability of the requirement to program type.							

Table 6. Exceptions, Waivers, and Alternative Management and Reporting Requirements, Continued

INFORMATION REQUIREMENT FOR WAIVER OR EXCEPTION	PROGRAM TYPE				WHEN REQUIRED	SOURCE	REPORTING PROCEDURE
	MDAP	MAIS	ACAT				
			II	≤ III			

CONGRESSIONAL NOTIFICATION OF SECRETARY OF DEFENSE WAIVER OF ACQUISITION LAWS TO ACQUIRE VITAL NATIONAL SECURITY CAPABILITIES	•	•	•	•	STATUTORY. The Secretary of Defense waiver authority discussed in paragraph 5a(2)(c) of this instruction is available upon a determination that:
					– The acquisition of the capability is in the vital national security interest of the United States.
					– The application of the law or regulation to be waived would impede the acquisition of the capability in a manner that would undermine the national security of the United States.
					– The underlying purpose of the law or regulation to be waived can be addressed in a different manner or at a different time.
					Waiver authority is limited to the statutory and regulatory provisions addressing the establishment of the requirement or specification; research, development, test, and evaluation; production, fielding, and sustainment; or solicitation, selection of sources, and award of contracts for the capability to be acquired. Statutory limitations prevent the waiver of the requirements of Section 806 of P.L. 114-92, or any provision of law either imposing civil or criminal penalties or governing the proper expenditures of appropriated funds.
					Congressional notification is due at least 30 days before exercising waiver authority. Notification includes:
					– An explanation of why the acquisition is vital to U.S. national security interests; and
					– Identification of each provision of law or regulation to be waived; and for each provision:
					  – An explanation of how the provision would impede the acquisition and undermine U.S. national security interests; and
					  – How and when the underlying purpose of the provision will be addressed.
					The Secretary, in exercising this authority, will designate a senior official to be personally responsible and accountable for the rapid and effective acquisition and deployment of the needed capability. The Secretary will provide the designated official such authority as the Secretary determines necessary to achieve this objective, and may use the waiver authority described above for this purpose.
						SEC. 806, P.L. 114-92 (Ref. (e))	Secretary of Defense to Congressional Defense Committees

Note: A dot (•) in a cell indicates the specific applicability of the requirement to program type.

Table 6. Exceptions, Waivers, and Alternative Management and Reporting Requirements, Continued

INFORMATION REQUIREMENT FOR WAIVER OR EXCEPTION	PROGRAM TYPE				WHEN REQUIRED	SOURCE	REPORTING PROCEDURE
	MDAP	MAIS	ACAT				
			II	≤ III			
CONGRESSIONAL NOTIFICATION OF SIGNIFICANT COST BREACH	•				STATUTORY. Due within 45 calendar days of a Program Deviation Report	10 U.S.C. 2433 (Ref. (h))	Service Secretary to Congress
COST-TYPE DEVELOPMENT CONTRACT DETERMINATION	•				Due at the Development RFP Release Decision Point upon MDA conditional approval of a cost type contract selected for a development program.	SEC. 818, P.L. 109-364 (Ref. (k))	MDA Written Determination
	STATUTORY. The MDA may authorize the use of a cost-type contract for a development program only upon a written determination that: (1) the program is so complex and technically challenging that it would not be practicable to reduce program risk to a level that would permit the use of a fixed-price contract; and (2) the complexity and technical challenge of the program are not the result of a failure to meet the requirements of 10 U.S.C. 2366b (Reference (h)). The MDA's written determination will include an explanation of the level of program risk, and, if the MDA determines that the program risk is high, the steps that have been taken to reduce program risk and the reasons for proceeding with Milestone B approval despite the high level of program risk. In considering program risk to determine whether a cost or fixed price engineering and manufacturing development contract meets the statutory requirement, the MDA will consider the following: the firmness of the capability requirements and maturity of the technology required; the experience level of potential offerors; and the capacity of industry to absorb potential overruns and the business case for industry to do so.						
COST-TYPE PRODUCTION CONTRACT CERTIFICATION	•				Applicable to contracts for the production of MDAPs: ▪ Entered into, on, or after October 1, 2014, and for which ▪ The USD(AT&L) has granted an exception to the prohibition against using a cost-type contract for MDAP production.	SEC. 811, P.L. 112-239 (Ref. (l))	USD(AT&L) to Congress
	STATUTORY. The USD(AT&L) may only grant the exception: (1) in the case of a particular cost-type contract; (2) if the USD(AT&L) provides written certification to the congressional defense committees that a cost-type contract is needed to provide a required capability in a timely and cost-effective manner; (3) the USD(AT&L) takes affirmative steps to make sure that the use of cost-type pricing is limited to only those line items or portions of the contract where such pricing is needed to achieve the purposes of the exception; and, (4) an explanation of the steps identified under clause (3), accompanies the written certification under clause (2).						

Note: A dot (•) in a cell indicates the specific applicability of the requirement to program type.

Table 6. Exceptions, Waivers, and Alternative Management and Reporting Requirements, Continued

INFORMATION REQUIREMENT FOR WAIVER OR EXCEPTION	PROGRAM TYPE				WHEN REQUIRED	SOURCE	REPORTING PROCEDURE
	MDAP	MAIS	ACAT				
			II	≤ III			
DT&E EXCEPTION REPORTING	•				Case 1: When an MDAP proceeds with implementing a TEMP that includes a developmental test plan disapproved by DASD(DT&E). Case 2: When an MDAP proceeds to IOT&E following an assessment by DASD(DT&E) that the program is not ready for operational testing.	SEC. 904, P.L. 112-239 (Ref. (l))	Program Manager to USD(AT&L) to Congress
	STATUTORY ▪ The report due for Case 1 must include a description of the specific aspects of the DT&E plan determined to be inadequate; an explanation of why the program disregarded the DASD(DT&E)'s recommendations; and identification of the steps taken to address the concerns of the DASD(DT&E). ▪ The report due for Case 2 must include an explanation of why the program proceeded to IOT&E despite the DASD(DT&E) findings; a description of the aspects of the TEMP that had to be set aside to enable the program to proceed to IOT&E; a description of how the program addressed the specific areas of concern raised in the assessment of operational test readiness; and a statement of whether IOT&E identified any significant shortcomings in the program. ▪ The USD(AT&L) will compile all such exception reports and annually, not later than 60 days after the end of each fiscal year through 2018, submit a report on each case to the congressional defense committees.						
LEAD SYSTEM INTEGRATOR EXCEPTION CERTIFICATION	•	•	•		Due if the MDA grants an exception.	10 U.S.C. 2410p (Ref. (h))	DAE to Congress
	STATUTORY. Satisfies the statutory restrictions applicable to exceptional use of a lead systems integrator (see paragraph 5d(9)(g)1 of this instruction for additional discussion).						
LFT&E WAIVER FROM FULL-UP, SYSTEM-LEVEL TESTING	•		•	•	Due at Milestone B or as soon as practicable after program initiation.	10 U.S.C. 2366 (Ref. (h))	DAE to Congress
	STATUTORY. Only required for programs on the DOT&E Oversight List for LFT&E that are requesting a waiver from full-up, system-level testing.						
MAIS CRITICAL CHANGE REPORT AND CERTIFICATION		•			Not later than 60 calendar days after a MAIS Quarterly Report indicating a critical change is due to the Senior Official.	10 U.S.C. 2445c (Ref. (h))	Senior Official through OSD to Congress
	STATUTORY. When the Senior Official is not an individual within OSD, the Critical Change Report will be signed by the Senior Official and provided to the cognizant OSD official for transmittal to Congress. The signed Critical Change Report should be provided to the appropriate OSD official with draft transmittal letters addressed to the congressional defense committees no later than 5 working days before expiration of the 60-day period.						
MAIS SIGNIFICANT CHANGE NOTIFICATION		•			Not later than 45 calendar days after a MAIS Quarterly Report indicating a significant change is due to the Senior Official.	10 U.S.C. 2445c (Ref. (h))	Senior Official to Congress
	STATUTORY. The notification must be coordinated with the USD(AT&L), the Deputy Chief Management Officer, or the DoD CIO, as appropriate, before sending to Congress.						
Note: A dot (•) in a cell indicates the specific applicability of the requirement to program type.							

Table 6. Exceptions, Waivers, and Alternative Management and Reporting Requirements, Continued

INFORMATION REQUIREMENT FOR WAIVER OR EXCEPTION	PROGRAM TYPE				WHEN REQUIRED	SOURCE	REPORTING PROCEDURE
	MDAP	MAIS	ACAT				
			II	≤ III			
Management of Joint DoD and Director of National Intelligence (DNI) Programs	•	•	•	•	When the DoD participates in a National Intelligence Program acquisition that is wholly or in the majority funded by the DNI.	MoA, Ref. (ar)	None
	Joint DoD and DNI oversight of wholly and majority National Intelligence Program-funded acquisition programs will be conducted in accordance with Intelligence Community Policy Guidance 801.1 (Reference (as)) and the Memorandum of Agreement (MoA) between the DNI and the Secretary of Defense (Reference (ar)).						
NUNN-MCCURDY ASSESSMENT AND CERTIFICATION	•				When a Service Secretary has reported an increase in cost that equals or exceeds the critical cost growth threshold.	10 U.S.C. 2433a (Ref. (h))	USD(AT&L)
	STATUTORY. The remedial actions required when a program or subprogram experiences critical cost growth.						
Program Deviation Report	•	•	•	•	Regulatory. • Due within 30 business days of occurrence of the deviation. • Initial MDA notification is due immediately upon becoming aware of an impending deviation.	Para. 4a of this enclosure	Program Manager to MDA
SURVIVABILITY AND LIVE FIRE TESTING STATUS REPORT	•	•	•	•	Due as soon as practicable after a decision to proceed to operational use or to make procurement funds available for a covered system is made prior to Milestone C approval.	10 U.S.C. 2366 (Ref. (h))	DOT&E to Congress
	STATUTORY. DOT&E LFT&E Oversight programs only, including those that respond to urgent needs. Program also requires the LFT&E Report (see LFT&E Report row on page 56 of this enclosure).						
Note: A dot (•) in a cell indicates the specific applicability of the requirement to program type.							

c. Table 7 summarizes CSDR requirements, and specifies when the reports are due.

Table 7. CSDR System Requirements

REQUIRED REPORT	WHEN REQUIRED	SOURCE
Contractor Cost Data Report (CCDR)	• All major contracts[1] and subcontracts, regardless of contract type, for ACAT I and IA programs and pre-MDAP and pre-MAIS programs subsequent to Milestone A approval, valued at more than $50 million[2] (then-year dollars). Reporting is continued even if a program has been downgraded from an ACAT I or IA, unless waived by DCAPE. • Not required for contracts priced below $20 million (then-year dollars). • The CCDR requirement on high-risk or high-technical-interest contracts priced between $20 million and $50 million is left to the discretion of the DoD Program Manager and/or the Deputy Director, Cost Assessment (DDCA). • Required for major components (i.e., government furnished equipment) of an ACAT I program that are managed by the Services as ACAT II or ACAT III, and if the contract value exceeds $50 million or if determined to be a high-risk or high-technical-interest contract priced between $20 million and $50 million by the Program Manager and/or the DDCA. • Not required under the following conditions, provided the DoD Program Manager requests and obtains approval for a reporting waiver from the DDCA: procurement of commercial systems or procurement of non-commercial systems bought under competitively-awarded firm fixed-price contracts, as long as competitive conditions continue to exist.	DoD 5000.04-M-1 (Reference (at)) This instruction
Software Resources Data Report (SRDR)	• All major contracts[1] and subcontracts, regardless of contract type, for contractors developing or producing software elements within ACAT I and IA programs and pre-MDAP and pre-MAIS programs subsequent to Milestone A approval for any software development element with a projected software effort greater than $20 million (then-year dollars). • The SRDR requirement on high-risk or high-technical-interest contracts priced below $20 million is left to the discretion of the DoD Program Manager and/or the DDCA.	DoD 5000.04-M-1 This instruction
Contractor Business Data Report	• Required for all contractor business entities (e.g., plant, site, or business unit) responsible for contracts with CSDR requirements.	DoD 5000.04-M-1
Contractor Sustainment Report	• All major contracts[1] and subcontracts, regardless of contract type, valued at more than $50 million[2] (then-year dollars).	SEC. 832 of P.L. 112-81 (Reference (v)) DoD 5000.04-M-1

Notes:

1. For CSDR purposes, the term "contract" (or "subcontract") may refer to the entire standalone contract, to a specific task or delivery order, to a series of tasks or delivery orders, to a contract line item number, or to a series of line item numbers within a contract. The intent is to capture data on contractual efforts necessary for cost estimating purposes irrespective of the particular contract vehicle used. All contracts for the procurement of end items, software, or services to support the acquisition of MDAP and MAIS programs (or ACAT II and III programs which meet the above thresholds) must include the Data Item Descriptions (DIDs) and Contract Data Requirements Lists necessary for the reporting of CSDR data.
2. For CSDR purposes, contract value will represent the estimated price at contract completion (i.e., initial contract award plus all expected authorized contract changes) and be based on the assumption that all contract options will be exercised.
3. CSDR is further discussed in section 4 of Enclosure 10.

d. Paragraph 6c in Enclosure 2 provides an overview of EVM. This paragraph details application requirements and reporting requirements.

(1) EVM Application. Table 8 summarizes EVM application requirements. EVM is applied to cost reimbursable or incentive contracts, inclusive of options, with 18 months or greater period of performance and based on the nature of the work scope.

Table 8. EVM Application Requirements

Contract Value	Applicability	Notes	Source
< $20M	EVM not required; may be applied at PM discretion based on risk to the Government	Requires business case analysis and MDA approval	Part 7 of OMB Circular A-11 (Reference (c)); DFARS 234.201 (Reference (al)); This instruction
≥ $20M & < $100M	EVM Required; contractor is required to have an EVM system (EVMS) that complies with the guidelines in EIA-748*	The Government reserves the right to review a contractor's EVMS when deemed necessary to verify compliance	
≥ $100M	EVM Required; contractor is required to have an EVMS that has been determined to be in compliance with the guidelines in EIA-748*	The Contractor will provide access to all pertinent records and data requested by the Contracting Officer or duly authorized representative as necessary to permit initial and ongoing Government compliance reviews to ensure that the EVMS complies, and continues to comply, with the guidelines in EIA-748*.	

Additional Information

For ACAT ID and IAM programs, OSD USD(AT&L) Performance Assessments and Root Cause Analyses (PARCA), in coordination with the CAE or designee, will review proposed contract work scope for EVM applicability and provide a recommendation to the DAE/MDA for a determination of EVM applicability. For all other ACAT levels, the CAE, or designee, will review and determine EVM applicability. If EVM is determined to apply, then threshold application in this table is utilized or a waiver from the CAE is required. If, based on the nature of the work, EVM is determined not to apply, then EVM is not placed on contract.

Applying EVM outside the thresholds and criteria above, to include application on firm, fixed-price (FFP) contracts, FFP task orders, or FFP delivery orders, a cost-benefit analysis will be conducted, MDA approval is required, and the results provided to the contracting officer for documentation in the contract file.

The term "contracts" includes contracts, subcontracts, intra-government work agreements, and other agreements.

For indefinite delivery, indefinite quantity (IDIQ) contracts, inclusion of EVM requirements is based on the estimated ceiling of the total IDIQ contract, and then is applied to the individual task/delivery orders, or group(s) of related task/delivery orders, that meet or are expected to meet the conditions of contract type, value, duration, and work scope. The EVM requirements should be placed on the base IDIQ contract and applied to the task/delivery orders, or group(s) of related task/delivery orders. "Related" refers to dependent efforts that can be measured and scheduled across task/delivery orders.

The Integrated Baseline Review is required when EVM is determined to be applicable.

The initiation of an over-target baseline or over-target schedule must be approved by the Government program manager.

Application thresholds are in then-year dollars.

* EIA-748 = Electronic Industries Alliance (EIA) 748-C (Reference (au))

(2) EVM Reporting. Table 9 summarizes EVM reporting requirements. The Integrated Program Management Report (IPMR) contains data for measuring cost and schedule performance on DoD acquisition contracts.

Table 9. EVM Reporting Requirements

Contract Value	Applicability	Notes	Source
< $20M	Not required	IPMR Should be used if cost and/or schedule reporting is requested by the PMO	IPMR DID DI-MGMT-81861A*
≥ $20M & < $50M	Required monthly when EVM requirement is on contract	Formats 2, 3, and 4 may be excluded from the contract data requirements list (CDRL) at program manager discretion based on risk	
≥ $50M	Required monthly when EVM requirement is on contract	All Formats must be included in the CDRL	
Additional Information			
For ACAT I contracts, task orders, and delivery orders, IPMR data will be delivered to the EVM Central Repository. The IPMR can be tailored to collect cost and/or schedule data for any contract regardless of whether EVM is required. For information on tailoring the IPMR, refer to the DoD IPMR Implementation Guide (Reference (cj)). Formats and reporting requirements for the IPMR are determined and managed by USD(AT&L) through the office of PARCA. Reporting thresholds are in then-year dollars. DI-MGMT-81861A = Data Item Management-81861 (Reference (av))			

6. CCA COMPLIANCE. Table 10 summarizes the requirements levied on all programs that acquire IT, including NSS, at any ACAT level. Amplifying guidance for CCA compliance is detailed in section 3 of Enclosure 11.

Table 10. CCA Compliance

Actions Required to Comply With the CCA (Subtitle III of title 40 of U.S. Code (Reference (p)))[1]	Applicable Program Documentation[2]
1. Make a determination that the acquisition supports core, priority functions of the DoD.[3]	ICD, IS ICD, or urgent need requirements documents
2. Establish outcome-based performance measures linked to strategic goals.[3, 4]	ICD, IS ICD, CDD, CPD, AoA, APB[7]
3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of commercial off-the-shelf technology.[3, 4]	ICD, IS ICD, Concept of Operations, AoA, Business Process Reengineering
4. Determine that no private sector or government source can better support the function.[4, 5]	Acquisition Strategy, AoA
5. Conduct an analysis of alternatives.[4, 5]	AoA
6. Conduct an economic analysis that includes a calculation of the return on investment; or for non-AIS programs, conduct a life-cycle cost estimate.[4, 5]	Component Cost Estimate, Component Cost Position, Program Economic Analysis for MAIS programs
7. Develop clearly established measures and accountability for program progress.[4]	Acquisition Strategy, APB[7], TEMP[7]
8. Ensure that the acquisition is consistent with the DoD Information Enterprise policies and architecture, to include relevant standards.[4]	CDD NR-KPP, CPD NR-KPP, ISP
9. Ensure that the program has a Cybersecurity Strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.[4]	Cybersecurity Strategy, Program Protection Plan, Risk Management Framework Security Plan
10. Ensure, 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.[4]	Acquisition Strategy
11. Register Mission-Critical and Mission-Essential systems with the DoD CIO.[4, 6]	DoD Information Technology Portfolio Repository

1. Table 2 in this enclosure indicates when the program manager must report CCA compliance.
2. 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. Include page(s) and paragraph(s), where appropriate. Urgent needs may cite the associated urgent needs documentation to demonstrate CCA compliance, e.g., the Course of Action and/or the network connection documentation.
3. 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.
4. These actions are also required to comply with section 811 of Public Law 106-398 (Reference (q)).
5. For NSS, these requirements apply to the extent practicable (40 U.S.C. 11103 (Reference (p)) discusses NSS).
6. Mission-Critical Information System. A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act (Subtitle III of title 40 of U.S. Code (Reference (p))), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of mission critical will be made by a DoD Component head, a Combatant Commander, or their designee. A financial management IT system will be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller) (USD(C)).) A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System."

   Mission-Essential Information System. A system that meets the definition of "information system" in 44 U.S.C. 3502 (Reference (aw)), that the acquiring DoD Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission-essential will be made by a DoD Component head, a Combatant Commander, or their designee. A financial management IT system will be considered a mission-essential IT system as defined by the USD(C).) A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System."
7. The APB and TEMP may be submitted in draft to expedite program assessment.

ENCLOSURE 2

PROGRAM MANAGEMENT

1. PURPOSE. This enclosure describes policies applicable to Program Managers, PEOs, and Component Acquisition Executives (CAEs) for defense acquisition programs. The enclosure also includes a range of applicable statutory and regulatory program management policies and responsibilities.

2. ACQUISITION CHAIN OF COMMAND. The chain of command for acquisition programs runs upward from the Program Manager, through the PEO to the CAE, and for Acquisition Category (ACAT) I and IA and other programs so designated, to the Defense Acquisition Executive (DAE). The responsibility and authority for program management, to include program planning and execution, is vested in these individuals. Staff and other organizations provide support to this chain of command. "Program Management" in this enclosure refers to this chain of command.

3. ASSIGNMENT OF PEOs

a. CAEs will assign acquisition program responsibilities to a PEO for all ACAT I and IA and sensitive classified programs, or for any other program determined by the CAE to require dedicated executive management.

b. A PEO must be experienced, qualified, and certified in program management, including having been a Program Manager for an ACAT I or IA program comparable to the programs he or she will be responsible for as PEO.

c. The PEO will be dedicated to executive management of assigned programs and will not have other command responsibilities.

d. The DAE may waive the provisions of paragraphs 3a, 3b, and/or 3c on a case-by-case basis.

e. The CAE will make this assignment no later than program initiation, or within 3 months of program cost estimates reaching the dollar threshold for an ACAT I or IA program. CAEs may determine that a specific Program Manager will report directly, without being assigned to a PEO, whenever such direct reporting is appropriate due to program size or criticality. The CAE will notify the DAE of the decision to have a Program Manager report directly to the CAE, and request a waiver from the DAE of the requirement to appoint a PEO.

f. Acquisition program responsibilities for programs not assigned to a PEO or a direct-reporting program manager may be assigned to a commander of a systems, logistics, or materiel command. A program may be transferred from a PEO or direct reporting program manager to a

commander of a systems, logistics, or materiel command only after the program or increment of capability has passed Initial Operational Capability and has been approved for Full-Rate Production or Full Deployment.

4. ASSIGNMENT OF PROGRAM MANAGERS

a. A Program Manager will be designated for each acquisition program by the appropriate CAE. This designation will be prior to Milestone A (as the Technology Maturation and Risk Reduction Phase is being planned) or the milestone associated with the entry phase specified by the MDA at the Materiel Development Decision.

b. It is essential that Program Managers be defense acquisition professionals with experience managing relevant engineering development or technology efforts, and who have a deep knowledge of contracting, financial systems, industry perspectives, and user needs. Unless a waiver is granted by the DAE or CAE, a Program Manager will be experienced in similar acquisition programs and Defense Acquisition Workforce Improvement Act Level III certified in program management. Waivers should be granted rarely.

c. By law, any Program Manager for an ACAT I or IA program assigned before Milestone B will be assigned at least through Milestone B approval. Any ACAT I or IA Program Manager assigned immediately following Milestone B approval will be assigned until initial operational capability is achieved. Program Managers outside of these periods will be assigned for at least 4 years or until the completion of the phase of the program that occurs closest in time to the date on which the person has served in the position for 4 years. Waivers for these tenure requirements can be granted by the respective CAE if it is determined that either of the above described periods is so long that it would not be appropriate for a single individual to serve as Program Manager for the entire period. CAEs will assist with the collection of data on waivers granted to assist OSD in recognizing status and trends.

d. The measure of a Program Manager's performance should be the successful execution of a phase that the Program Manager has submitted for approval. DoD Components should, whenever possible, assign incoming Program Managers to programs approximately 6 months **before** a major milestone so that they are responsible for approval of a plan that they will execute. Early arrival will assist them in monitoring and, where applicable, influencing the plan to be approved at the upcoming milestone review.

e. Program Managers for the period leading to Milestone B approval will have responsibilities that include:

(1) Bringing technologies to maturity and identifying the manufacturing processes that will be needed to carry out the program.

(2) Ensuring continuing focus during program development on meeting stated mission requirements and other requirements of the Department of Defense.

(3) Recommending trade-offs between program cost, schedule, and performance for the life-cycle of the program.

(4) Developing a business case for the program.

(5) Ensuring that appropriate information is available to MDA to complete the Certification and Determination required by 10 U.S.C. 2366b (Reference (h)) and make the Milestone B decision.

f. The Program Manager responsibilities for an MDAP immediately after Milestone B include:

(1) Consultations on the addition of new program requirements that would be inconsistent with the Program Management Agreement (PMA) directed by paragraph 4g in this enclosure.

(2) Recommendation of trade-offs between cost, schedule, and performance, consistent with the PMA.

(3) Development of interim goals and milestones to achieve the parameters established in the PMA.

g. PMA agreements establish achievable and measurable annual plans that are fully resourced and reflect the approved program.

(1) To maximize management accountability, ACAT I and IA Program Managers are required to enter into a PMA with the manager's immediate supervisor for such program within 6 months of assignment. Specifically, this agreement will:

(a) Establish expected parameters for the cost, schedule, and performance of the program consistent with the business case for the program.

(b) Provide the supervisor's commitment to the level of funding and resources required to meet such parameters.

(c) Provide the assurance of the Program Manager that such parameters are achievable and that the Program Manager will be accountable for meeting such parameters.

(2) PMAs will be updated annually or more frequently if the conditions that formed the basis of the agreement (requirements, funding, or execution plans) have changed.

(3) The PMA format is at the discretion of the Component and may be as simple as a cover memo for all signatories with the Acquisition Program Baseline, budget exhibits, and capabilities documents attached.

h. Program managers for ACAT II and other significant non-major programs will be assigned for not less than 3 years.

5. PROGRAM OFFICE STRUCTURE AND ORGANIZATIONS

a. Program Office Structure. It is program management's responsibility to fully understand the skills and capacity required for successful program execution and for the CAE to provide those skills to ensure that the program executes successfully. For new starts, Program Managers will establish program offices as soon as possible after their selection. Program offices for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs will be staffed in key leadership positions with military or DoD civilian employees qualified in accordance with DoD Instruction 5000.66 (Reference (ax)), as amended by the Under Secretary of Defense for Acquisition, Technology, and Logistics' Policy Memorandum, Key Leadership Positions and Qualification Criteria, (Reference (ay)). Key leadership positions include the Program Manager and Deputy Program Manager, and the additional positions identified in Reference (ay).

b. Joint Program Office Organization

(1) A Joint Program Office will be established when a defense acquisition program involves the satisfaction of validated capability requirements from multiple DoD Components and/or international partners, and is funded by more than one Component or partner during any phase of the acquisition process In most joint programs, a lead Component will be designated to manage the acquisition process and act as the acquisition agent for the participating DoD Components. The participating Components, those with a requirement for the program's products, support and participate with the lead DoD Component in managing the acquisition process. Joint programs will be managed in accordance with the provisions of a memorandum of agreement, and with the lead DoD Component's acquisition procedures and acquisition chain of command, unless directed otherwise by the DAE.

(2) DoD Components will neither terminate nor substantially reduce participation in joint MDAP and MAIS programs without capability requirements validation authority review and DAE approval. The DAE may require a DoD Component to continue some or all funding, as necessary, to sustain the joint program in an efficient manner, despite approving a request to terminate or reduce participation. Memorandums of agreement between DoD Components should address termination or reduced participation by any parties to the agreement. Substantial reduction will be determined by the MDA in coordination with the requirements validation authority, and is defined as a funding or quantity decrease that impacts the viability of the program and/or significantly increases the costs to the other participants in the program.

6. PROGRAM MANAGEMENT RESPONSIBILITIES. Program managers direct the development, production, and deployment of new defense systems. Management activities will be designed to achieve the cost, schedule, and performance parameters specified in the MDA-

approved Acquisition Program Baseline (APB). The following tools will be used to facilitate effective program planning and execution.

a. Acquisition Strategies

(1) Overview. The Program Manager will develop and execute an approved Acquisition Strategy. This document is the Program Manager's plan for program execution across the entire program life cycle. It is a comprehensive, integrated plan that identifies the acquisition approach and key framing assumptions, and describes the business, technical, and support strategies that the Program Manager plans to employ to manage program risks and meet program objectives. The strategy evolves over time and should continuously reflect the current status and desired goals of the program. The Acquisition Strategy defines the relationship between the acquisition phases and work efforts, and key program events such as decision points and reviews. The strategy must reflect the Program Manager's understanding of the business environment; technical alternatives; small business strategy; costs, risks and risk mitigation approach; contract awards; the incentive structure; test activities; production lot or delivery quantities; operational deployment objectives; opportunities in the domestic and international markets; foreign disclosure, exportability, technology transfer, and security requirements; and the plan to support successful delivery of the capability at an affordable life-cycle price, on a realistic schedule. Acquisition Strategies are baseline plans for the execution of the program and should be prepared and submitted in time to obtain approval to support more detailed planning and the preparation of Requests for Proposal. The Acquisition Strategy is an approved plan; it is not a contract. Minor changes to the plan reflected in the Acquisition Strategy due to changed circumstances or increased knowledge are to be expected and do not require MDA pre-approval. Major changes, such as contract type or basic program structure, do require MDA approval prior to implementation. All changes should be noted and reflected in an update at the next program decision point or milestone.

(2) Business Approach and Risk Management. The business approach detailed in the Acquisition Strategy should be designed to manage the risks associated with the product being acquired. It should fairly allocate risk between industry and the government. The approach will be based on a thorough understanding of the risks associated with the product being acquired and the steps that should be taken to reduce and manage that risk. The business approach should be based on market analysis that considers market capabilities and limitations. The contract type and incentive structure should be tailored to the program and designed to motivate industry to perform in a manner that rewards achievement of the government's goals. The incentives in any contract strategy should be significant enough to clearly promote desired contractor behavior and outcomes the government values, while also being realistically attainable. When risk is sufficiently reduced, Program Managers will consider the use of fixed-price contracts when the use of such contracts is cost-effective.

(3) Competition. The Acquisition Strategy will address how program management will create and sustain a competitive environment, from program inception through sustainment. Program management should use both direct competition at various levels and indirect means to create competitive environments that encourage improved performance and cost control. Decisions made in the early phases of the acquisition process can either improve or reduce

program management's ability to maintain a competitive environment throughout the life cycle of a program. Strategies to be considered include: competitive prototyping, dual sourcing, and a modular open systems approach (MOSA) that enable competition for upgrades, acquisition of complete technical data packages, and competition at the subsystem level. This also includes providing opportunities for small business and organizations employing the disabled.

(4) IP Strategy. Program management must establish and maintain an IP Strategy to identify and manage the full spectrum of IP and related issues (e.g., technical data and computer software deliverables, patented technologies, and appropriate license rights) from the inception of a program and throughout the life cycle. The IP Strategy will describe, at a minimum, how program management will assess program needs for, and acquire competitively whenever possible, the IP deliverables and associated license rights necessary for competitive and affordable acquisition and sustainment over the entire product life cycle, including by integrating, for all systems, the IP planning elements required by subpart 207.106 (S-70) of the Defense Federal Acquisition Regulation Supplement (Reference (al)) for major weapon systems and subsystems thereof. The IP Strategy will be updated throughout the entire product life cycle, initially as part of the Acquisition Strategy, and during the Operations and Support Phase as part of the Life-Cycle Sustainment Plan.

(5) MOSA. Program management is responsible for evaluating and implementing a MOSA to the maximum extent feasible and cost effective. This approach integrates technical requirements with contracting mechanisms and legal considerations to support a more rapid evolution of capabilities and technologies throughout the product life cycle through the use of architecture modularity, open systems standards, and appropriate business practices. The Acquisition Strategy for the system should identify where, why, and how a MOSA will or will not be used in the program.

b. Program Baseline Development and Management. The Program Manager is responsible for developing the APB. The APB (see section 4 in Enclosure 1 of this instruction) is a summary of the program cost, schedule, and performance baselines, and is the fundamental binding agreement between the MDA, the CAE (if applicable), the PEO, and the Program Manager. The APB serves as the basis for reporting to the MDA through the DoD management information system.

c. Earned Value Management (EVM). EVM is one of DoD's and industry's most powerful program planning and management tools. It is normally used in conjunction with cost plus and fixed-price incentive contracts with discrete work scope. The purpose of EVM is to ensure sound planning and resourcing of all tasks required for contract performance. It promotes an environment where contract execution data is shared between project personnel and government oversight staff and in which emerging problems are identified, pinpointed, and acted upon as early as possible. EVM provides a disciplined, structured, objective, and quantitative method to integrate technical work scope, cost, and schedule objectives into a single cohesive contract baseline plan called a Performance Measurement Baseline for tracking contract performance. Table 8 in Enclosure 1 summarizes EVM applicability and Table 9 summarizes EVM reporting requirements.

d. Risk Management

(1) The Program Manager is responsible for implementing effective risk management and tracking to include the identification of all known risks, key assumptions, probability of occurrence, consequences of occurrence (in terms of cost, schedule, and performance) if not mitigated, analysis of mitigation options, decisions about actions to mitigate risk, and execution of those actions. Risk management is proactive and should be focused on the actions that will be taken and resources that will be allocated to reduce both the likelihood and consequences of risks being realized. Effective risk management is not just risk identification and tracking.

(2) Program Managers are responsible for prioritizing programmatic risks and mitigating them within program constraints. Most of program management is about the process of eliminating programmatic risk over the life of the program. Formal risk management is one tool to accomplish that objective. Top program risks and associated risk mitigation plans will be detailed in the program acquisition strategy and presented at all relevant decision points and milestones. At a minimum, the Program Manager will consider the following risk management techniques:

(a) Prototyping at the system, subsystem, or component level; and competitive prototyping, where appropriate.

(b) Modeling and simulation (detailed in section 9 in Enclosure 3), to include the need for development of any new modeling and simulation tools to support a comprehensive risk management and mitigation approach.

(c) Technology demonstrations and decision points to discipline the insertion of planned technologies into programs or the selection of alternative technologies (sections 3 through 8 in Enclosure 3 provide additional discussions of technical management activities).

(d) Multiple design approaches.

(e) Alternative designs, including designs that meet requirements but with reduced performance.

(f) Phasing program activities or related technology development efforts to address high-risk areas early.

(g) Manufacturability (section 10 in Enclosure 3 addresses manufacturing and producibility in more detail).

(h) Industrial base availability and capabilities (further discussed in section 8 of this enclosure).

(i) Independent risk assessments by outside subject matter experts.

(j) Providing schedule and funding margins for identified risks.

e. Cost Baseline Control and Use of "Should Cost" Management

(1) For MDAPs and MAIS programs, it is DoD policy to budget to the DCAPE Independent Cost Estimate (ICE) unless an alternative estimate is specifically approved by the MDA. However, program managers will develop a Should Cost estimate as a management tool to control and reduce cost. Program managers should not allow the ICE to become a self-fulfilling prophecy. Should Cost is a management tool designed to proactively target cost reduction and drive productivity improvement into programs. Should Cost management challenges managers to identify and achieve savings below budgeted most-likely costs. Should Cost analysis can be used during contract negotiations (particularly for sole source procurements), and throughout program execution including sustainment. Program managers are to proactively seek out and eliminate low-value-added or unnecessary elements of program cost, to motivate better cost performance wherever possible, and to reward those that succeed in achieving those goals. Should Cost estimates used in contract negotiations will be based on the government's reasonable expectation of successful contractor performance, consistent with the contractor's previous experience and other relevant data. Realized Should Cost savings will be retained at the lowest organizational level possible and applied to priority needs. Should Cost applies to programs in all ACATs, in all phases of the product's life cycle, and to all elements of program cost.

(2) Program management will develop, own, track, and report against Should Cost targets. Estimates and results will be provided at milestone reviews and at specified decision points. For MDAPs and MAIS programs, Program Managers will report progress against Should Cost goals at Defense Acquisition Executive Summary reviews.

7. INTERNATIONAL ACQUISITION AND EXPORTABILITY

a. International Acquisition and Exportability Considerations. Program management is responsible for integrating international acquisition and exportability considerations into the program's Acquisition Strategy at each major milestone or decision point. Program management will consider the potential demand and likelihood of cooperative development or production, Direct Commercial Sales, or Foreign Military Sales early in the acquisition planning process; and consider U.S. export control laws, regulations, and DoD policy for international transfers when formulating and implementing the acquisition strategy; in accordance with DoD Instruction 2040.02 (Reference (az)). Where appropriate, program managers will pursue cooperative opportunities and international involvement throughout the acquisition life cycle to enhance international cooperation and improve interoperability in accordance with DoD Instruction 2010.06 (Reference (ba)).

b. International Cooperative Program Management

(1) An international cooperative program (ICP) is any acquisition program or technology project that includes participation by the U.S. and one or more foreign nations, through an international agreement, during any phase of a system's life cycle. When applicable, program

staff members are encouraged to use streamlined agreement procedures. All ICPs will consider applicable U.S.-ratified materiel international standardization agreements in accordance with Chairman of the Joint Chiefs of Staff Instruction 3170.01I (Reference e)), and fully comply with applicable foreign disclosure, export control, technology transfer, program protection, and security requirements. Programs containing classified information will have a Delegation of Disclosure Authority Letter or other written authorization issued by the DoD Component's cognizant foreign disclosure office prior to entering discussions with potential foreign partners.

(2) DoD Components will notify and obtain the approval of the DAE for MDAP and MAIS programs before terminating or substantially reducing participation in ICPs under signed international agreements. The DAE may require the DoD Component to continue to provide some or all of the funding for that program. A substantial reduction is defined as a funding or quantity decrease that impacts the viability of the program and/or significantly increases the costs to the other participants in the program.

c. Waivers. Any foreign military sales or direct commercial sales of major defense equipment prior to successful completion of operational test and evaluation require Under Secretary of Defense for Acquisition, Technology and Logistics approval (i.e., a Yockey Waiver). (Details of this requirement are found in paragraph C5.1.8.3. in the Security Assistance Management Manual (Reference (bb))).

8. INDUSTRIAL BASE ANALYSIS AND CONSIDERATIONS

a. Industrial base analysis is a continuing process with two primary components, both of which rely in part on information from program management. The first gathers program specific industrial base information to create the appropriate acquisition strategy for a program; the second engages throughout the life cycle of the program to provide feedback and updates. The objective is to ensure that the Department can:

(1) Identify and support economic and stable development and production rates.

(2) Identify and mitigate industrial capabilities risks such as single points of failure and unreliable suppliers.

(3) Avoid, to the maximum extent practicable, lock-in to sole and single source suppliers at any tier.

(4) Support resilience of critical defense industrial base capabilities.

(5) Support DoD's management of defense procurement surges and contractions.

b. Program management is responsible for incorporating industrial base analysis, to include capacity and capability considerations, into acquisition planning and execution. The industrial base considerations should be documented in the Acquisition Strategy and include identification of industrial capability problems (e.g., access to raw materials, export controls, production

capabilities) that have the potential to impact the DoD near- and long-term, and identification of mitigation strategies that are within the scope of program management. Program management provided information is aggregated with other sources of information at CAE and DAE levels to inform Service and Department level industrial base decisions.

9. LIFE-CYCLE MANAGEMENT OF INFORMATION AND DATA PROTECTION. Program managers will ensure that all program office documents and records, regardless of media or security classification, are created, maintained, used, and disposed of or preserved in accordance with DoD 5015.02-STD (Reference (bc)).

ENCLOSURE 3

SYSTEMS ENGINEERING

1. PURPOSE. This enclosure describes the policies and procedures regarding the application of systems engineering to defense acquisition. Systems engineering provides the integrating technical processes and design leadership to define and balance system performance, life-cycle cost, schedule, risk, and system security within and across individual systems and programs. The Program Manager, with support from the Lead Systems Engineer, will embed systems engineering in program planning and execution to support the entire system life cycle.

2. SYSTEMS ENGINEERING PLAN

a. Program Managers will prepare a Systems Engineering Plan (SEP) as a management tool to guide the systems engineering activities on the program. The SEP will be submitted to the MDA for approval before each milestone review, beginning with Milestone A. At each milestone and at the Development RFP Release Decision Point, the SEP will support the acquisition strategy, including the program interdependencies, and communicate the overall technical approach to balance system performance, life-cycle cost, and risk in addressing warfighter needs. The SEP will describe the program's overall technical approach, including key technical risks, processes, resources, organization, metrics, and design considerations. It will also detail the timing and criteria for the conduct of technical reviews. The use of mandatory tables in the SEP is intended to support more detailed technical planning during the system life cycle in order to provide effective management and control of the program's technical progress and the execution of risk mitigation activities. The SEP will address system integration with existing and approved architectures and capabilities. Program managers will identify and manage risk of external dependencies which are outside their span of control in order to ensure timely design, development, deployment, and sustainment of the system. Program managers will document interface requirements and interface products to track interdependent program touch points. The technical planning documented in the SEP will guide the details in the program's schedule. Program managers should include the SEP (either an approved Plan or a draft Plan) in the RFP as either guidance or a compliance document depending on the maturity of the plan and the acquisition strategy.

b. The Deputy Assistant Secretary of Defense (Systems Engineering) (DASD(SE)) will review the SEP for all Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs.

(1) DoD Components will submit the SEPs to the DASD(SE) at least 45 calendar days before the scheduled DAB milestone review.

(2) For Milestone B, the DoD Component-approved draft SEP will be provided to the DASD(SE) 45 calendar days prior to the Development RFP Release Decision Point. If continuing engineering activities such as the Preliminary Design Review (PDR) create the need

for substantive changes to the SEP, it will be revised and resubmitted for review before Milestone B. Program managers will update the SEP as needed after contract award to reflect any changes due to the contractor's technical approach and details not available prior to contract award. The updated SEP will be provided to the DASD(SE).

3. DEVELOPMENT PLANNING. The decisions to enter into the acquisition process, to mature technologies, and to begin system design must be based on early systems engineering analysis and assessments and a strong technical foundation.

a. In preparation for the Materiel Development Decision, and to inform an Analysis of Alternatives (AoA), the DoD Components will conduct early systems engineering analyses and conduct an assessment of how the proposed candidate materiel solution approaches are technically feasible and have the potential to effectively address capability gaps, desired operational attributes, and associated external dependencies.

b. During the Materiel Solution Analysis Phase, the Components will conduct early systems engineering analyses, informed by and in support of the AoA, to support selection of a preferred materiel solution and development of the draft Capability Development Document (or equivalent requirements document).

c. In preparation for Milestone A, and to provide the technical basis for executing the Technology Maturation and Risk Reduction Phase, the Program Manager will conduct an early systems engineering assessment of technical risks and develop the technical approach for acquiring the product. This technical assessment will include software, integration, manufacturing, and reliability risks. The results will be incorporated in the SEP for Milestone A.

4. SYSTEMS ENGINEERING TRADE-OFF ANALYSES

a. During the acquisition life cycle, the Program Manager will conduct systems engineering trade-off analyses to assess system affordability and technical feasibility to support requirements, investment, and acquisition decisions. Systems engineering trade-off analyses will depict the relationships between system life-cycle cost and the system's performance requirements, design parameters, and delivery schedules. The analysis results should be reassessed over the life cycle as system requirements, design, manufacturing, test, and logistics activities evolve and mature.

b. In support of the validation of the Capability Development Document (or equivalent requirements document), the Program Manager will conduct a systems engineering trade-off analysis showing how cost varies as a function of system requirements (including KPPs), major design parameters, and schedule. The results will be provided to the MDA and will identify major affordability drivers and show how the program meets affordability constraints.

5. TECHNICAL RISK AND OPPORTUNITY MANAGEMENT. Technical risk management should address risk identification, analysis, mitigation planning, mitigation implementation, and

tracking. Technical risks should be quantified and implications reflected in the program's Integrated Master Schedule and Integrated Master Plan. The Program Manager should also work with the applicable science and technology communities and Component acquisition leadership to influence technology investment planning. The goal is to both mitigate risks and create opportunities for technology development outcomes that could have a positive impact on meeting performance objectives as well as thresholds. Program risks, and opportunities as applicable, will be assessed at technical reviews and will include specific cost and schedule implications.

6. TECHNICAL PERFORMANCE MEASURES AND METRICS. The Program Manager will use technical performance measures and metrics to assess program progress. Analysis of technical performance measures and metrics, in terms of progress against established plans, will provide insight into the technical progress and risk of a program.

7. TECHNICAL REVIEWS. Program Managers will:

a. Conduct technical reviews of program progress for systems in development as a basis for transitioning between phases within the development plan of work. Reviews will be event-driven and based on the review entrance criteria as documented in the SEP.

b. Program Managers will plan for and conduct design reviews as needed to manage program planning and execution. Design review planning will be included in the SEP. Any program that is not initiated at Milestone C will include the following design reviews:

(1) PDR. The PDR assesses the maturity of the preliminary design supported by the results of requirements trades, prototyping, and critical technology demonstrations. The PDR will establish the allocated baseline and confirm that the system under review is ready to proceed into detailed design (development of build-to drawings, software code-to documentation, and other fabrication documentation) with acceptable risk. For MDAPs and MAIS programs, a system-level PDR assessment will be conducted and provided to the MDA. For Acquisition Category (ACAT) ID and ACAT IAM programs, DASD(SE) will conduct the PDR assessment to inform the MDA of technical risks and the program's readiness to proceed into detailed design. The Program Manager will make the program information needed for this assessment available and provide for DASD(SE) participation in the program's PDR process. For ACAT IC and ACAT IAC programs, the Component Acquisition Executive (CAE) will conduct the PDR assessment.

(2) Critical Design Review (CDR). The CDR assesses design maturity, design build-to or code-to documentation, and remaining risks and establishes the initial product baseline. It will be used as the decision point that the system design is ready to begin developmental prototype hardware fabrication or software coding with acceptable risk. For MDAPs and MAIS programs, a system-level CDR assessment will be conducted and the results will be provided to the MDA. For ACAT ID and IAM programs, DASD(SE) will conduct the CDR assessment to inform the MDA of the program's design maturity, technical risks, and the program's readiness to begin

developmental prototype hardware fabrication and/or software coding with acceptable risk. As the basis for preparation of a CDR assessment, the Program Manager will provide for DASD(SE) participation in the program's CDRs and the Program Manager will make needed program artifacts and information available. For ACAT IC and IAC programs, the CAE will conduct the CDR assessment.

8. CONFIGURATION MANAGEMENT. The Program Manager will use a configuration management approach to establish and control product attributes and the technical baseline across the total system life cycle. This approach will identify, document, audit, and control the functional and physical characteristics of the system design; track any changes; provide an audit trail of program design decisions and design modifications; be integrated with the SEP and technical planning; and be consistent with the IP Strategy. At completion of the system level CDR, the Program Manager will assume control of the initial product baseline, to the extent that the competitive environment permits.

9. MODELING AND SIMULATION. The Program Manager will integrate modeling and simulation activities into program planning and engineering efforts. These activities will support consistent analyses and decisions throughout the program's life cycle. Models, data, and artifacts will be integrated, managed, and controlled to ensure that the products maintain consistency with the system and external program dependencies, provide a comprehensive view of the program, and increase efficiency and confidence throughout the program's life cycle.

10. MANUFACTURING AND PRODUCIBILITY. The Program Manager will ensure manufacturing and producibility risks are identified and managed throughout the program's life cycle. Beginning in the Materiel Solution Analysis Phase, manufacturing readiness and risk will be assessed and documented in the SEP. By the end of the Technology Maturation and Risk Reduction Phase, manufacturing processes will be assessed and demonstrated to the extent needed to verify that risk has been reduced to an acceptable level. During the Engineering and Manufacturing Development Phase, Program Managers will assess the maturity of critical manufacturing processes to ensure they are affordable and executable. Prior to a production decision, the Program Manager will ensure manufacturing and producibility risks are acceptable, supplier qualifications are completed, and any applicable manufacturing processes are or will be under statistical process control.

11. SOFTWARE. The development and sustainment of software can be a major portion of the total system life-cycle cost and should be considered at every decision point in the acquisition life cycle. A phased software development approach using testable software builds and/or fieldable software increments enables the developers to deliver capability in a series of manageable, intermediate products to gain user acceptance and feedback for the next build or increment, and reduce the overall level of risk. The SEP should address the following: software unique risks; inclusion of software in technical reviews; identification, tracking, and reporting of metrics for software technical performance, process, progress, and quality; software safety and

security considerations; and software development resources. Software assurance vulnerabilities and risk based remediation strategies will be assessed, planned for, and included in the Program Protection Plan (PPP).

12. RELIABILITY AND MAINTAINABILITY (R&M)

a. The Program Manager will formulate a comprehensive R&M program using an appropriate strategy to ensure reliability and maintainability requirements are achieved. The program will consist of engineering activities including for example: R&M allocations, block diagrams and predictions; failure definitions and scoring criteria; failure mode, effects and criticality analysis; maintainability and built-in test demonstrations; reliability testing at the system and subsystem level; and a failure reporting, analysis, and corrective action system maintained through design, development, production, and sustainment. The R&M program is an integral part of the systems engineering process.

b. For MDAPs, the Program Manager will prepare a preliminary Reliability, Availability, Maintainability and Cost Rationale (RAM-C) Report in support of the Milestone A decision. This report provides a quantitative basis for reliability requirements, and improves cost estimates and program planning. This report will be attached to the SEP at Milestone A, and updated in support of the Development RFP Release Decision Point, Milestone B, and Milestone C.

c. Reliability growth curves (RGCs) will reflect the reliability growth strategy and be employed to plan, illustrate, and report reliability growth. RGCs will be included in the SEP at Milestone A and updated in the draft SEP submitted at the Development RFP Release Decision Point and in the final approved SEP and Test and Evaluation Master Plan submitted at Milestone B. RGCs will be stated in a series of intermediate goals and tracked through fully integrated, system-level test and evaluation events at least until the reliability threshold is achieved. If a single curve is not adequate to describe overall system reliability, curves for critical subsystems should also be employed.

d. Program offices, developmental test agencies, and operational test agencies will assess the reliability growth required for the system to achieve its reliability threshold during testing, and report the results of those assessments to the acquisition chain of command including the MDA.

e. Reliability growth will be monitored and reported throughout the acquisition process. Program managers will report the status of R&M objectives and/or thresholds as part of the formal design review process, and during systems engineering technical reviews or other reviews. RGCs will be employed to report reliability growth status at Defense Acquisition Executive Summary reviews.

13. PROGRAM PROTECTION. Program protection is the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle. Where a DoD capability advantage derives from a DoD-unique

or critical technology, program protection manages and controls the risk that the enabling technology will be lost to an adversary. Where a DoD capability advantage derives from the integration of commercially available or custom-developed components, program protection manages the risk that design vulnerabilities or supply chains will be exploited to destroy, modify, or exfiltrate critical data, degrade system performance, or decrease confidence in a system. Program protection also supports international partnership building and cooperative opportunities objectives by enabling the export of capabilities without compromising underlying U.S. technology advantages.

a. PPP. Program managers will employ system security engineering practices and prepare a PPP to guide their efforts and the actions of others to manage the risks to critical program information and mission-critical functions and components associated with the program. The PPP will be submitted for MDA approval at each milestone review, beginning with Milestone A. For programs with the Defense Acquisition Executive as the MDA, PPPs will be submitted to the DASD(SE) not less than 45 calendar days prior to the relevant review. For Milestone B, the DoD Component-approved draft PPP will be provided to the DASD(SE) 45 days prior to the Development RFP Release Decision Point. Program managers should include the PPP in RFPs, and prepare updates to the PPP after any contract award to reflect the contractor's approved technical approach and the details or necessary changes that were not available or appropriate prior to contract award.

b. Countermeasures. Program managers will describe in their PPP the program's critical program information and mission-critical functions and components; the threats to and vulnerabilities of these items; the plan to apply countermeasures to mitigate associated risks; and planning for exportability and potential foreign involvement. Countermeasures should include anti-tamper, exportability features, security (including cybersecurity, operations security, information security, personnel security, and physical security), secure system design, supply chain risk management, software assurance, anti-counterfeit practices, procurement strategies, and other mitigations in accordance with DoD Instruction 5200.39 (Reference (ai)), DoD Instruction 5200.44 (Reference (aj)), and DoD Instruction 8500.01 (Reference (x)). Program managers will submit the program's Cybersecurity Strategy as part of every PPP. Countermeasures should mitigate or remediate vulnerabilities throughout the product life cycle, including design, development, developmental and operational testing, operations, sustainment, and disposal. Program Managers will implement the use of automated software vulnerability detection and analysis tools and ensure risk-based remediation of software vulnerabilities is addressed in PPPs, included in contract requirements, and verified through continued use of such tools and testing (as required by section 933 of P.L. 112-239, Reference (l)).

14. MODULAR OPEN SYSTEMS APPROACH. Program Managers, with support from the Lead Systems Engineer, are responsible for applying modular approaches in product designs where feasible and cost-effective. They are also responsible for acquiring data and IP that are both appropriate (10 U.S.C. 2320 (Reference (h)) and essential to achieving the expected benefits (see paragraphs 6a(4) and 6a(5) in Enclosure 2 of this instruction for additional information on MOSA and IP). Modular designs coupled with an appropriately open business model provide a

valuable mechanism for continuing competition and incremental upgrades, and to facilitate reuse across the joint force.

15. CORROSION PREVENTION AND CONTROL. The Program Manager will identify and evaluate corrosion considerations throughout the acquisition and sustainment phases that reduce, control, or mitigate corrosion in sustainment. The Program Manager will perform corrosion prevention and control planning and include corrosion control management and design considerations for corrosion prevention and control in the SEP and Life-Cycle Sustainment Plan. The Program Manager will ensure that corrosion control requirements are included in the design and verified as part of test and acceptance programs.

16. ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH (ESOH). The Program Manager will integrate ESOH risk management into the overall systems engineering process for all engineering activities throughout the system's life cycle. As part of risk reduction, the Program Manager will eliminate ESOH hazards where possible, and manage ESOH risks where hazards cannot be eliminated. The Program Manager will use the methodology in MIL-STD-882E (Reference (bd)). Program Managers will assess the status of ESOH risks and acceptance decisions at technical reviews. Acquisition program reviews and fielding decisions will address the status of all high and serious risks. Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, the Program Manager will document that the associated risks have been accepted by the following acceptance authorities: the CAE for high risks, PEO-level for serious risks, and the Program Manager for medium and low risks. The user representative, as defined in MIL-STD-882E, must be part of this process throughout the life cycle and will provide formal concurrence prior to all serious- and high-risk acceptance decisions. For joint programs, the ESOH risk acceptance authorities reside within the lead DoD Component. Program managers will document the ESOH planning in the SEP and will document the results of the planning implementation in the Programmatic ESOH Evaluation (PESHE) and the compliance schedule required by the National Environmental Policy Act (NEPA) (Reference (ag)) and Executive Order (E.O.) 12114 (Reference (ah)) (NEPA/E.O. 12114).

a. PESHE. The Program Manager, regardless of ACAT level, will prepare and maintain a PESHE to document data generated by ESOH analyses conducted in support of program execution. The PESHE will include at a minimum identification of ESOH risks and their status; and, identification of hazardous materials, wastes, and pollutants (discharges/emissions/noise) associated with the system and its support as well as the plans for minimization and/or safe disposal.

b. NEPA/ E.O. 12114. The Program Manager will prepare and maintain a NEPA/E.O. 12114 Compliance Schedule that covers all known or projected system-related activities that may trigger compliance requirements including testing, fielding, and support of the system. The Compliance Schedule will incorporate the test schedules and locations identified in the Test and Evaluation Master Plan to enable consideration of potential impacts to the environment and completion of appropriate documentation in accordance with DoD Component implementing

procedures. The Program Manager will conduct and document the NEPA/E.O. 12114 analyses for which the Program Manager is the action proponent, and provide system-specific analyses and data to support other organizations' NEPA/E.O. 12114 analyses of system-related activities for which the Program Manager is not the proponent. The CAE (for joint programs, the CAE of the lead DoD Component) or designee, is the approval authority for system-related NEPA/E.O. 12114 documentation for which the Program Manager is the proponent.

c. Mishap Investigation Support. The Program Manager will support system-related Class A and B mishap investigations by providing analyses of hazards that contributed to the mishap and recommendations for materiel risk mitigation measures, especially those that minimize human errors, as required by 10 U.S.C. 2255 (Reference (h)).

17. INSENSITIVE MUNITIONS. For all systems containing energetics, the Program Manager will comply with Insensitive Munitions requirements in accordance with the DoD and Component policy requirements (as required by 10 U.S.C. 2389 (Reference (h)).

18. ITEM UNIQUE IDENTIFICATION. The Program Manager will plan for and implement item unique identification to identify and track applicable major end items, configuration-controlled items, and government-furnished property to enhance life-cycle management of assets in systems acquisition and sustainment, and to provide more accurate asset valuation and property accountability. Item unique identification planning and implementation will be documented in an Item Unique Identification Implementation Plan linked to the program's SEP. DoD Instruction 8320.04 (Reference (ae)) provides the standards for unique item identifiers.

19. SPECTRUM SUPPORTABILITY. Program managers are responsible for ensuring compliance of their programs with U.S. and host nation electromagnetic spectrum regulations, in accordance with 47 U.S.C. section 305 and sections 901 through 904 (Reference (aa)) and section 104 of P.L.102-538 (Reference (z)). Program managers will also submit written determinations to the Component Chief Information Officer (CIO) or equivalent that the electromagnetic spectrum necessary to support the operation of the system during its expected life cycle is or will be available in accordance with DoD Instruction 4650.01 (Reference (am)). These determinations will be the basis for recommendations provided to the MDA by the Component CIO or equivalent.

20. PROGRAM SUPPORT ASSESSMENTS (PSAs). The Office of the DASD(SE) will conduct independent, cross-functional PSAs of MDAPs' and MAIS programs, and other program's as directed by the DAE, to assess technical management and systems engineering progress and plans. PSAs are for the purpose of assisting program managers' technical planning, and to improve execution by sharing best practices and lessons learned from other programs. The DASD(SE) will advise technical authorities on the incorporation of best practices for systems engineering from across the DoD. Risk identification and risk mitigation assistance will be one focus of the PSAs. These reviews may also support acquisition milestones, decision

reviews, or be conducted in response to technical issues on ACAT ID and IAM programs. These assessments are intended to help program managers shape their programs' technical planning and improve execution by providing actionable recommendations and identifying engineering and integration risks, as well as potential mitigation activities. The DoD Components will provide access to all program records and data including technical review artifacts and classified, unclassified, competition sensitive, and proprietary information that the DASD(SE) considers necessary to carry out these assessments in accordance with 10 U.S.C. 139b (Reference (h)).

ENCLOSURE 4

DEVELOPMENTAL TEST AND EVALUATION (DT&E)

1. PURPOSE. This enclosure provides policy and procedure for developmental test and evaluation of defense acquisition programs.

2. OVERVIEW

a. Program managers use DT&E activities to manage and mitigate risks during development, to verify that products are compliant with contractual and operational requirements, and to inform decision makers throughout the program life cycle. DT&E provides program engineers and decision makers with knowledge to measure progress, identify problems, and to characterize system capabilities and limitations, and manage technical and programmatic risks. DT&E results are also used as exit criteria to ensure adequate progress prior to investment commitments or initiation of phases of the program, and as the basis for contract incentives.

b. DT&E starts with capability requirements and continues through product development, delivery, and acceptance; transition to operational test and evaluation (T&E); production; and operations and support. Consideration of developmental test and evaluation in the requirements and systems engineering processes ensures that capability requirements are measurable, testable, and achievable. Identifying and correcting deficiencies early is less costly than discovering system deficiencies late in the acquisition process.

c. The Program Manager will use a Test and Evaluation Master Plan (TEMP) as the primary planning and management tool for the integrated test program. Whenever feasible, testing will be conducted in an integrated fashion to permit all stakeholders to use data in support of their respective functions. Integrated testing requires the collaborative planning and collaborative execution of test phases and events to provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders, particularly the systems engineering, developmental (both contractor and government) and operational T&E communities. The Program Manager will establish an integrated test planning group consisting of empowered representatives of test data producers and consumers (to include all applicable stakeholders) to ensure collaboration and to develop a strategy for robust, efficient testing to support systems engineering, evaluations, and certifications throughout the acquisition life cycle.

d. The Program Manager will identify the test resources needed to execute the DT&E program to acquire the data that will be used to understand program progress, identify issues, verify compliance, and balance cost and performance. Test resource requirements will be included in the TEMP.

e. The Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) will monitor the development test and evaluation program activities of Major Defense Acquisition Programs (MDAPs) and review the DT&E plans for those programs in the

TEMP. The DASD(DT&E) will provide a recommendation to approve or disapprove the MDAP DT&E plans as well as advise the relevant technical authorities for these programs on the incorporation of best practices for developmental test from across the Department. For ACAT IA, and ACAT II and below programs, the Component Acquisition Executive will designate a DT&E organization to monitor DT&E activities and recommend approval or disapproval of the DT&E plans in the TEMP. For all programs, the MDA (or designee) will approve or disapprove the DT&E plans in the TEMP. DASD(DT&E) authorities, responsibilities, and functions are described in 10 U.S.C. 139b (Reference (h)).

3. T&E MANAGEMENT

a. Program managers for MDAPs and MAIS programs will designate a Chief Developmental Tester in accordance with 10 U.S.C. 139b and 1706 (Reference (h)). The Chief Developmental Tester will be responsible for coordinating the planning, management, and oversight of all DT&E activities; maintaining insight into contractor activities; overseeing the T&E activities of other participating government activities; and helping the Program Manager make technically informed, objective judgments about contractor and government T&E planning and results. The Chief Developmental Tester will chair the integrated test planning group.

b. Program managers for MDAPs will designate a government test agency to serve as the lead DT&E organization in accordance with 10 U.S.C. 139b. The lead DT&E organization will be responsible for providing technical expertise on T&E issues to the Chief Developmental Tester; conducting DT&E activities as directed by the Chief Developmental Tester or his or her designee; supporting certification and accreditation activities when feasible; assisting the Chief Developmental Tester in providing oversight of contractors; and assisting the Chief Developmental Tester in reaching technically informed, objective judgments about contractor and government T&E planning and results. For all other programs, a lead DT&E organization should be used, when feasible, and identified in the TEMP.

c. The designation of a Chief Developmental Tester and lead DT&E organization will be made as soon as practicable after the program office is established.

d. The Program Manager will use the TEMP as the primary planning and management tool for all test activities starting at Milestone A. The Program Manager will prepare and update the TEMP as needed and to support acquisition milestones or decision points. For the Full-Rate Production Decision Review or the Full Deployment Decision and thereafter, the MDA may require TEMP updates or addendums to plan for additional testing. Section 5 in Enclosure 5 of this instruction has additional policy for the TEMP in the context of operational testing.

e. Program managers for programs under DASD(DT&E) oversight will designate a T&E Working-level Integrated Product Team (WIPT) (also known as an Integrated Test Team), as soon as practicable after the Materiel Development Decision. The T&E WIPT develops and tracks the T&E program in all phases. The T&E WIPT will include empowered representatives of test data stakeholders such as Systems Engineering, DT&E, Operational T&E, Live Fire T&E, Product Support, the user, the intelligence community, and applicable certification authorities.

f. The Program Manager will take full advantage of DoD ranges, labs, and other resources. Systems have become more complex and resource constraints often force tradeoffs in the type and scope of testing that can be performed. The DT&E budget and schedule must allow testing that adequately verifies performance to contractual requirements in a controlled environment and to operational requirements.

4. DT&E ACTIVITIES

a. DT&E activities will start when requirements are being developed to ensure that key technical requirements are measurable, testable, and achievable.

b. A robust DT&E program includes a number of key activities to provide the data and assessments for decision making. The DT&E program will:

(1) Verify achievement of critical technical parameters and the ability to achieve KPPs, and assess progress toward achievement of critical operational issues.

(2) Assess the system's ability to achieve the thresholds prescribed in the capabilities documents.

(3) Provide data to the Program Manager to enable root cause determination and to identify corrective actions.

(4) Validate system functionality.

(5) Provide information for cost, performance, and schedule tradeoffs.

(6) Assess system specification compliance.

(7) Report on program progress to plan for reliability growth and to assess reliability and maintainability performance for use during key reviews.

(8) Identify system capabilities, limitations, and deficiencies.

(9) Include T&E activities to detect cyber vulnerabilities within custom and commodity hardware and software.

(10) Assess system safety.

(11) Assess compatibility with legacy systems.

(12) Stress the system within the intended operationally relevant mission environment.

(13) Support cybersecurity assessments and authorization, including Risk Management Framework security controls.

(14) Support the interoperability certification process.

(15) Document achievement of contractual technical performance, and verify incremental improvements and system corrective actions.

(16) Assess entry criteria for Initial Operational Test and Evaluation (IOT&E) and Follow-On Operational Test and Evaluation.

(17) Provide DT&E data to validate parameters in models and simulations.

(18) Assess the maturity of the chosen integrated technologies.

5. DT&E PLANNING CONSIDERATIONS

a. The Program Manager will:

(1) Use the TEMP as the primary test planning and management document.

(2) The TEMP will:

(a) Contain an integrated test program summary and master schedule of all major test events or test phases.

(b) Include an event-driven testing schedule that will allow adequate time to support pre-test predictions; testing; post-test analysis, evaluation, and reporting; reconciliation of predictive models; and adequate time to support execution of corrective actions in response to discovered deficiencies. The schedule should allow sufficient time between DT&E and IOT&E for rework, reports, and analysis and developmental testing of critical design changes.

(c) Be a source document when developing the RFP.

(d) Guide how contractor proposals will address program test needs such as: test articles; T&E data rights; government access to the Failure Reporting, Analysis and Corrective Action System and other test outcome repositories; built-in test and embedded instrumentation data (including software log files); contractor verification requirements; government use of contractor-conducted T&E; government review and approval of contractor T&E plans; government witness of contractor test events; and government review of contractor evaluations. See section 5 in Enclosure 5 of this instruction for additional details.

(e) Include identification of all contractor and government system level reliability testing needed to support initial reliability planning estimates. The Program Manager will include the reliability developmental evaluation methodology for reliability critical items. The

military departments/program managers will collect and retain data from the T&E of the reliability and maintainability of major weapon systems to inform system design decisions, provide insight into sustainment costs, and inform estimates of operating and support costs for such systems.

(f) Starting at Milestone B, include one or more reliability growth curves (RGCs).

1. If a single curve is not adequate to describe the overall system reliability, curves for critical subsystems with rationale for their selection will be provided.

2. For software (in any system), the TEMP will include projected and observed software maturity metrics. For hardware acquisitions, Milestone B RGCs will consist of observed (when available) and projected reliability.

3. RGCs will be stated in a series of intermediate goals tracked through fully integrated, system-level T&E events until the reliability threshold is achieved.

(3) Use scientific test and analysis techniques to design an effective and efficient test program that will produce the required data to characterize system behavior across an appropriately selected set of factors and conditions.

(4) Identify each developmental test phase or major developmental test event as a contractor or government DT&E. All programs will plan for the conduct of DT&E and/or integrated testing to provide confidence in the system design solution. Each major developmental test phase or event (including Test Readiness Reviews) will have test entrance and exit criteria. The developmental test completion criteria (customer needs) will dictate what data are required from the test event.

(5) Ensure that all test infrastructure and/or tools (e.g., models, simulations, automated tools, synthetic environments) to support acquisition decisions will be verified, validated, and accredited (VV&A) by the intended user or appropriate agency. Test infrastructure, tools, and/or the VV&A strategy including the VV&A authority for each tool or test infrastructure asset will be documented in the TEMP. Program Managers will plan for the application and accreditation of any modeling and simulation tools supporting DT&E.

(6) Develop complete resource estimates for T&E to include: test articles, test sites and instrumentation, test support equipment, threat representations and simulations, test targets and expendables, support for operational forces used in test (both friendly and threat), models and simulations, testbeds, joint mission environment, distributed test networks, funding, manpower and personnel, training, federal/state/local requirements, range requirements, and any special requirements (e.g., explosive ordnance disposal requirements or corrosion prevention and control). Resources will reflect the best estimate for conducting all test activities. Resources will be mapped against the developmental evaluation framework and schedule to ensure adequacy and availability.

(7) Ensure that resource estimates identified in the TEMP are matched against the schedule and justified by analysis.

(8) Resource and ensure threat-appropriate Red Team/Penetration testing to emulate the threat of hostile penetration of program information systems in the operational environment. Additional guidance on Red Team operations is included in Chairman of the Joint Chiefs of Staff Instruction 6510.01F (Reference (bf)).

(9) Develop a strategy and budget resources for cybersecurity testing. The test program will include, as much as possible, activities to test and evaluate a system in a mission environment with a representative cyber-threat capability.

(10) Ensure that each major developmental test phase or event in the planned test program has a well-defined description of the event, specific objectives, scope, appropriate use of modeling and simulation, and a developmental evaluation methodology.

(11) Describe a developmental evaluation methodology in the TEMP starting at Milestone A that will provide essential information on programmatic and technical risks as well as information for major programmatic decisions. Starting at Milestone B, the developmental evaluation methodology will include a developmental evaluation framework to identify key data that will contribute to assessing progress toward achieving: KPPs, critical technical parameters, key system attributes, interoperability requirements, cybersecurity requirements, reliability growth, maintainability attributes, developmental test objectives, and others as needed. In addition, the developmental evaluation framework will show the correlation and mapping between test events, key resources, and the decision supported. The developmental evaluation methodology will support a Milestone B assessment of planning, schedule, and resources and a Milestone C assessment of performance, reliability, interoperability, and cybersecurity.

(12) Develop a software test automation strategy to include when key test automation software components or services will be acquired and how those decisions will be made.

b. Programs will use government T&E capabilities unless an exception can be justified as cost-effective to the government. Program managers will conduct a cost-benefit analysis for exceptions to this policy and obtain approval through the TEMP approval process before acquiring or using non-government, program unique test facilities or resources.

c. In accordance with DoD Instruction 8510.01 (Reference (bg)), all programs must have security controls implemented consistent with their information and system categorization. Program managers will ensure appropriate testing to evaluate capability to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The Defense Intelligence Agency (DIA), in coordination with the Program Manager, will determine the generation of the relevant operational threat environment based on the Validated On-line Life-cycle Threat Report, the Multi-Service Force Deployment, the Joint Country Forces Assessment and scenario support products in accordance with DIA Directive 5000.200 (Reference (t)) and DIA Instruction 5000.002 (Reference (u)).

d. Systems that operate as part of a system of systems may require deployment of additional test assets to evaluate end-to-end capabilities. Program managers will ensure that adequate testing of total system of systems performance is conducted as part of the DT&E program.

e. For accelerated acquisition and urgent need programs, the levels of developmental testing required will be highly tailored to emphasize schedule over other considerations. Required testing to verify safety, capabilities, and limitations will be performed consistent with the urgency of fielding the capability. Responsibility for determining developmental testing requirements will be delegated to the lowest practical level. Urgent need programs will generally not be on an OSD DT&E Engagement list. If an Accelerated Acquisition program is on the DT&E Engagement list, complete developmental testing may be deferred so as not to impede early fielding; however, an operational assessment will typically be conducted. See paragraph 6a in Enclosure 5 of this instruction for a discussion of operational assessments, and Enclosure 12 for the policy and procedure regarding acquisition programs that respond to urgent needs.

6. DT&E EXECUTION, EVALUATION, AND REPORTING

a. DT&E Execution. As the Program Manager executes the program's strategy for the DT&E, the Program Manager and test team will develop detailed test plans for each developmental test event identified in the TEMP. Test plans must consider the potential impacts on personnel and the environment in accordance with 10 U.S.C. 4321-4347 (Reference (ag)) and Executive Order 12114 (Reference (ah)). The Program Manager, in concert with the user and T&E community, will provide safety releases (to include National Environmental Policy Act documentation, safety, and occupational health risk acceptance in accordance with section 16 in Enclosure 3 of this instruction) to testers prior to any test that may impact safety of personnel. A Test Readiness Review will be conducted for those events identified in the TEMP.

b. DASD(DT&E) Program Assessments. For MDAPs, MAIS programs, and USD(AT&L)-designated special interest programs, the DASD(DT&E) will provide the MDA with a program assessment at the Development RFP Release Decision Point, Milestones B and C, and updated to support the Operational Test Readiness Review or as requested by the MDA or Program Manager. The program assessment will be based on the completed DT&E and any Operational T&E activities completed to date, and will address the adequacy of the program planning, the implications of testing results to date, and the risks to successfully meeting the goals of the remaining T&E events in the program.

c. DT&E Reports and Data

(1) The DASD(DT&E) and the acquisition chain of command (including the Program Manager) and their designated representatives will have full and prompt access to all ongoing developmental testing, and all developmental test records and reports, including but not limited to: data from all tests, system logs, execution logs, test director notes, certifications, and user/operator assessments and surveys. This applies to all government accessible data including classified, unclassified, and competition sensitive or proprietary data. Data may be preliminary and will be identified as such.

(2) The Program Manager and test agencies for all programs will provide the Defense Technical Information Center (DTIC) with all reports and the supporting data for the test events in those reports. Paragraphs 11c(5) through 11c(7) in Enclosure 5 of this instruction include a more detailed discussion.

(3) The DoD Components will collect and retain data from developmental test and evaluation, integrated testing, and operational test and evaluation on the reliability and maintainability of Acquisition Category I and II programs.

(4) Tables 2 and 6 in Enclosure 1 identify statutory and regulatory reporting and notification requirements associated with the conduct of DT&E.

ENCLOSURE 5

OPERATIONAL AND LIVE FIRE TEST AND EVALUATION (OT&E AND LFT&E)

1. OVERVIEW

a. The fundamental purpose of test and evaluation (T&E) is to enable the DoD to acquire systems that work. To that end, T&E provides engineers and decision-makers with knowledge to assist in managing risks, to measure technical progress, and to characterize operational effectiveness, suitability, and survivability. This is done by planning and executing a robust and rigorous T&E program.

b. The Program Manager is responsible for resourcing and executing the system's approved T&E program. The Program Manager assembles a test team of empowered representatives of the various test data consumers. The team starts early (i.e., pre-Milestone A) to develop a robust, rigorous, and efficient test program that will be conducted in support of systems engineering, evaluations, and certifications throughout the program life cycle. The Program Manager documents the test program planning in the Test and Evaluation Master Plan (TEMP). All TEMPs will require DoD Component approval; TEMPs for programs under DOT&E oversight will also require DOT&E approval. The operational and select live fire test events in the TEMP must have approved test plans. Test plans are written and approved by the test organization responsible for the test. Operational test plans (OTPs) for programs under DOT&E OT&E oversight and live fire test plans (LFTPs) for programs under DOT&E LFT&E oversight will require DOT&E approval.

c. For programs under DOT&E OT&E or LFT&E oversight, the DOT&E will provide the MDA with milestone assessments. DOT&E will submit a report to the Secretary of Defense and the congressional defense committees before programs under DOT&E OT&E or LFT&E oversight may proceed beyond Low-Rate Initial Production (LRIP), in accordance with 10 U.S.C. 2366 and 2399 (Reference (h)).

2. APPLICABILITY. This enclosure applies to all defense acquisition programs under OSD OT&E or LFT&E oversight. This enclosure is written to the Hardware Intensive Program model described in paragraph 5c(3)(b) of this instruction , with tailoring instructions for the software within those programs and the software-specific acquisition models. When there is no distinction between Defense Unique Software Intensive Programs (Model 2) and Incrementally Deployed Software Intensive Programs (Model 3), they are referenced herein as "Software Acquisitions." Tailoring for any software, irrespective of acquisition model, is identified as being "for software in any system." Tailoring for Accelerated Acquisition models will be considered on a case-by-case basis.

3. DOT&E OVERSIGHT LIST

a. DOT&E may place any program or system on the DOT&E Oversight List for OT&E or LFT&E oversight at any time.

b. DOT&E maintains the DOT&E Oversight List continuously online at https://extranet.dote.osd.mil/oversight/ (requires login with a Common Access Card).

c. The DOT&E Oversight List is unclassified. Classified and sensitive programs that are placed on DOT&E oversight will be identified directly to their MDAs.

d. The DOT&E Oversight List is the list of Major Defense Acquisition Programs (MDAPs) under DOT&E oversight. MDAPs on DOT&E oversight include those programs that meet the statutory definition of 10 U.S.C. 2430 (Reference (h)), and those that are designated by the DOT&E as MDAPs for the purposes of OT&E under the authority of paragraph (a)(2)(B) of 10 U.S.C. 139 (Reference (h)). The latter programs are not MDAPs for any other purpose.

e. Unless specifically waived, the test-related documentation that is required for MDAP programs will be required for all programs on the DOT&E Oversight List, including submission of Defense Intelligence Agency or DoD Component Validated On-line Life-cycle Threat Reports, TEMPs, OTPs, Live Fire Test Plans (LFTPs), and reporting of test results.

f. Force protection equipment (including non-lethal weapons) will be subject to DOT&E oversight, as determined by DOT&E. The DOT&E will approve required LFTPs and/or live fire strategies for such systems.

g. Capability upgrades, other alterations that materially change system performance, and alterations that pose substantial risk of degrading fielded military capabilities (if they fail) will be tested operationally. Product improvements or upgrades to system survivability will also be tested and evaluated.

h. The DOT&E Oversight List will identify programs grouped for coordinated or synchronized testing.

4. T&E PROGRAM MANAGEMENT

a. Early Engagement. Program managers for programs under DOT&E oversight will designate a T&E WIPT (also known as an Integrated Test Team), as soon as practicable after the Materiel Development Decision. The T&E WIPT develops and tracks the T&E program in all phases. The T&E WIPT will include empowered representatives of test data stakeholders such as Systems Engineering, Developmental Test and Evaluation (DT&E), OT&E, LFT&E, the user, Product Support, the intelligence community, and applicable certification authorities.

b. Lead Operational Test Agency (OTA). The lead OTA is the responsible OTA for a program. When more than one OTA is responsible for a program, the responsible OTAs will jointly identify the lead OTA.

c. Required Documentation. T&E program documentation that already exists in other acquisition documents may be provided by working links. Documentation that directly impacts the OT&E or LFT&E program will be included or linked in the applicable T&E documentation or else the documentation in question will be approved by DOT&E in addition to any other applicable approvals. DOT&E approval or disapproval of a document incorporating links constitutes approval or disapproval of the content applicable to operational testing in all of the links. Specifically, although DOT&E does not approve all the content of linked documents, DOT&E may require changes to linked content dealing specifically with operational or live-fire testing.

5. T&E PROGRAM PLANNING

a. The TEMP is a signed contract among DOT&E, senior DoD Component leadership, the lead OTA, the MDA, and the Program Manager.

b. The Program Manager and T&E WIPT will prepare and then update the TEMP to support the acquisition milestones. For the Full-Rate Production Decision Review or the Full Deployment Decision and thereafter (for DOT&E OT&E or LFT&E Oversight programs), DOT&E, the MDA, or the senior DoD Component leadership may require TEMP updates or addendums to address additional testing.

c. Working through the T&E WIPT, program managers for DOT&E oversight programs will make draft TEMPs available to program stakeholders as early and as frequently as possible. DoD Component-approved TEMPs will be submitted to OSD for approval not later than 45 calendar days prior to the milestone decision.

(1) A TEMP may be waived for select Accelerated or Urgent Acquisitions. In cases when DOT&E decides a TEMP is not needed, early briefings to DOT&E (in lieu of the TEMP) are recommended to facilitate subsequent DOT&E approval of the OTPs and LFTPs. DOT&E will approve the OTPs and LFTPs for accelerated acquisition (including capabilities acquired in response to an urgent need and acquisitions granted Rapid Acquisition Authority) if those acquisitions are under DOT&E OT&E or LFT&E oversight. If DOT&E has placed an Accelerated Acquisition on oversight, it is because DOT&E has determined that OT&E or LFT&E is required before fielding. Testing to verify safety, survivability, and operational performance will be conducted consistent with the urgency of deploying the capability. The Secretary of Defense may authorize the Rapid Acquisition Official to defer some testing until after fielding if he or she determines that the testing would unnecessarily impede the deployment of the needed capability. Testing should normally include user feedback to support design and operational use improvements.

(2) Initial Operational Test and Evaluation (IOT&E) is required for all programs under DOT&E oversight in accordance with 10 U.S.C. 2399 (Reference (h)). The lead OTA will conduct an independent, dedicated phase of IOT&E before full-rate production or full deployment that provides objective test results free from potential conflicts of interest or bias. The primary purpose of IOT&E is to determine a system's operational effectiveness and operational suitability. IOT&E can also be used to support system certification requirements and training requirements as long as the primary purpose is accomplished.

d. The lead OTA for the program and the Program Manager will initiate coordinated planning for IOT&E as early as possible so that developing activities will be aware of expectations at IOT&E:

(1) The lead OTA for the program will provide an assessment of the T&E implications of the initial concept of operations (CONOPS) provided by the user in the Milestone A TEMP.

(2) Beginning at Milestone A, the lead OTA will provide a working link in the TEMP to a living document in which the DoD Component's operational rationale for the requirements in the draft Capability Development Document (CDD) or equivalent requirements document will be tracked.

(3) For software acquisitions, the lead OTA will conduct an analysis of operational risk to mission accomplishment covering all planned capabilities or features in the system (see paragraph 7d in this enclosure for additional details). The analysis will include commercial and non-developmental items. The initial analysis will be documented in the Milestone A TEMP and updated thereafter.

(4) The TEMP will include evaluation of mission-level interoperability across key interfaces. Systems that provide capabilities for joint missions will be tested in the expected joint mission environment.

e. Scientific test and analysis techniques (also referred to as Design of Experiments methodologies) should be employed to design an effective and efficient T&E program. The TEMP should document the test program that will produce the required data to characterize combat mission capability across an appropriately selected set of factors and conditions.

(1) Starting at Milestone A, the TEMP should document T&E for phase completion (major test events required for milestone exit and entrance criteria). In addition, each major test phase or event should have test entrance and test completion criteria.

(2) Each major test phase or event should have a synopsis of the intended analysis. A synopsis should indicate how the required data for test completion will contribute to one or more standard measures of program progress. These include the following terms:

(a) Critical operational issues (also known as critical operational issues and criteria).

(b) KPPs.

(c) Critical technical parameters.

(d) Key system attributes.

(3) Every TEMP will include a table of independent variables (or "conditions," "parameters," "factors," etc.) that may have a significant effect on operational performance. Starting at Milestone B, the updated table of variables will include the anticipated effects on operational performance, the range of applicable values (or "levels," "settings," etc.), the overall priority of understanding the effects of the variable, and the intended method of controlling the variable during test (uncontrolled variation, hold constant, or controlled systematic test design).

(4) Starting at Milestone B, every TEMP will include an evaluation overview. The overview will show how the major test events and test phases link together to form a systematic, rigorous, and structured approach to evaluating mission capability across the applicable values of the independent variables. Test resources will be derived from the evaluation overview (see section 10 in this enclosure).

6. OT&E ACTIVITIES

a. Operational Assessments (OAs)

(1) The lead OTA will prepare and report results of one or more early OAs (EOAs) as appropriate in support of one or more of the design phase life-cycle events (namely, the CDD Validation, the Development RFP Release Decision Point, or Milestone B). An EOA is typically an analysis, conducted in accordance with an approved test plan, of the program's progress in identifying operational design constraints, developing system capabilities, and mitigating program risks. For programs that enter development at Milestone B, the lead OTA will (as appropriate) prepare and report EOA results after program initiation and prior to the Critical Design Review.

(2) An OA is a test event that is conducted before initial production units are available and which incorporates substantial operational realism. An OA is conducted by the lead OTA in accordance with a test plan approved by DOT&E for programs that are under OSD OT&E oversight. As a general criterion for proceeding through Milestone C, the lead OTA will conduct and report results of at least one OA. For an acquisition program employing the Incrementally Deployed Software Intensive Program model, a risk-appropriate OA is usually required in support of every limited deployment (see Model 3 at paragraph 5c(3)(d) in this instruction). An operational test, usually an OA, is required prior to deployment of accelerated or urgent acquisition programs that are under OSD OT&E or LFT&E oversight. An OA may be combined with training events (see paragraph 11a(9) in this enclosure). An OA is not required for programs that enter the acquisition system at Milestone C.

b. RFPs. An up-to-date TEMP will be provided prior to release of RFPs for Milestone B and Milestone C. To the maximum extent feasible, RFPs should be consistent with the operational test program documented in the TEMP.

c. OT&E for Reliability and Maintainability

(1) The TEMP will include a plan (typically via working link to the Systems Engineering Plan) to allocate top-level reliability requirements down to the components and sub-components. Reliability allocations will include hardware and software, and will include commercial and non-development items.

(2) Reliability Growth

(a) Beginning at Milestone B, the TEMP will include T&E for reliability growth and reliability growth curves (RGCs) for the whole system and the reliability of critical systems, sub-systems, components, and sub-components. Reliability-critical items require test to mitigate risk resulting from the use of new technologies or from challenging operating environments. T&E for reliability growth will provide data on initial reliability (namely: identify the contractor and government reliability testing needed to achieve initial reliability) and reliability test events. RGCs will display planned initial reliability, the allocated reliability requirement, a curve showing reliability that is expected during each reliability test event, and points marking reliability test results to date.

(b) For software (in any system) reliability growth will be measured by software maturity metrics (e.g., counts of high priority defects) at regular intervals.

(c) Beginning at Milestone B, the TEMP will include a working link to the Failure Modes, Effects and Criticality Analysis (FMECA) of identified or anticipated system failure modes, the impacted components and sub-components, and the method of failure mode discovery. A software defect or failure tracking database(s) may replace the FMECA in software acquisitions.

(3) Updated TEMPs at Milestone C will include updated RGCs that reflect test results to date, any updates to the planned T&E for reliability growth, and a working link to the updated FMECA.

d. Use of Modeling and Simulation. Models or simulations that utilize or portray threat characteristics or parameters must have that portrayal accredited by the Defense Intelligence Agency. Every distinct use of a model or simulation in support of an operational evaluation will be accredited by an OTA, and, for programs under DOT&E Oversight, its use for the operational evaluation will be approved by DOT&E.

7. OT&E FOR SOFTWARE

a. Acquisition of software for any system will normally be supported by specialized models and early user involvement:

(1) As feasible, testing of software for any system should be supported by a model (or emulated hardware or virtual machine) of the digital device(s) on which the software runs.

(2) To the extent feasible, program managers should test prototype human interfaces with operational users.

(3) Program managers for software acquisitions should develop process models of the time and effort needed to perform critical tasks and functions. Such models support operational test design and analysis of results as well as managerial needs such as sustainment cost projections and analysis of impacts of process changes.

(4) Program managers must sustain an operationally realistic maintenance test environment in which software patches can be developed and upgrades of all kinds (developed or commercial) can be tested. The maintenance test environment is a model of the operational environment in that it should be able to replicate software defects found in the operational environment.

b. Program managers for software acquisitions will provide plans at Milestone B indicating how system logs and system status records will interface with operational command and control. At IOT&E or a prior test event, program managers for software acquisitions will demonstrate performance monitoring of operational metrics to manage and operate each system capability (or the whole system, as appropriate).

c. For software in any system, the evaluation of operational suitability will include a demonstrated capability to maintain the software. IOT&E or a prior test event will include an end-to-end demonstration of regression test, preferably automated, in the maintenance test environment. The demonstration will show how changes in requirements or discovered defects are mapped to lines of software that must be modified, and how modifications in software are mapped to the regression test scripts that will verify correct functioning of the modified software.

d. Risk-Assessed Level of Operational Test for Software Acquisitions (Models 3, 4, and Hybrids)

(1) OT&E for software acquisitions will be guided by the assessment of operational risks of mission failure. A significant operational risk of mission failure is a risk that is at least moderately likely to occur, and if the risk does occur then the impact will cause a degradation or elimination of one or more operational capabilities.

(2) At any level of risk, the lead OTA will coordinate with DOT&E on the required level of test and then observe the agreed-upon testing. At the lowest risk level, the lead OTA will review plans and observe developmental testing or developmental testing and integrated testing.

At the highest risk level, the lead OTA will execute a full OT&E in accordance with the DOT&E-approved OTP. For intermediate risks, the lead OTA will coordinate with the responsible developmental testing organization to observe and execute some integrated developmental testing/operational testing in accordance with a DOT&E-approved OTP.

(3) DOT&E will require an operational test or OA for every Limited Deployment in any acquisition model. The scope of the OT&E or OA will be guided by the risk of capability being fielded or deployed.

(4) IOT&E is required for every increment, in any acquisition model (except as noted for urgent operational needs). IOT&E will normally occur prior to the Full Deployment Decision. IOT&E will be guided by an updated assessment of the operational risks in the capabilities and system interactions that have not been successfully evaluated in previous operational testing.

8. CYBERSECURITY

a. Beginning at Milestone A, the TEMP will document a strategy and resources for cybersecurity T&E. At a minimum, software in all systems will be assessed for vulnerabilities. Mission critical systems or mission critical functions and components will also require penetration testing from an emulated threat in an operationally realistic environment during OT&E.

b. Beginning at Milestone B, appropriate measures will be included in the TEMP and used to evaluate operational capability to protect, detect, react, and restore to sustain continuity of operation. The TEMP will document the threats to be used, which should be selected based on the best current information available from the intelligence community.

c. The Program Manager, T&E subject matter experts, and applicable certification stakeholders will assist the user in writing testable measures for cybersecurity and interoperability.

d. The Program Manager and OTA will conduct periodic cybersecurity risk assessments to determine the appropriate Blue/Green/Red Team, and operational impact test events in alignment with the overall test strategy for evaluating the program for real world effects. Defense business systems will undergo Theft/Fraud operational impact testing.

9. LFT&E. 10 U.S.C. 2366 (Reference (h)) mandates the LFT&E and formal LFT&E reporting for all covered systems, as determined by DOT&E, including Accelerated Acquisitions, survivability improvement, and kit programs to address urgent needs. DOT&E will require approval of LFT&E strategies and LFT&E test plans (including survivability test plans) for covered systems as defined in section 2366. The DOT&E will determine the quantity of test articles procured for all LFT&E test events for any system under DOT&E LFT&E oversight.

10. RESOURCES AND SCHEDULE. All TEMPs will identify the resources needed to execute the planned T&E activities. Resource estimates will be matched against the schedule and justified by analysis in the TEMP. All TEMPs will contain an updated integrated test program summary and master schedule of all major test events or test phases, to include LFT&E events.

a. Resource estimates (including but not limited to quantities of test articles, targets, expendables, threat simulations, operational forces, etc.) will be derived from defensible statistical measures of merit (power and confidence) associated with quantification of the differences among the factors affecting operational performance as well as the risk to the government of accepting a poorly performing system or incorrectly rejecting a system with acceptable performance. Specifically, the TEMP must discuss and display, or provide a reference to, the calculations done to derive the content of testing and to develop the associated resource estimates.

b. The Program Manager and the Services or Defense Agencies will allocate the resources identified in the TEMP. Each TEMP update will include an updated and complete T&E resource estimate.

c. Test infrastructure, resources (including threat representations), and tools to be used in operational tests must undergo verification by the developer, validation by the DoD Component, and accreditation by the OTA. Test infrastructure, resources, and tools, and their associated verification, validation, and accreditation strategies will be documented in the TEMP.

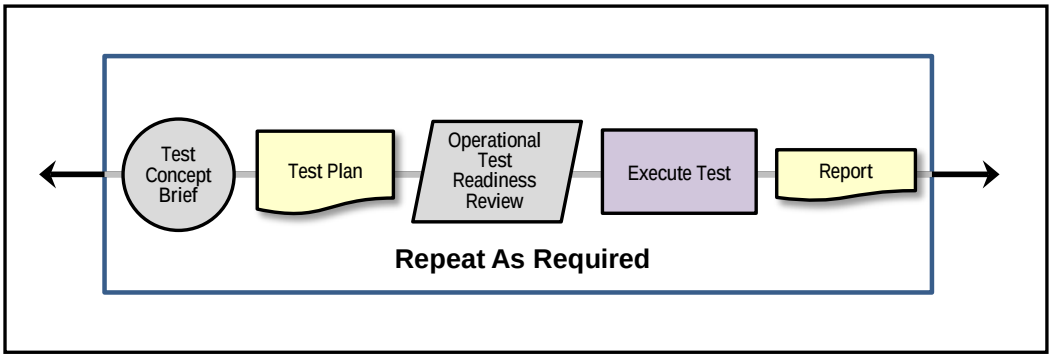
d. In accordance with 10 U.S.C. 2399 (Reference (h)), DOT&E will approve the quantity of test articles required for all operational test events for any system under DOT&E oversight. The DoD Component OTA will determine the quantity for programs that are not under DOT&E oversight.

e. The T&E schedule will be event-driven and allow adequate time to support pre-test predictions; testing; post-test analysis, evaluation, and reporting; reconciliation of predictive models; and adequate time to support execution of corrective actions in response to discovered deficiencies.

f. For incremental software acquisitions employing limited deployments (see Model 3 at paragraph 5c(3)(d) in this instruction), the Milestone B TEMP will show a general schedule for the routine test sequence (developmental tests, certifications, integrated and operational tests) that will occur with every limited deployment within the allotted time for each limited deployment.

11. OPERATIONAL AND LIVE FIRE T&E EXECUTION. The general process for planning, executing, and reporting on operational and major live fire test events is shown in Figure 9.

Figure 9. Operational or Major Live Fire Test Event:
Planning, Approval, Execution, and Reporting



a. Planning Test Events

(1) For all programs under DOT&E oversight, including Accelerated Acquisitions, DOT&E will approve OTPs and LFTPs prior to the corresponding operational or major live fire test events in accordance with 10 U.S.C. 2399. DOT&E will approve any LFTP for a major test event such as Full-up System Level test, Total Ship Survivability Trial, or Full Ship Shock Trials. The major live fire test events will be identified in the TEMP (or LFT&E strategy or equivalent document). Test plans are developed by a lead test organization (LTO). The LTO is the lead OTA for OT&E. The LTO varies for LFT&E.

(2) For programs under DOT&E oversight, the appropriate LTO will brief the DOT&E on T&E concepts for the OTP or the major LFT&E as early as possible and not less than 180 calendar days prior to start of any such testing. DOT&E and DoD Component leads will be kept apprised of changes in test concept and progress on the OTP. The lead OTA will deliver the DoD Component-approved OTP for DOT&E review not later than 60 calendar days before test start. The LTO for major live fire events will deliver the DoD Component-approved LFTP for DOT&E review not later than 90 days before test start.

(3) OTPs and major LFTPs will include the plans for data collection and management.

(4) Integrated Testing

(a) Integrated testing is the collaborative planning and collaborative execution of test phases and events to provide shared data in support of independent analysis, evaluation and reporting by all stakeholders particularly the developmental (both contractor and government) and operational test and evaluation communities. It requires the active participation of the lead OTA in planning the integrated tests with the program office so that the operational objectives are understood, the testing is conducted in an operationally realistic manner, and the resultant data is relevant for use in operational evaluations.

(b) For integrated test results to count for operational testing, the lead OTA must develop a plan for the integrated test to be approved by DOT&E before the start of testing that, at a minimum, details the required test realism and conditions, operational test objectives, operational test metrics and data collection requirements. Data collected outside an approved OTP or major LFTP can be used for a DOT&E operational or live fire evaluation if the data is approved by DOT&E. Depending on circumstances, DOT&E approval will not necessarily be possible in the TEMP and may require some other documentation. Data approval will be based on understanding of the realism of the test scenario(s) used and the pedigree (test conditions and methodologies) of the data. The data in question will typically come from operational exercises, certification events, and developmental test events conducted in operationally relevant environments. Data approval should be coordinated with the LTO and DOT&E prior to the start of testing. When advance coordination is not possible, the LTO will facilitate data re-use (in a DOT&E assessment or evaluation) through independent documentation of the test data pedigree (test conditions and methodologies).

(5) In OT&E, typical users or units will operate and maintain the system or item under conditions simulating combat stress in accordance with 10 U.S.C. 139 (Reference (h)) and peacetime conditions, when applicable. The lead OTA, in consultation with the user and the Program Manager, will identify realistic operational scenarios based on the CONOPS (per paragraph 5d(1) in this enclosure) and mission threads derived from the Joint Mission Essential Task List or DoD Component-specific Mission Essential Task List. See paragraph 7d of this enclosure for risk-assessed OT&E of software acquisitions.

(6) In accordance with 10 U.S.C. 2399 (Reference (h)), persons employed by the contractor for the system being developed may only participate in OT&E of systems under OSD OT&E oversight to the extent they are planned to be involved in the operation, maintenance, and other support of the system when deployed in combat.

(a) A contractor that has participated (or is participating) in the development, production, or testing of a system for a DoD Component (or for another contractor of the DoD) may not be involved in any way in establishing criteria for data collection, performance assessment, or evaluation activities for OT&E.

(b) These limitations do not apply to a contractor that has participated in such development, production, or testing, solely in test or test support on behalf of the DoD.

(7) IOT&E for all programs will use production or production-representative test articles that, at a minimum, will incorporate the same parts and software items to be used in LRIP articles. Production-representative systems meet the following criteria:

(a) The hardware and software must be as defined by the system-level critical design review, functional configuration audit, and system verification review, including correction of appropriate major deficiencies identified during prior testing.

(b) For hardware acquisitions, production-representative articles should be assembled using the parts, tools, and manufacturing processes intended for use in full-rate production; utilize the intended production versions of software; and the operational logistics systems including mature drafts of maintenance manuals intended for use on the fielded system should be in place. The manufacturing processes to be used in full-rate production should be adhered to as closely as possible, and program managers for programs under DOT&E OT&E oversight will provide DOT&E a detailed description of any major manufacturing process changes.

(c) For software acquisitions, a production-representative system consists of typical users performing operational tasks with the hardware and software intended for deployment, in an operationally realistic computing environment, with representative DoD information network operations and supporting cybersecurity capabilities. All manuals, training, helpdesk, continuity of operations, system upgrade and other life-cycle system support should be in place.

(8) IOT&E will require more than an evaluation that is based exclusively on computer modeling, simulation, or an analysis of system requirements, engineering proposals, design specifications, or any other information contained in program documents in accordance with 10 U.S.C. sections 2399 and 2366 (Reference (h)). IOT&E will feature end-to-end testing of system capabilities including all interrelated systems needed to employ and support those capabilities.

(9) Program managers for all programs (and particularly Accelerated Acquisitions) may, in coordination with the lead OTA, elect to perform integrated testing in conjunction with training, joint and operational exercises, or synchronized test events. Such testing is efficient, but inherently increases the risk that a significant problem will not be discovered. If no subsequent operational testing is conducted prior to fielding, then additional testing will typically be required subsequent to initial fielding. When subsequent testing is required, the plan for the T&E and reporting of results will be included in the applicable TEMP or other planning documentation.

b. Conducting Test Events

(1) Test plans must consider the potential impacts on personnel and the environment, in accordance with 42 U.S.C. 4321-4347 (Reference (ag)) and Executive Order 12114 (Reference (ah)). The Program Manager, working with the user and the T&E community, will provide safety releases (to include formal environment, safety, and occupational health risk acceptance in accordance with section 16 of Enclosure 3 of this instruction) to the developmental and operational testers prior to any test that may impact safety of personnel.

(2) Barring significant unforeseen circumstances, all elements of an approved OTP or LFTP must be fully satisfied by the end of an operational or live fire test. If an approved plan cannot be fully executed, DOT&E concurrence with any changes must be obtained before revised test events are executed. Once testing has begun, deviations from approved elements of the test plan cannot be made prior to the beginning of their execution without consultation with the OTA commander (for OTP) or appropriate LTO (for LFTP) and the concurrence of DOT&E. DOT&E concurrence is not required when a need to change the execution of an element of the test plan arises in real time as its execution is underway. If DOT&E on-site representatives are

not present and the test director concludes changes to the plan are warranted that would revise events yet to be conducted, the test director must contact the relevant DOT&E personnel to obtain concurrence with the proposed changes. If it is not possible to contact DOT&E personnel in a timely manner, the test director can proceed with execution of the revised test event but must inform DOT&E of the deviations from the test plan as soon as possible.

(3) When the order of execution is identified in the TEMP as affecting the analysis of the data, test plans should include details on the order of test event execution and/or test point data collection.

(4) Operating instructions (i.e., tactics, techniques and procedures, standard operating procedures, technical manuals, technical orders) should be considered for their impact on the test outcomes and included in OTPs when relevant.

(5) Test plans must include the criteria to be used to make routine changes (delays for weather, test halts, etc.).

(6) If required data for the test completion criteria are lost, corrupted, or not gathered, then the test is not complete unless the requirement is waived by DOT&E.

c. Data Management, Evaluation, and Reporting

(1) DOT&E, the Program Manager and their designated representatives who have been properly authorized access, will all have full and prompt access to all records, reports, and data, including but not limited to data from tests, system logs, execution logs, test director notes, and user and operator assessments and surveys. Data include but are not limited to classified, unclassified, and (when available) competition sensitive or proprietary data. Data may be preliminary and will be identified as such.

(2) OTAs and other T&E agencies will record every OT&E and LFT&E event in some written form. Full reports will often contain multiple test events and will be accomplished in the most timely manner practicable. Interim summaries or catalogues of individual events will be prepared as results become available.

(3) Significant problems will be reported promptly to senior DoD leadership when those problems are identified. OTAs will publish interim test event summaries as interim reports when the test events provide information of immediate importance to the program decision makers. This will occur particularly in support of accelerated acquisitions and time critical operational needs. Such reports should provide the most complete assessment possible based on the available data and should not be delayed. Such reports will be followed by the planned comprehensive reporting.

(4) For DOT&E OT&E and LFT&E oversight programs, DOT&E will be kept informed of available program assets, assessments, test results and anticipated timelines for reporting throughout report preparation.

(5) The Program Manager and test agencies for all programs will provide the Defense Technical Information Center (DTIC) with all reports, and the supporting data and metadata for the test events in those reports. If there are limitations in the data or metadata that can be provided to DTIC, those limitations will be documented in the TEMP starting at Milestone B.

(6) Test agencies will provide the DoD Modeling and Simulation Coordination Office with a descriptive summary and metadata for all accredited models or simulations that can potentially be reused by other programs.

(7) The Secretaries of the Military Departments, in coordination with the Defense Acquisition Executive, DOT&E, and the Under Secretary of Defense for Personnel and Readiness, will establish a common set of data for each major weapon system type to be collected on damage incurred during combat operations. This data will be stored in a single dedicated and accessible repository at DTIC. The lessons learned from analyzing this data will be included, as appropriate, in both the capability requirements process and the acquisition process for new acquisitions, modifications, and/or upgrades.

12. OPERATIONAL TEST READINESS. The DoD Components will each establish an Operational Test Readiness Review process to be executed for programs under DOT&E oversight prior to any Operational Test. Prior to IOT&E, the process will include a review of DT&E results, an assessment of the system's progress against the KPPs, key system attributes, and critical technical parameters in the TEMP, an analysis of identified technical risks to verify that those risks have been retired or mitigated to the extent possible during DT&E and/or OT&E, a review of system certifications, and a review of the IOT&E entrance criteria specified in the TEMP.

13. CERTIFICATIONS. Testing in support of certifications should be planned in conjunction with all other testing.

a. The Program Manager is responsible for determining what certifications are required; ensuring involvement of the representatives of applicable certifying authorities in the T&E WIPT; and satisfying the certification requirements.

b. The Program Manager will provide the MDA, DOT&E, and the lead OTA with all data on certifications as requested.

c. In accordance with DoD Instruction 8330.01 (Reference (ab)), the TEMP for all programs must reflect interoperability and supportability requirements, and serve as the basis for interoperability assessments and certifications.

14. TEMP EVOLUTION THROUGH THE ACQUISITION MILESTONES. The preceding policies are summarized together with associated DOT&E guidance and TEMP outlines at http://www.dote.osd.mil/temp-guidebook/index.html.

ENCLOSURE 6

LIFE-CYCLE SUSTAINMENT

1. PURPOSE. This enclosure describes the application of life-cycle sustainment planning policies and procedures. The enclosure addresses sustainment across the life cycle, and the elements of the Life-Cycle Sustainment Plan (LCSP).

2. SUSTAINMENT ACROSS THE LIFE CYCLE. Sustainment planning, including the requirements in 10 U.S.C. 2337 (Reference (h)), and in Appendix E to Enclosure B of the Manual for the Operation of the Joint Capabilities Integration and Development System (Reference (r)), must be an integral element of the capability requirements and acquisition process from inception.

a. The Program Manager, with the support of the Product Support Manager (PSM), will:

(1) Develop and implement an affordable and effective performance-based product support strategy. The product support strategy will be the basis for all sustainment efforts and lead to a product support package to achieve and sustain warfighter requirements.

(a) The product support strategy will address, at a minimum:

1. An integrated product support capability implementing the program's mix of government and industry providers supported by appropriate analyses included in 10 U.S.C. 2337.

2. Sustainment metrics mapped to the sustainment KPP and key system attributes to manage sustainment performance.

3. Implementation of a reliability improvement program based on Failure Modes, Effects and Critically Analysis (or defect tracking for software), other engineering data developed during the systems engineering process, system health information generated by applicable on-board and off-board technologies, and data sources in accordance with DoD Instruction 4151.22 (Reference (bi)).

4. Competition, or the option of competition, at the prime and subcontract levels for large and small businesses, and system and sub-system levels.

5. The necessary IP deliverables and associated license rights, consistent with and integrated with the program IP Strategy. Paragraph 6a(4) in Enclosure 2 of this instruction details IP policy.

6. How and when computer software and computer software documentation (as defined in Defense Federal Acquisition Regulation Supplement (Reference (al)) section 252.227-

7014) and other material and activities required to maintain and sustain the software after Initial Operational Capability (IOC) will be provided to the government for systems that require core logistics support or when depot level software maintenance is required. Paragraph 3d(2) in this enclosure addresses core logistics requirements.

7. The use of existing government owned inventory prior to use of product support arrangements as required in 10 U.S.C. 2337 (Reference (h)).

8. The government accountable property system that documents all government owned property whether it is held and managed by the government, contractor, or third party, in accordance with 40 U.S.C. 524 (Reference (p)).

(b) Product support integrators and product support providers may be organic, commercial, or a combination.

(2) Ensure identification of obsolete parts in specifications and develop plans for suitable replacements in accordance with P.L. 113-66, section 803 (Reference (bj)) as part of the program's plan to prevent the acquisition of counterfeit material in the DoD supply chain as required by DoD Instruction 4140.67 (Reference (ck)).

(3) Employ effective performance-based logistics (PBL) planning, development, implementation, and management in developing a system's product support arrangements. PBL is performance-based product support, where outcomes are acquired through performance-based arrangements that deliver warfighter requirements and incentivize product support providers to reduce costs through innovation.

(4) Continually assess and refine the product support strategy based on projected and actual performance.

(5) Employ a "Should-Cost" management and analysis approach to identify and implement system and enterprise sustainment cost reduction initiatives. Should-cost targets will be established and reviewed periodically based on analysis of acquisition sustainment costs and operations and support (O&S) cost element drivers. Program managers will capture product support metrics and cost data in DoD Component- and DoD-level information systems, and track performance against should-cost targets.

(6) Continually monitor product support performance and correct trends that could negatively impact availability and cost.

(7) Minimize unique automatic test equipment (ATE) by utilizing designated DoD automatic test system families for all ATE hardware and software in DoD field and depot operations.

(8) Begin demilitarization and disposal planning, including demilitarization and controlled inventory item coding of system, subsystems, or components, as required by DoD Manual 4160.28-M (Reference (bk)), with sufficient lead time before the disposal or retirement

of the first asset to reduce costs and risks and to ensure compliance with statutory and regulatory requirements.

(9) Plan for corrosion prevention and control (CPC) in systems engineering and life cycle sustainment as required by DoD Instruction 5000.67 (Reference (bl)). Product support planning, especially maintenance planning and sustaining engineering, will incorporate appropriate mitigation of CPC risks inherent in the design to meet sustainment requirements.

b. DoD Components will:

(1) Ensure that sustainment factors are fully considered at all key life-cycle management decision points, and that appropriate measures are taken to reduce operating and support costs by influencing system design early in development, developing sound product support strategies, and addressing key drivers of cost.

(2) Periodically assess product support performance and assist program managers, users, resource sponsors, and materiel enterprise stake holders to take corrective action to prevent degraded materiel readiness or O&S cost growth.

(3) Initiate system modifications, as necessary, to improve performance and reduce ownership costs, consistent with the limitations prescribed in 10 U.S.C. 2244a (Reference (h)).

(4) Ensure Program Managers responsible for renewal of sustainment contracts that include public-private partnerships with DoD maintenance depots will include the use of Defense Logistics Agency (DLA) storage and distribution capacity in the terms of renewal public-private partnership arrangements and negotiate the transfer of government-owned inventory from commercial to DLA facilities, as specified in the arrangement.

3. LIFE-CYCLE SUSTAINMENT PLAN (LCSP). Program managers for all programs are responsible for developing and maintaining an LCSP consistent with the product support strategy, beginning at Milestone A. The plan will describe sustainment influences on system design and the technical, business, and management activities to develop, implement, and deliver a product support package that maintains affordable system operational effectiveness over the system life cycle and seeks to reduce cost without sacrificing necessary levels of program support. The Acquisition Strategy will also include an overview of the product support strategy and sustainment-related contracts.

a. The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) (or as designated) will approve acquisition category (ACAT) ID, ACAT IAM, and USD(AT&L)-designated special interest program LCSPs.

b. The Component Acquisition Executive (CAE), or designee, will approve LCSPs for ACAT IC, ACAT IAC, and ACAT II and below programs.

c. The LCSP will be updated at each milestone and specified decision points to reflect the increased maturity of the product support strategy, any changes in the corresponding product support package, current risks, and any cost reduction activities.

(1) At Milestone A, the LCSP will focus on development of sustainment metrics to influence design and the product support strategy, and on actions that can be taken prior to Milestone B to reduce future operating and support costs, including software sustainment. Planning will use factors and assumptions consistent with those used in the analysis of alternatives and affordability analysis, or justify any deviation from those factors and assumptions.

(2) At the Development RFP Release Decision Point and Milestone B, the LCSP will focus on finalizing the sustainment metrics, integrating sustainment considerations with design and risk management activities, and refining the execution plan for the design, acquisition, fielding, and competition of sustainment activities.

(3) At Milestone C, if applicable, the LCSP will focus on ensuring operational supportability and verifying performance.

(4) At the Full-Rate Production Decision or Full Deployment Decision, the LCSP will focus on how sustainment performance is measured, managed, assessed, and reported; and the actions to adjust the product support package to ensure continued competition and cost control while meeting warfighter mission requirements.

(5) After IOC, the LCSP is the principle document governing the system's sustainment. Programs will update the plan whenever there are changes to the product support strategy, or every 5 years, whichever occurs first, supported by appropriate analyses, sustainment metrics, sustainment costs, system components or configuration (hardware and software), environmental requirements, and disposal plans or costs.

d. The LCSP will include the following annexes:

(1) Business Case Analyses. The Program Manager will attach relevant assumptions, constraints, and analyses used to develop the product support strategy to the LCSP. The DLA will participate in supply support related business case analyses by developing and providing data for ACAT I, II, and III programs. PSMs will revalidate analyses based on changes to the assumptions, constraints, and operating environment, or every 5 years, whichever occurs first.

(2) Core Logistics Analysis. By Milestone A, the DoD Component will document its determination of applicability of core depot-level maintenance and repair capability requirements in the LCSP in accordance with 10 U.S.C. 2366a (Reference (h)). For Milestone B, the Program Manager will attach the program's estimated requirements for maintenance, repair and associated logistics capabilities and workloads to the LCSP in accordance with 10 U.S.C. 2366b. The program's maintenance plan will ensure that core depot-level maintenance and repair capabilities and capacity are established not later than 4 years after IOC in accordance with 10 U.S.C. 2464. The Program Manager will ensure that a depot source of repair designation is made not later than

90 days after the Critical Design Review. Before entering into a contract for low rate initial production, supportability analysis must include detailed requirements for core depot-level maintenance and repair capabilities, and associated sustaining workloads required to support such requirements. Program plans will include the use of DLA-operated storage and distribution facilities where collocated with the DoD Component's selection of organic depot maintenance.

(3) Preservation and Storage of Unique Tooling Plan. For Major Defense Acquisition Programs (MDAPs), the plan, as outlined and required by section 815 of P.L. 110-417 (Reference (g)), is prepared to support Milestone C. It must include the review cycle for assessing tool retention across the life of the system. If an MDA (other than the Defense Acquisition Executive (DAE)) determines that preservation and storage of unique tooling is no longer required, a waiver will be submitted to the DAE for notification to Congress.

(4) IP Strategy. The program's IP Strategy will be included in the LCSP and updated appropriately during the O&S Phase (see paragraph 6a(4) in Enclosure 2 of this instruction for additional information).

(5) Additional Annexes. Program Managers will consider including additional annexes, or reference other documents that integrate a program's sustainment planning or product support strategy.

e. Life-cycle sustainment for information systems may be provided via multiple approaches, including service level agreements, support agreements, performance work statements, and enterprise services. Where feasible and as approved by the MDA, programs may employ portfolio-level documents to satisfy their LCSP requirements. Commercial off-the-shelf and government off-the-shelf products used as intended will normally be supported via standard warranties and support agreements. Effective life-cycle sustainment requires continuous monitoring to ensure investments are maintained at the right size, cost, and condition, to include vulnerability management, to support warfighter and business missions and objectives. Information technology investment LCSPs will address Management-in-Use guidelines published in Office of Management and Budget Circular A-11 (Reference (c)).

4. SUSTAINMENT METRICS. The sustainment KPP (Availability) is as critical to a program's success as cost, schedule, and performance. ACAT I and II program managers will use availability and sustainment cost metrics as triggers to conduct further investigation and analysis into drivers of those metrics, to develop Should Cost targets, and to develop strategies for improving reliability, availability, and maintainability of such systems at a reduced cost. The materiel availability portion of the KPP will be based on the entire system inventory and supported by the following sustainment metrics:

a. Materiel Reliability. As required by the Manual for the Operation of the Joint Capabilities Integration and Development System (Reference (r)), materiel reliability is the design metric that has the most significant impact on the program's operational availability and O&S cost.

b. O&S Cost. DoD Components will ensure reliability and maintainability data from operational and developmental testing and evaluation and fielding informs estimates of O&S costs for major weapon systems.

c. Mean Down Time. The average total downtime required to restore an asset to its operational capability, measures the effectiveness of the supply chain and support infrastructure (e.g., customer wait time, logistics response time, retrograde time). It is an important element in assessing a system's affordability across its life cycle and identifies constraints and opportunities of a system's product support strategy and product support arrangements.

d. Other Metrics. Outcome metrics to support sustainment elements included in capability requirements documentation or required by the DoD Component to manage the system development, product support package, and supply chain to develop and maintain the system.

5. PRODUCT SUPPORT REVIEWS

a. The program's PSM will assess logistics as a focused part of the program's Program Support Assessments and technical reviews (e.g., systems engineering, test) to ensure the system design and product support package are integrated to achieve the sustainment metrics and inform applicable modeling and simulation tools.

b. The DoD Components will conduct independent logistics assessments (ILAs) for all weapon system MDAPs prior to Milestones B and C and the Full-Rate Production Decision to assess the adequacy of the product support strategy, and to identify features that are likely to drive future operating and support costs, changes to system design that could reduce costs, and effective strategies for managing such costs. The reviews will focus on sustainment planning and execution, to include the core logistics analyses and establishment of organic capabilities. Each DoD Component will establish its criteria for independence, and will provide (1) guidance to ensure consistency within the respective Component and (2) the scope of the assessment for key acquisition decision points. At a minimum, these reviews will be chartered by the CAE and conducted by logistics, program management, and business experts from outside the program office.

c. After IOC, the DoD Components will continue to conduct ILAs at a minimum interval of every 5 years. DoD Components will provide results to the Assistant Secretary of Defense for Logistics and Materiel Readiness. Assessments will focus on the weapon system-level product support performance in satisfying warfighter needs, meeting sustainment metrics, and providing best-value outcomes. They must specifically assess O&S costs to identify and address factors resulting in growth in O&S costs and adapt strategies to reduce such costs. Results will inform LCSP and analyses updates.

ENCLOSURE 7

HUMAN SYSTEMS INTEGRATION (HSI)

1. PURPOSE. This enclosure describes the HSI policy and procedure applicable to defense acquisition programs.

2. GENERAL. The Program Manager will plan for and implement HSI beginning early in the acquisition process and throughout the product life cycle. The goal will be to optimize total system performance and total ownership costs, while ensuring that the system is designed, operated, and maintained to effectively provide the user with the ability to complete their mission. Program Managers will ensure that the DoD Component HSI staff is aware of and engaged with WIPTs tasked with the development and review of program planning documents that reflect HSI planning and inform program decisions.

3. HSI PLANNING. HSI planning and implementation will address the following seven HSI domains recognized by the DoD:

a. Human Factors Engineering. The Program Manager will take steps (e.g., contract deliverables and government/contractor integrated product teams) to ensure ergonomics, human factors engineering, and cognitive engineering is employed during systems engineering over the life of the program to provide for effective human-machine interfaces and to meet HSI requirements. System designs will minimize or eliminate system characteristics that require excessive cognitive, physical, or sensory skills; entail extensive training or workload-intensive tasks; result in mission-critical errors; or produce safety or health hazards.

b. Personnel. The Program Manager will, in conjunction with designated DoD Component HSI staff, define the human performance characteristics of the user population based on the system description, projected characteristics of target occupational specialties, and recruitment and retention trends. To the extent possible, systems will not require special cognitive, physical, or sensory skills beyond that found in the specified user population. For those programs that have skill requirements that exceed the knowledge, skills, and abilities of current military occupational specialties, or that require additional skill indicators or hard-to-fill military occupational specialties, the Program Manager will consult with personnel communities to mitigate readiness, personnel tempo, and funding issues.

c. Habitability. The Program Manager will, in conjunction with designated DoD Component staff, establish requirements for the physical environment (e.g., adequate space and temperature control) and, if appropriate, requirements for personnel services (e.g., medical and mess) and living conditions (e.g., berthing and personal hygiene) for conditions that have a direct impact on meeting or sustaining system performance or that have such an adverse impact on quality of life and morale that recruitment or retention is degraded.

d. Manpower. In advance of contracting for operational support services, the Program Manager will, in conjunction with the designated DoD Component manpower authority, determine the most efficient and cost-effective mix of DoD manpower and contract support. The mix of military, DoD civilian, and contract support necessary to operate, maintain, and support (to include providing training) the system will be determined based on the manpower mix criteria (see DoD Instruction 1100.22 (Reference (bm))). Manpower mix data will be reported to cost analysts and factored into the preparation of independent cost estimates and DoD Component cost estimates. Economic analyses used to support workforce mix decisions will use costing tools, to include DoD Instruction 7041.04 (Reference (bn)), that account for fully loaded costs (i.e., all variable and fixed costs, compensation and non-compensation costs, current and deferred benefits, and cash and in-kind benefits) approved by the DoD Component manpower authority.

e. Training. The Program Manager will, in conjunction with designated DoD Component staff, develop options for individual, collective, and joint training for operators, maintenance and support personnel, and, where appropriate, base training decisions on training effectiveness evaluations (which can be integrated with other test and evaluation). The major tasks identified in the job task analysis, training device document coordinating paper and training plans will support a comprehensive analysis with special emphasis on options that enhance user capabilities, maintain skill proficiencies, and reduce individual and collective training costs. The Program Manager will develop training system plans that consider the use of new learning techniques, simulation technology, embedded training and distributed learning, and instrumentation systems that provide “anytime, anyplace” training and reduce the demand on the training establishment. Where cost effective and practical, the Program Manager will use simulation-supported embedded training, and the training systems will fully support and mirror the interoperability of the operational system in accordance with DoD Directive 1322.18 (Reference (bo)).

f. Safety and Occupational Health. The Program Manager will ensure that appropriate HSI and environmental, safety, and occupational health efforts are integrated across disciplines and into systems engineering to determine system design characteristics that can minimize the risks of acute or chronic illness, disability, or death or injury to operators and maintainers; and enhance job performance and productivity of the personnel who operate, maintain, or support the system.

g. Force Protection and Survivability. The Program Manager will assess risks to personnel and address, in terms of system design, protection from direct threat events and accidents (such as chemical, biological, and nuclear threats). Design consideration will include primary and secondary effects from these events and consider any special equipment necessary for egress and survivability.

ENCLOSURE 8

AFFORDABILITY ANALYSIS AND INVESTMENT CONSTRAINTS

1. PURPOSE. This enclosure establishes the fundamental concepts and approaches for developing and applying affordability constraints to acquisition programs as part of life-cycle investment analysis, decision making, and management.

2. OVERVIEW

a. Affordability analysis is a DoD Component leadership responsibility that should involve the Component's programming, resource planning, requirements, intelligence, and acquisition communities. The Department has a long history of starting programs that proved to be unaffordable. The result of this practice has been costly program cancelations and dramatic reductions in inventory objectives. Thus, the purpose of Affordability Analysis is to avoid starting or continuing programs that cannot be produced and supported within reasonable expectations for future budgets. Affordability constraints for procurement and sustainment will be derived early in program planning processes. These constraints will be used to ensure capability requirements prioritization and cost tradeoffs occur as early as possible and throughout the program's life cycle.

b. The intent of this policy is to require affordability analysis that addresses the total life cycle of the planned program, including beyond the FYDP. Program life-cycle affordability is a cornerstone of DoD acquisition planning as indicated in DoD Directive 5000.01 (Reference (a)). Affordability within the FYDP is part of the MDA certification and monitoring required by 10 U.S.C. 2366b (Reference (h)) for Major Defense Acquisition Programs (MDAPs) at and beyond Milestone B. Assessing life-cycle affordability of new and upgraded systems is also crucial for establishing fiscal feasibility of the program, informing Analyses of Alternatives (AoAs), guiding capability requirements and engineering tradeoffs, and setting realistic program baselines to control life-cycle costs and help instill more cost-conscious management in the DoD. Affordability analysis and management necessitates effective and ongoing communication with the requirements community on the cost and risk implications of capability requirements.

c. Affordability analysis and constraints are not intended to produce rigid, long-term plans. Rather, they are tools to promote responsible and sustainable investment decisions by examining the likely long-range implications of today's capability requirements choices and investment decisions based on reasonable projections of future force structure equipment needs—before substantial resources are committed to a program.

d. Affordability analysis and affordability constraints are not synonymous with cost estimation and approaches for reducing costs. Constraints are determined in a top-down manner by the resources a DoD Component can allocate for a system, given inventory objectives and all other fiscal demands on the Component. Constraints then provide a threshold for procurement and sustainment costs that cannot be exceeded by the Program Manager. On the other hand, cost

estimates are generated in a bottom-up or parametric manner and provide a forecast of what a product will cost for budgeting purposes. The difference between the affordability constraints and the cost estimates indicates whether actions must be taken to further reduce cost in order to remain within affordability constraints. Independent of affordability constraints or cost estimates, program managers should always be looking for ways to control or reduce cost. Proactive cost control is central to maximizing the buying power of the Department and should be an integral part of all phases and aspects of program management. Cost estimating approaches are discussed in Enclosure 10 of this instruction.

e. When approved affordability constraints cannot be met—even with aggressive cost control and reduction approaches—then technical requirements, schedule, and required quantities must be revisited; this will be accomplished with support from the DoD Component's CSB, and with any requirements reductions proposed to the validation authority. If constraints still cannot be met, and the Component cannot afford to raise the program's affordability cap(s) by lowering constraints elsewhere and obtaining MDA approval, then the program will be cancelled.

3. LIFE- CYCLE AFFORDABILITY ANALYSIS. DoD Components are responsible for developing life-cycle affordability constraints for Acquisition Category (ACAT) I and IA acquisition programs for procurement unit cost and sustainment costs by conducting portfolio affordability analyses that contain a product life-cycle funding projection and supporting analysis. The basic procurement unit cost calculation is the annual estimated procurement budget divided by the number of items that should be procured each year to sustain the desired inventory. (As a simple example, if a Component plans to maintain an inventory of 200,000 trucks, and the trucks have an expected service life of 20 years, then an average of 10,000 trucks must be procured each year. If the Component can afford to spend an average of $1 billion per year on trucks, then the affordability constraint for procurement is $1 billion divided by 10,000, or $100,000 per truck. The Component's requirements for a new truck must be restricted to those that can fit into a $100,000 package. Similar calculations will be made to derive sustainment affordability constraints.) If they are provided, Components will use office of the Under Secretary of Defense for Acquisition, Technology and Logistics standardized portfolios for their analysis. Portfolios can be based on mission areas or commodity types, and will define a collection of products or capabilities that can be managed together for investment analysis and oversight purposes. Components will normally make tradeoffs within portfolios, but if necessary, can and should make tradeoffs across portfolios to provide adequate resources for high-priority programs.

a. A Product Life Cycle, Component Portfolio Analysis (30 to 40 Years Nominal). Component leadership—not the acquisition community or program management—conducts affordability analysis with support and inputs from their programming, resource planning, requirements, intelligence, and acquisition communities. Each Component determines the processes and analytic techniques they use for affordability analysis within the following basic constructs:

(1) Future Budget. A future total budget projection for each DoD Component for affordability analysis provides the first-order economic estimate for allocation of future resources to each portfolio. This projection establishes a nominal rather than optimistic foundation for the future and covers all fiscal demands that compete for resources in the Component, including those outside acquisition and sustainment.

(2) Time Horizon. Component level affordability analysis examines all programs and portfolios together, extending over enough years to reveal the life-cycle cost and inventory implications of planned program for the Component. The same analysis is used as individual programs come up for review. Nominally, affordability analysis covers 30 to 40 years into the future.

(3) Consistency. The aggregation of portfolio cost estimates for each year, when combined with all other fiscal demands on the Component, may not exceed the Component's reasonably anticipated future budget levels.

(4) Fiscal Guidance. Absent specific Component-level guidance by the DCAPE or the Defense Acquisition Executive, each Component projects its topline budget beyond the FYDP using the average of the last 2 years of the current FYDP and the OSD inflator provided by the Under Secretary of Defense (Comptroller) (USD(C)), resulting in zero real growth.

(5) Inflators. Affordability analysis assumes constant purchasing power. Each Component uses the OSD inflator provided by USD(C) in the Component's future total budget projection and to inflate their cost estimates for comparison against affordability constraints, assuming budgets will be adjusted later for any differential inflator issues.

(6) Portfolios. Components will subdivide their accounts into portfolios to facilitate trade-off analysis; but when summed, the total cost for all portfolios and their elements cannot be above the Component's future total budget projection. Components may use existing affordability portfolios, which will be stable between affordability analysis updates. When the analysis is presented for a specific program's review, the Component will employ the relevant portfolio to facilitate understanding and discussion of life-cycle costs and inventories of related acquisition systems.

(7) Other Portfolio Plans. The Component's affordability analyses should be consistent with any relevant existing portfolio plans and strategies such as those required by statute (i.e., the 30-year plans required by 10 U.S.C. 231 (for ships) and 10 U.S.C. 231a (for aircraft) (Reference (h))).

(8) Affordability Analysis Updates. Each Component maintains and updates its affordability analysis as needed at the Component or portfolio level to reflect significant changes such as large cost growths in portfolios and programs, changes in defense strategy, force structure changes, or major budgetary changes.

b. Affordability Analysis Output Format. Each Component's affordability analysis is presented within the governance framework to the MDA in preparation for major acquisition

decisions in a format that demonstrates the affordability of the program within the Component and portfolio context, to ensure that the resulting affordability constraints are understood and consistent with the future total budget projection. Transparency ensures that the risk, cost implications, and alternatives of system acquisitions and sustainment are sufficiently understood by the Component leadership and the programming, resource planning, requirements, intelligence, and acquisition communities.

(1) Data Format. At each major acquisition decision point or milestone, the DoD Component will provide stacked area charts ("sand charts") and underlying spreadsheets. These provide the estimated allocations by year for each program and portfolio of the analysis—including all programs in all portfolios—against the future total budget projection equivalent to the DoD Component's Total Obligation Authority.

(2) Data Requirements for Programs. Affordability analysis must be consistent with the data in the Cost Analysis Requirements Description for a program under review, including the capability requirements, quantity, and schedule used in the analysis. Affordability analysis also provides data to support the procurement and sustainment constraints that will be documented in the ADMs resulting from the Materiel Development Decision (MDD), Milestone A, and Development RFP Release Decision Point, and in the acquisition program baselines normally set at Milestone B and beyond.

c. Timing of Affordability Analysis. Affordability analysis should be conducted as early as possible in a system's life cycle so that it can inform early capability requirements trades and the selection of alternatives to be considered during the AoA. Affordability constraints are not required before the MDD; however, conducting some analysis before that point is beneficial. The best opportunity for ensuring that a program will be affordable is through tailoring capability requirements before and during the AoA(s) and early development. Thus, the Components will incorporate estimated funding streams for future programs within their affordability analyses at the earliest conceptual point and specify those estimates at the MDD and beyond to inform system design and alternative selection.

d. Importance of AoAs to Affordability. Examination of key requirements cost-performance relationships, when merged with affordability analysis results during AoAs, provides the information needed to support sound materiel solution decisions about affordable products.

e. Affordability Constraints: Goals and Caps

(1) Affordability constraints are established to inform the capability requirements validation authority, Program Manager, and AoA team of the cost limitations dictated by the Component's affordability analysis. Early in a program, affordability **goals** are set to inform capability requirements and major design tradeoffs needed to define the product being acquired. Once requirements and the product definition are firm (prior to Milestone B), affordability **caps** are established to provide fixed cost requirements that are functionally equivalent to KPPs. Based on the Component's affordability analysis and recommendations, the MDA will set and enforce affordability constraints as follows:

(a) At MDD. Tentative affordability cost goals (e.g., total funding, annual funding profiles, unit procurement and/or sustainment costs, as appropriate) and inventory goals to help scope the AoA and provide targets around which to consider alternatives.

(b) At Milestone A. Affordability goals for unit procurement and sustainment costs.

(c) At the Development RFP Release Decision Point, Milestone B, and Beyond. Binding affordability caps.

(2) These constraints will be documented in the ADMs for these decision points. At Milestone B and beyond, the affordability caps will be documented in the program's Acquisition Program Baseline. Any programs that do not include a Milestone B decision will receive goals or caps commensurate with their position in the acquisition cycle and their level of maturity.

(3) The metrics used for MDA-approved affordability constraints on procurement and sustainment costs may be tailored to the type of acquisition and the specific circumstances of a given program. In addition to capability requirements tradeoffs approved by the requirements validation authority; prudent investments in research, development, and test and evaluation; innovative acquisition strategies; and incentives to reduce costs can be used to ensure that affordability constraints are achieved.

f. Monitoring and Reporting. The MDA will enforce affordability constraints throughout the life cycle of the program. If a program manager concludes that, despite efforts to control costs and reduce requirements, an affordability constraint will be exceeded, then the Program Manager will notify the Component Acquisition Executive (CAE) and the MDA to request assistance and resolution. Program managers will also report progress relative to affordability constraints at Defense Acquisition Executive Summary reviews.

4. LOWER ACAT PROGRAMS. Each CAE will develop and issue similar guidance to ensure life-cycle affordability for lower ACAT programs that have resource implications beyond the FYDP.

ENCLOSURE 9

ANALYSIS OF ALTERNATIVES (AOA)

1. PURPOSE. The AoA assesses potential materiel solutions that could satisfy validated capability requirement(s) documented in the Initial Capabilities Document, and supports a decision on the most cost effective solution to meeting the validated capability requirement(s). In developing feasible alternatives, the AoA will identify a wide range of solutions that have a reasonable likelihood of providing the needed capability.

2. AOA PROCEDURES

a. The DCAPE develops and approves study guidance for the AoA for potential and designated Acquisition Category (ACAT) I and IA programs and for each joint military or business requirement for which the Chairman of the JROC or the Deputy Chief Management Officer of the Department of Defense (DCMO) is the validation authority. In developing the guidance, the DCAPE solicits the advice of other DoD officials and ensures that the guidance requires, at a minimum:

(1) Full consideration of possible tradeoffs among life-cycle cost, schedule, and performance objectives (including mandatory KPPs) for each alternative considered.

(2) An assessment of whether the joint military requirement can be met in a manner consistent with the cost and schedule objectives recommended by the JROC or other requirements validation authority.

(3) Consideration of affordability analysis results and affordability goals if established by the MDA.

b. The DCAPE provides the AoA Study Guidance to the DoD Component or organization designated by the MDA or, for ACAT IA programs, to the office of the principal staff assistant responsible for the mission area, prior to the Materiel Development Decision (MDD) and in sufficient time to permit preparation of the study plan prior to the decision event. The study plan will be coordinated with the MDA and approved by the DCAPE prior to the MDD. The designated DoD Component or other organization or the principal staff assistant will designate responsibility for completion of the study plan and the AoA.

c. The final AoA written report will be provided to the DCAPE not later than 60 calendar days prior to the Milestone A review (or the next decision point or milestone as designated by the MDA). Not later than 15 business days prior to the Milestone A review, DCAPE evaluates the AoA and provides a memorandum to the MDA, with copies to the DoD Component head or other organization or principal staff assistant assessing whether the analysis was completed consistent with DCAPE study guidance and the DCAPE-approved study plan. In the memorandum, the DCAPE assesses:

(1) The extent to which the AoA:

(a) Examines sufficient feasible alternatives.

(b) Considers tradeoffs among cost, schedule, sustainment, and required capabilities for each alternative considered.

(c) Achieves the affordability goals established at the MDD and with what risks.

(d) Uses sound methodology.

(e) Discusses key assumptions and variables and sensitivity to changes in these.

(f) Bases conclusions or recommendations, if any, on the results of the analysis.

(g) Considers the fully burdened cost of energy (FBCE), in cases where FBCE is a significant discriminator among alternatives.

(2) Whether additional analysis is required.

(3) How the AoA results will be used to influence the direction of the program.

d. The final AoA will also be provided to and reviewed by the requirements validation authority prior to the Milestone A decision or the release of the RFP for the Technology Maturation and Risk Reduction Phase activities. The requirements validation authority will, at a minimum:

(1) Assess how well the recommended alternative satisfies validated requirements in the most cost effective manner for the warfighter.

(2) Identify any opportunities to adjust or align capability requirements for better synergy across the joint force capabilities.

(3) In accordance with the responsibilities identified in Title 10, U.S.C. (Reference (h)), offer alternative recommendations to best meet the validated capability requirements.

ENCLOSURE 10

COST ESTIMATING AND REPORTING

1. PURPOSE. This enclosure describes the primary tools and methods that the DoD uses to ensure that the most cost-effective solution to a validated capability need is chosen, budgets are adequate, and viable cost saving opportunities through multi-year contracting are exploited.

2. COST ESTIMATION

a. Per 10 U.S.C. 2334 (Reference (h)) and DoD Directive 5105.84 (Reference (bp)), the DCAPE provides policies and procedures for the conduct of cost estimates and cost analyses for all DoD acquisition programs, including issuance of guidance relating to program life-cycle cost estimation and risk analysis; reviews cost estimates and cost analyses conducted in connection with Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs; and leads the development of DoD cost community training. The procedures associated with these policies are detailed in DoD Instruction 5000.73 (Reference (w)), DoD Manual 5000.04-M-1 (Reference (at)), and the Office of the Secretary of Defense, Cost Assessment and Program Evaluation, "Operating and Support Cost-Estimating Guide" (Reference (bq)).

(1) The DCAPE conducts Independent Cost Estimates (ICEs) and cost analyses for MDAPs for which the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) is the MDA and as requested by the MDA for other MDAPs:

(a) In advance of any decision to grant Milestone A or Milestone B approval or entry into LRIP or full-rate production.

(b) In advance of any certification pursuant to 10 U.S.C. 2433a (Reference (h)).

(c) At any other time considered appropriate by the DCAPE or upon the request of the MDA.

(2) The DCAPE conducts ICEs and cost analyses for MAIS programs for which the USD(AT&L) is the MDA and as requested by the MDA for other MAIS programs:

(a) In advance of any report pursuant to paragraph (f) of 10 U.S.C. 2445c (Reference (h)).

(b) At any other time considered appropriate by the DCAPE or upon the request of the MDA.

(3) The DCAPE prepares an ICE for Acquisition Category (ACAT) IC and IAC programs at any time considered appropriate by the DCAPE or upon the request of the USD(AT&L) or the MDA.

(4) For MDAPs for which DCAPE does not develop an ICE, the ICE supporting a milestone review decision will be provided to the MDA by the applicable Service Cost Agency or defense agency equivalent following review and concurrence by DCAPE.

(5) DCAPE representatives will meet with representatives from the Service Cost Agency and program office no later than 180 calendar days before the scheduled Development RFP Release Decision Point to determine what cost analysis, if any, will be presented at the decision review and who will be responsible for preparing the cost analysis. Following the meeting, DCAPE will notify the MDA of the type of cost analysis that will be presented. The type of cost analysis will vary depending on the program and the information that is needed to support the decision to release the RFP. For some programs, no new cost analysis may be necessary, and the DCAPE representative will present the Milestone A ICE or an update to the Milestone A ICE. In other cases, the cost analysis may be a cost assessment or a complete ICE.

(6) The DCAPE reviews all cost estimates and cost analyses conducted in connection with MDAPs and MAIS programs, including estimates of operating and support (O&S) costs for all major weapon systems. To facilitate the review of cost estimates, the DCAPE receives the results of all cost estimates and cost analyses and associated studies conducted by the DoD Components for MDAPs and MAIS programs.

(7) The DCAPE, DoD Components, and Service Cost Agencies will be provided timely access to any records and data in the DoD (including the records and data of each military department and defense agency, to include classified, unclassified, and proprietary information) it considers necessary to review cost analyses and conduct the ICEs and cost analyses described in sections 2 and 3 of this enclosure.

(8) For MDAP and MAIS programs, the DCAPE participates in the discussion of issues related to and/or differences between competing program cost estimates, comments on methodologies employed and the estimate preparation process, coordinates on the cost estimate used to support establishment of baselines and budgets, and participates in the consideration of any decision to request authorization of a multi-year procurement contract for an MDAP.

(9) The documentation of each MDAP or MAIS program cost estimate prepared by DCAPE and/or Service or Agency includes the elements of program cost risk identified and accounted for, how they were evaluated, and possible mitigation measures. DCAPE then assesses the proposed program's baseline and associated program budget's ability to provide the necessary high degree of confidence that the program can be completed without the need for significant adjustment to future program budgets. If the MDAP or MAIS program baseline or budget determined by DCAPE as appropriately high confidence is not adopted by the MDA, the MDA will document the rationale for the decision. For MDAPs, the next Selected Acquisition Report prepared in compliance with 10 U.S.C. 2432 (Reference (h)), and for MAIS programs, the next quarterly report prepared in compliance with 10 U.S.C. 2445c will disclose the

confidence level used in establishing the cost estimate for the MDAP or MAIS program and the rationale for selecting the confidence level.

(10) In addition to O&S cost estimates included in the ICEs conducted at the reviews identified in paragraphs 2a(1) through 2a(4) of this enclosure, Military Departments must update estimates of O&S costs periodically throughout the life cycle of a major weapon system to determine whether preliminary information and assumptions remain relevant and accurate and to identify and record reasons for variances. Further, an independent review of O&S cost estimates must be conducted at post-Initial Operational Capability reviews. Each O&S cost estimate must be compared to earlier cost estimates and the program's O&S affordability cap, and, as appropriate, this information will be used to update the life-cycle affordability analysis provided to the MDA and requirements validation authority. This comparison must identify the reasons for significant changes and categorize those reasons into external and internal factors.

b. The MDA may request that the DCAPE, within the DCAPE's discretion, develop cost assessments for any other program regardless of its ACAT.

c. Per 10 U.S.C. 2434 (Reference (h)), the MDA may not approve the engineering and manufacturing development or the production and deployment of an MDAP unless an independent estimate of the full life-cycle cost of the program, prepared or approved by the DCAPE, has been considered by the MDA.

d. The DoD Component will develop a DoD Component Cost Estimate that covers the entire life cycle of the program for all MDAPs prior to Milestone A, B, and C reviews and the Full-Rate Production Decision; and for all MAIS programs at any time an Economic Analysis is due.

e. The DoD Component and the Service Cost Agency will establish a documented DoD Component Cost Position that covers the entire life cycle of the program for all MDAPs and MAIS programs prior to the Milestone A, B, and C reviews, and the Full-Rate Production Decision or Full Deployment Decision Review. The DoD Component Cost Position must be signed by the appropriate DoD Component Deputy Assistant Secretary for Cost and Economics (or defense agency equivalent) and must include a date of record.

f. At the Milestone A, B, and C reviews and for the Full-Rate Production Decision or Full Deployment Decision review, the DoD Component must fully fund the program to the Component Cost Position in the current FYDP, or commit to full funding of the cost position in the next FYDP, with identification of specific offsets to address any funding shortfalls that may exist in the current FYDP. The Component Acquisition Executive and the DoD Component Chief Financial Officer must endorse and certify in the Full Funding Certification Memorandum that the FYDP fully funds, or will fully fund, the program consistent with the DoD Component Cost Position. If the program concept evolves after a milestone review, the Service Cost Agency may update the DoD Component Cost Position, and the DoD Component may fully fund the program in the FYDP to the updated DoD Component Cost Position.

3. COST ANALYSIS REQUIREMENTS DESCRIPTION (CARD). The foundation of a sound and credible cost estimate is a well-defined program. The DCAPE requires use of the CARD and provides guidance on the content of the CARD in DoD Instruction 5000.73 (Reference (w)) to provide that foundation. For ACAT I and IA programs, the Program Manager will prepare, and an authority no lower than the DoD Component PEO will approve, the CARD. For joint programs, the CARD will cover the common program as agreed to by all participating DoD Components, as well as any DoD Component-unique requirements. The DCAPE and the organization preparing the DoD Component Cost Estimate must receive a draft CARD 180 calendar days, and the final CARD 45 calendar days, prior to a planned OIPT or equivalent staff coordination body review or DoD Component review, unless DCAPE agrees to other due dates. The Program Manager and PEO will insure the draft and final CARDs are consistent with other final program documentation.

a. Recognizing that program details are refined over time, with fewer details available for MDAPs and MAIS programs approaching Milestone A than Milestone B, DCAPE will provide CARD development guidance tailored to the specific review being conducted and the type of system being developed. However, all CARDs, no matter how tailored, will provide a program description that includes a summary of the acquisition approach; expected constraints; system characteristics; quantities; operational factors; operational support strategy; manpower, personnel, and training requirements; preliminary schedules; test programs; technology maturation and risk reduction plans; and appropriate system analogs. Additional content may be required as requested by DCAPE.

b. When Milestone A occurs prior to release of the Technology Maturation and Risk Reduction Phase RFP, the DCAPE or DCAPE-approved DoD Component ICE will not be able to reflect information provided by the competing contractors in their proposals. Should the contractor proposed solutions entering the Technology Maturation and Risk Reduction Phase differ significantly from the design reflected in the Milestone A CARD, the Program Manager will report any differences that might alter the basis for the MDA's Milestone A decision to DCAPE and the MDA. The MDA will determine whether an additional review is required prior to contract award.

c. At the Development RFP Release Decision Point, the program described in the final CARD will reflect the Program Manager's and PEO's best estimate of the materiel solution that will be pursued following Milestone B. The final CARD will be updated to reflect all new program information prior to Milestone B.

4. DATA TO SUPPORT COST ESTIMATING. Standardized data collection procedures and formats are essential for credible cost estimates for current and future programs. DCAPE establishes procedural guidance for cost data collection and monitoring systems. Table 7 in Enclosure 1 of this instruction provides detailed information on Cost and Software Data Reporting (CSDR) requirements.

a. DoD has three primary sources for data to use for cost estimation: CSDR, the Integrated Program Management Report, and the Visibility and Management of Operating and Support

Costs (VAMOSC) systems. The CSDR and the Integrated Program Management Report instruments serve as the primary sources of data when estimating acquisition costs for major contracts and subcontracts associated with MDAPs and MAIS programs. DCAPE defines procedural and standard data formatting requirements for the CSDR system in DoD Manual 5000.04-M-1 (Reference (at)). Formats and reporting requirements for Integrated Program Management Reports are determined and managed by USD(AT&L). VAMOSC data systems are managed by each Military Department and collect historical O&S costs for major fielded weapon systems. DCAPE conducts annual reviews of VAMOSC systems to address data accessibility, completeness, timeliness, accuracy, and compliance with CAPE guidance. The annual reviews also assess the adequacy of each military department's funding and resources for its VAMOSC systems. DoD Instruction 5000.73 (Reference (w)) provides the procedural and data reporting requirements for VAMOSC.

b. The two components of the CSDR system are Contractor Cost Data Reporting and Software Resources Data Reporting. CSDR plans are developed pursuant to the requirements in DoD Manual 5000.04-M-1, and are required for each phase of program acquisition. Proposed CSDR plan(s) for ACAT I and IA programs must be approved by DCAPE prior to the issuance of a contract solicitation. The DCAPE has the authority to waive the information requirements of Table 7. Program managers will use the CSDR system to report data on contractor costs and resource usage incurred in performing DoD programs.

c. In addition to the historic O&S cost data stored in VAMOSC systems, each program must also retain and submit to CAPE, DoD Component and Service Cost Agency O&S cost estimates developed at any time during the life cycle of a major weapon system, together with copies of reports, briefings, and other supporting documentation that were used to prepare the cost estimates. This includes documentation used to prepare cost estimates for acquisition milestones or other program reviews, as well as O&S cost estimates incorporated into Selected Acquisition Reports.

5. DCAPE PROCEDURES. The DoD Component responsible for acquisition of a system will provide the cost, programmatic, and technical information required for estimating costs and appraising programmatic risks to DCAPE. The DoD Component will also facilitate DCAPE staff visits to the program office, product centers, test centers, and system contractor(s) as DCAPE deems necessary to support development of its cost estimate or assessment. The process through which the ICE is prepared will be consistent with the policies set forth in DoD Instruction 5000.73 (Reference (w)). The DCAPE's current policies and procedures are as follows, but may be modified by DCAPE according to program needs:

a. DCAPE representatives participate in integrated product team meetings (i.e., cost WIPTs).

b. The DCAPE, DoD Component, and Program Manager:

(1) Share data and use the same CARD.

(2) Raise and resolve issues in a timely manner and at the lowest possible level.

(3) Address differences between the ICE, the DoD Component cost estimate, and the DoD Component cost position.

c. The Program Manager will identify issues projected to be brought to the OIPT to the DCAPE in a timely manner.

d. For joint programs:

(1) The lead DoD Component or executive agent will prepare the DoD Component Cost Estimate.

(2) All DoD Components involved must either jointly sign or individually submit a DoD Component Cost Position and Full Funding Certification Memorandum.

6. MULTI-YEAR PROCUREMENT—COST ANALYSIS REQUIREMENTS

a. General. In accordance with 10 U.S.C. 2306b (Reference (h)), a multi-year procurement contract is a contract for the purchase of property for more than 1, but not more than 5, program years. Multi-year contracts in an amount equal to or greater than $500 million may not be entered into unless the contract is specifically authorized by law in an Act other than an appropriations Act. In accordance with 10 U.S.C. 2306b, when submitting a request for authorization for a multi-year contract, the Secretary of Defense must include in the request a report containing the preliminary findings of the DoD Component head regarding the following:

(1) The use of such a contract will result in significant savings of the total anticipated costs of carrying out the program through annual contracts.

(2) The minimum need for the property to be purchased is expected to remain substantially unchanged during the contemplated contract period in terms of production rate, procurement rate, and total quantities.

(3) There is a reasonable expectation that throughout the contemplated contract period the head of the DoD Component will request funding for the contract at the level required to avoid contract cancellation.

(4) There is a stable design for the property to be acquired and the technical risks associated with such property are not excessive.

(5) The estimates of both the cost of the contract and the anticipated cost avoidance through the use of a multi-year contract are realistic.

(6) The use of such a contract will promote the national security of the United States.

b. CAPE Role and Requirements. Prior to the Secretary's submission under paragraph 6a, DCAPE is required to complete a cost analysis and determine such analysis supports the DoD Component head's findings in paragraph 6a of this enclosure. In order for DCAPE to complete the cost analysis in a timely manner, the DoD Component head must submit a list of multi-year procurement contract candidates and supporting information to DCAPE no later than October 1 of the fiscal year prior to the fiscal year in which the request for legislative authority, with accompanying certification, will be made.

c. Additional Requirements. 10 U.S.C. 2306b (Reference (h)) sets forth several other requirements for multi-year contracts. Prior to requesting authority to enter into a multi-year contract, the program manager should consult with his or her agency's counsel to confirm that the proposed multi-year contract complies with all relevant statutes and regulations.

ENCLOSURE 11

REQUIREMENTS APPLICABLE TO ALL PROGRAMS CONTAINING INFORMATION TECHNOLOGY (IT)

1. PURPOSE. This enclosure identifies the additional policy and procedure that apply to all programs containing IT, including National Security Systems (NSS).

2. APPLICABILITY. This enclosure applies to:

a. IT, as defined in title 40 of U.S. Code (Reference (p)), is any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services, and related resources). IT is equipment used by the DoD directly or is used by a contractor under a contract with the DoD that requires the use of that equipment. IT does not include any equipment acquired by a federal contractor incidental to a federal contract.

b. NSS, as defined in 44 U.S.C. 3552 (Reference (aw)), are telecommunications or information systems operated by or on behalf of the Federal Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or, is critical to the direct fulfillment of military or intelligence missions. NSS do not include systems that are used for routine administrative and business applications (including payroll, finance, and personnel management applications).

c. Information systems, as defined in 44 U.S.C. 3502 (Reference (aw)), are a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

3. CLINGER-COHEN ACT (CCA) COMPLIANCE. Subtitle III of title 40 of U.S. Code (Reference (p)) (formerly known as Division E of CCA) (hereinafter referred to as “CCA”) applies to all IT investments, including NSS.

a. For all programs that acquire IT, including NSS, at any acquisition category (ACAT) level, the MDA will not initiate a program nor an increment of a program, or approve entry into any phase of the acquisition process that requires formal acquisition milestone approval, and the DoD Component will not award a contract for the applicable acquisition phase until:

(1) The sponsoring DoD Component or program manager has satisfied the applicable acquisition phase-specific requirements of the CCA as shown in Table 10 in Enclosure 1 of this instruction; and

(2) The Program Manager has reported CCA compliance to the MDA and the DoD Component Chief Information Officer (CIO), or their designee.

b. Table 10 in Enclosure 1 of this instruction identifies the specific requirements for CCA compliance. These requirements will be satisfied to the maximum extent practicable through documentation developed under the JCIDS and the Defense Acquisition System. To report compliance, the Program Manager will prepare a table similar to Table 10 to indicate which documents demonstrate compliance with the CCA requirements. The Program Manager's table will provide links to the cited documents and serve as Program Manager's "CCA Compliance Report."

4. POST IMPLEMENTATION REVIEW (PIR). The functional sponsor, in coordination with the Component CIO and Program Manager, is responsible for developing a plan and conducting a PIR for all fully deployed IT, including NSS. PIRs will report the degree to which doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy changes have achieved the established measures of effectiveness for the desired capability; evaluate systems to ensure positive return on investment and decide whether continuation, modification, or termination of the systems is necessary to meet mission requirements; and document lessons learned from the PIR. If the PIR overlaps with Follow-on Operational Test and Evaluation, the sponsor should coordinate planning of both events for efficiency. The preparation of the TEMP and the MDA's decision to proceed with full-rate production satisfy the requirement for weapons systems. The post fielding assessment(s), the disposition assessment, and the disposition decision for an urgent need (as described in Enclosure 12), meet the requirement for a PIR.

5. DOD INFORMATION ENTERPRISE ARCHITECTURE. The DoD Information Enterprise Architecture will underpin all information architecture development to realize the Joint Information Environment. Program Managers must develop solution architectures that comply with the DoD Information Enterprise Architecture, applicable mission area and component architectures, and DoD Component architecture guidance. A program's solution architecture should define capability and interoperability requirements, establish and enforce standards, and guide security and cybersecurity requirements. The standards used to form the Standard Viewpoints of integrated architectures will be selected from those contained in the current approved version of the DoD IT Standards Registry within the Global Information Grid Technical Guidance Federation service (Reference (br)). The IT will be tested to measures of performance derived from the solution architecture.

6. CYBERSECURITY

a. Cybersecurity Risk Management Framework (RMF). Cybersecurity RMF steps and activities, as described in DoD Instruction 8510.01 (Reference (bg)), should be initiated as early as possible and fully integrated into the DoD acquisition process including requirements management, systems engineering, and test and evaluation. Integration of the RMF in acquisition processes reduces required effort to achieve authorization to operate and subsequent management of security controls throughout the system life cycle.

b. Cybersecurity Strategy. All acquisitions of systems containing IT, including NSS, will have a Cybersecurity Strategy. The Cybersecurity Strategy is an appendix to the Program Protection Plan (PPP) that satisfies the statutory requirement in section 811 of P.L. 106-398 (Reference (q)) for mission essential and mission critical IT systems. Beginning at Milestone A, the Program Manager will submit the Cybersecurity Strategy to the cognizant Component CIO for review and approval prior to milestone decisions or contract awards.

(1) For ACAT ID, IAM, and IAC programs, the DoD CIO will review and approve the Cybersecurity Strategy prior to milestone decisions or contract awards.

(2) CIOs will document the results of all reviews.

(3) If contract award is authorized as part of an acquisition milestone decision, a separate review of the Cybersecurity Strategy prior to contract award is not required.

(4) The approved Cybersecurity Strategy will be an appendix to the PPP.

7. TRUSTED SYSTEMS AND NETWORKS (TSN). Program managers of NSS; systems that have a high impact level for any of the three security objectives, Confidentiality, Integrity, or Availability; or other DoD information systems that the Component Acquisition Executive or Component CIO determines to be critical to the direct fulfillment of military or intelligence missions must identify and protect mission critical functions and components as required by DoD Instruction 5200.44 (Reference (aj)). TSN plans and implementation activities are documented in PPPs and relevant cybersecurity plans and documentation (see section 13 in Enclosure 3 of this instruction for additional details). Program managers will manage TSN risk by:

a. Conducting a criticality analysis to identify mission critical functions and critical components and reducing the vulnerability of such functions and components through secure system design.

b. Requesting threat analysis of suppliers of critical components (Supplier All Source Threat Analysis).

c. Engaging the pertinent TSN focal point for guidance on managing identified risk.

d. Applying TSN best practices, processes, techniques, and procurement tools prior to the acquisition of critical components or their integration into applicable systems.

8. LIMITED DEPLOYMENT FOR A MAJOR AUTOMATED INFORMATION SYSTEM (MAIS) PROGRAM. At Milestone C, the MDA for a MAIS program will approve, in coordination with the DOT&E, the quantity and location of sites for a limited deployment of the system for Initial Operational Test and Evaluation. MDAs, in coordination with DOT&E, may also make this determination at Milestone B for incrementally deployed programs, consistent with the procedures in paragraph 5c(3)(d) in this instruction.

9. CLOUD COMPUTING. Cloud computing services can deliver more efficient IT than traditional acquisition approaches. Program managers will acquire DoD or non-DoD provided cloud computing services when the business case analysis determines that the approach meets affordability and security requirements. Program managers will ensure that cloud services are implemented in accordance with Defense Information Systems Agency (DISA) provided Cloud Computing Security Requirements Guidance; and will only use cloud services that have been issued both a DoD Provisional Authorization by DISA and an Authority to Operate by their Component's Authorizing Official. In addition, non-DoD cloud services used for Sensitive Data must be connected to customers through a Cloud Access Point that has been approved by the DoD CIO. Program managers report cloud service funding investments through the submission of the Office of Management of Budget (OMB) Exhibit 53 in accordance with OMB Circular A-11(Reference (c)).

10. DOD ENTERPRISE SOFTWARE INITIATIVE (ESI). When acquiring commercial IT, Program Managers must consider the DoD ESI, Federal Strategic Sourcing Initiative procurement vehicles, and Defense Component level Enterprise Software Licenses. The Defense Federal Acquisition Regulation Supplement subpart 208.74 (Reference (al)) and OMB Policy Memorandums M-04-08, M-04-16 and M-05-25 (References (bt) through (bv)) and the DoD ESI web site at http://www.esi.mil/ provide additional detail.

11. DOD DATA CENTER CONSOLIDATION. Any program manager who intends to obligate funds for data servers, data centers, or the information systems technology used therein, must obtain prior approval from the DoD CIO. The request must be signed by the Component CIO and include a completed request for the Authorization of Funds for Data Centers and Data Server Farms in accordance with section 2867 of P.L. 112-81 (Reference (v)).

12. IT, INCLUDING NSS, INTEROPERABILITY. To achieve the information superiority and interoperability goals of DoD Directive 5000.01 (Reference (a)), program managers will design, develop, test and evaluate systems to ensure IT interoperability requirements are achieved. At key decision points and acquisition milestones, interdependencies, dependencies, and synchronization with complementary systems must be addressed. The Program Manager will

ensure that interoperability certification is achieved in accordance with DoD Instruction 8330.01 (Reference (ab)).

13. DATA PROTECTION. Program managers of DoD IT systems (including those supported through contracts with external sources) that collect, maintain, use, or disseminate data must protect against disclosure to non-approved sources while meeting the organization's record keeping needs.

a. Personally Identifiable Information (PII) must be managed in a manner that protects privacy. PII will be collected, maintained, disseminated, and used in accordance with DoD Directive 5400.11 (Reference (bw)) and DoD Regulation 5400.11-R (Reference (bx)). Privacy Impact Assessments will be managed in accordance with DoD Instruction 5400.16 (Reference (by)).

b. Scientific and technical information must be managed to make scientific knowledge and technological innovations fully accessible to the research community, industry, the military operational community, and the general public within the boundaries of law, regulation, other directives, and executive requirements, in accordance with DoD Instruction 3200.12 (Reference (bz)).

c. 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 5015.02-STD (Reference (bc)) for additional information on the DoD Records Management Program). Electronic record-keeping systems must preserve the information submitted, as required by 44 U.S.C. 3101 (Reference (aw)) and implementing regulations. Program managers will develop data archiving plans that delineate how records are collected, created, and stored within their systems. These plans must include processes for disposition of both temporary and permanent records. Program managers should work with Component records managers early and throughout the acquisition process.

14. SECTION 508 - ACCESSIBILITY OF ELECTRONIC AND INFORMATION TECHNOLOGY FOR INDIVIDUALS WITH DISABILITIES. Program managers will ensure that electronic and information technology developed, procured, maintained, and used by the DoD will allow persons with disabilities access to information comparable to that afforded persons without disabilities, in accordance with section 508 of the Rehabilitation Act (i.e., 29 U.S.C. 794d (Reference (ca))). For exceptions to section 508 compliance, refer to DoD Manual 8400.01-M (Reference (cb)).

ENCLOSURE 12

URGENT CAPABILITY ACQUISITION

1. PURPOSE. This enclosure provides policy and procedure for acquisition programs that provide capabilities to fulfill urgent operational needs and other quick reaction capabilities that can be fielded in less than 2 years and are below the cost thresholds of Acquisition Category (ACAT) I and IA programs.

2. URGENT OPERATIONAL NEEDS AND OTHER QUICK REACTION CAPABILITIES

a. DoD's highest priority is to provide warfighters involved in conflict or preparing for imminent contingency operations with the capabilities urgently needed to overcome unforeseen threats, achieve mission success, and reduce risk of casualties, as described in DoD Directive 5000.71 (Reference (cc)). The objective is to deliver capability quickly, within days or months. DoD Components will use all available authorities to expeditiously fund, develop, assess, produce, deploy, and sustain these capabilities for the duration of the urgent need, as determined by the requesting DoD Component. Approval authorities for each acquisition program covered by this enclosure will be delegated to a level that promotes rapid action.

b. This enclosure applies to acquisition programs for the following types of quick reaction capabilities:

(1) A validated Urgent Operational Need (UON). UONs include:

(a) Joint Urgent Operational Needs (JUONs) and Joint Emergent Operational Needs (JEONs). These are either an urgent need identified by a Combatant Commander, the Chairman of the Joint Chiefs of Staff (CJCS), or the Vice Chairman of the Joint Chiefs of Staff (VCJCS) involved in an ongoing contingency operation (i.e., a JUON) or an emergent need identified by a Combatant Commander, CJCS, or VCJCS for an anticipated or pending contingency operation (i.e., a JEON). For JUONs and JEONs, the validation approval will be by the Joint Staff in accordance with the Joint Capability Integration Development System (JCIDS) detailed in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01I (Reference (e)). Program execution for JUONs and JEONs will be assigned in accordance with DoD Directive 5000.71. The MDA for JUONs and JEONs will be determined at the DoD Component level except in very rare cases when the MDA will be designated in an ADM by the Defense Acquisition Executive (DAE).

(b) DoD Component-specific UON. These are defined in CJCSI 3170.01I and further discussed in DoD Directive 5000.71. Approval authorities for DoD Component UONs, including their validation, program execution, and the designation of the MDA, will be at the DoD Component level.

(2) A Warfighter Senior Integration Group (SIG)-Identified Urgent Issue. This is a critical warfighter issue, e.g., materiel support to a coalition partner, identified by the Co-Chairs of the Warfighter SIG in accordance with DoD Directive 5000.71. The Co-Chairs of the Warfighter SIG will approve a critical warfighter issue statement and provide instructions to DoD Component(s) on program execution and management.

(3) A Secretary of Defense or Deputy Secretary of Defense Rapid Acquisition Authority (RAA) Determination. This is a Secretary of Defense or Deputy Secretary of Defense signed determination that is made in response to a documented deficiency following consultation with the Joint Staff. RAA should be considered when, within certain limitations, a waiver of a law, policy, directive, or regulation will greatly accelerate the delivery of effective capability to the warfighter in accordance with section 806(c) of P.L. 107-314 (Reference (cd)).

3. PROCEDURES

a. MDAs and program managers will tailor and streamline program strategies and oversight. This includes program information, acquisition activity, and the timing and scope of decision reviews and decision levels. Tailoring and streamlining should be based on program complexity and the required timelines to meet urgent need capability requirements consistent with applicable laws and regulations.

b. DoD Components will employ, to the extent possible, parallel rather than sequential processes to identify and refine capability requirements, identify resources, and execute acquisitions to expedite delivery of solutions. Formal milestone events may not be required. Acquisition decision making and associated activity will be tailored to expedite acquisition of the capability. Development will generally be limited, and the MDA can authorize production at the same time development is approved.

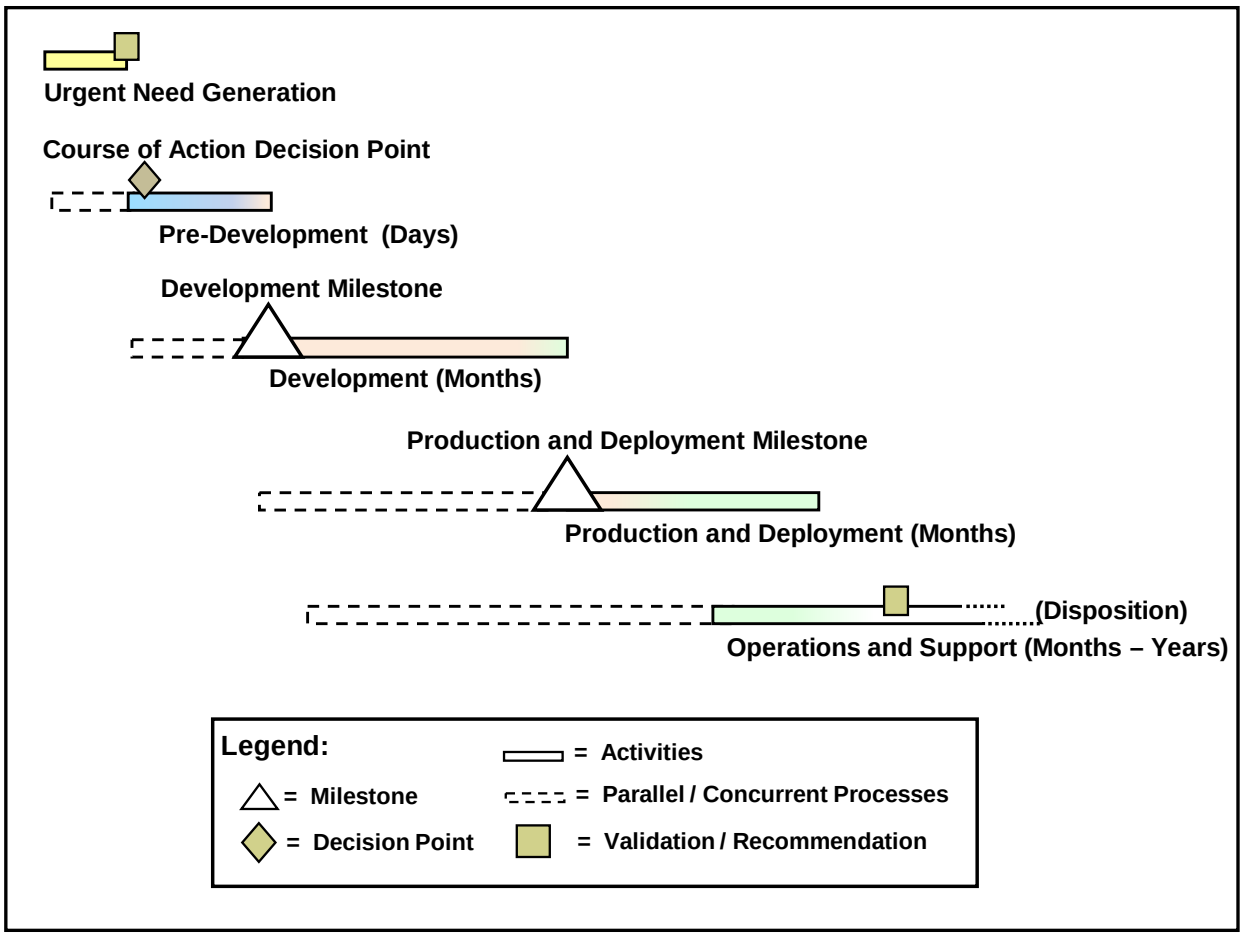
c. DoD Components will ensure that financial, contracting, and other support organizations (e.g., Defense Contract Audit Agency, Defense Contract Management Agency, General Counsel) and prime and subcontractors involved with aspects of the acquisition program are fully aware of the urgency of the need and will ensure expedited action.

d. Generally, funds will have to be reprioritized and/or reprogrammed to expedite the acquisition process. If a capability can be fielded within an acceptable timeline through the normal Planning, Programming, Budgeting, and Execution System, it would not be considered appropriate for urgent capability acquisition.

e. Consistent with the emphasis on urgency, if the desired capability cannot be delivered within 2 years, the MDA will assess the suitability of partial or interim capabilities that can be fielded more rapidly. In those cases, the actions necessary to develop the desired solution may be initiated concurrent with the fielding of the interim solution. Critical warfighter issues identified by the Warfighter SIG, per DoD Directive 5000.71 (Reference (cc)), will be addressed as determined by the Co-Chairs of the Warfighter SIG.

4. URGENT CAPABILITY ACQUISITION ACTIVITIES. The following paragraphs describe the main activities associated with Urgent Capability Acquisitions: Pre-Development, Development, Production and Deployment (P&D), and Operations and Support (O&S). The activities detailed in this enclosure are not separate from or in addition to activities performed as part of the acquisition system but are a highly tailored version of those activities and are intended to expedite the fielding of capability by tailoring the documentation and reviews normally required as part of the deliberate acquisition process. Figure 10 depicts a representative acquisition.

Figure 10. Urgent Capability Acquisitions



a. Pre-Development

(1) Purpose. The purpose of Pre-Development is to assess and select a course or courses of action to field a quick reaction capability and to develop an acquisition approach.

(2) Initiation. Pre-Development begins upon receipt of either a validated UON, approval of a critical warfighter issue statement by the co-chairs of the Warfighter SIG per DoD Directive

5000.71, or a Secretary of Defense or Deputy Secretary of Defense RAA determination document, where the associated documentation serves as the justification to continue the action until such time as the disposition action discussed in paragraph 4e(5) of this enclosure.

(3) Pre-Development Activities

(a) Upon Pre-Development initiation, the designated Component Acquisition Executive (CAE) will immediately appoint a Program Manager and an MDA. If the DAE has retained MDA authority, he or she will either appoint a Program Manager or task a CAE to do so.

(b) The Program Manager in collaboration with the intended user and the requirements validation authority:

1. Assesses the required capability and any recommended non-materiel options and, if not adequately stated, determines the performance thresholds for the minimal set of performance parameters required to mitigate the capability gap.

2. Performs an analysis of potential courses of action, if not already performed, that considers:

a. The range of feasible capabilities, near, mid, and/or long term, to include consideration of an existing domestic or foreign-made system.

b. The acquisition risk (cost, schedule, and performance) and the operational risk of each solution.

c. The operational risk to the requesting Commander if an effective solution is not deployed in the time specified by the Commander.

3. Presents a recommended course of action for review and approval by the MDA.

4. If the Program Manager is unable to identify an effective solution, the Program Manager will notify the MDA. The MDA will in turn notify the DoD Component validation authority. If it is a JUON or JEON, a critical warfighter issue identified by the Warfighter SIG, or a Secretary of Defense RAA Determination, the MDA will notify the DAE and the requirements validation authority through the Director, Joint Rapid Acquisition Cell (JRAC), and the Deputy Director of Requirements, Joint Staff.

(c) The Program Manager will present the recommended course(s) of action to the MDA and the requirements validation authority. The selected course of action will be documented in an ADM. More than one course of action may be selected to provide the phased or incremental fielding of capabilities.

(d) For each approved course of action, the Program Manager will develop a draft Acquisition Strategy and an abbreviated program baseline based on readily available information. In the context of this enclosure, the documentation requirement is for the minimal amount necessary to define and execute the program and obtain MDA approval. This documentation may take any appropriate, written form; will typically be coordinated only with directly affected stakeholders; and will evolve in parallel with urgent capability acquisition activities as additional information becomes available as a result of those activities.

(e) The Acquisition Strategy will comply with the requirements in Table 11 of this enclosure and the items in Table 2 of Enclosure 1 that are required for ACAT II and III programs (unless modified by Table 11); however, a streamlined, highly tailored strategy consistent with the urgency of the need will be employed. Regulatory requirements will be tailored or waived. The tailored Acquisition Strategy should be relatively brief and contain only essential information, such as resourcing needs and sources, key deliverables, performance parameters, key risks and mitigation approaches, a production schedule, a contracting methodology and key terms, preliminary plans for assessment (which may or may not include test and evaluation (T&E)), deployment, training, and sustainment. Information technology (IT), including National Security Systems (NSS), provided in response to an urgent need require an Authority to Operate in accordance with DoD Instruction 8510.01 (Reference (bg)). A disposition decision should be made as early as feasible and decided upon at appropriate milestones or other decision points.

(f) Funding for the acquisition program may be in increments over the program's life cycle. The program life cycle begins upon Pre-Development initiation and ends upon completing the final disposition of the capability as described in the O&S portion of this enclosure.

(g) When designing the Acquisition Strategy, the Program Manager, in collaboration with the requesting operational commander or sponsoring user representative will determine whether an operational prototype is necessary and include this determination in the Acquisition Strategy.

(h) If the program has been placed under DOT&E oversight, a plan for operational testing must be approved by the DOT&E. DOT&E will report the results of required testing to the Secretary of Defense and provide copies to Congress and the MDA.

b. Development Milestone. Entry into Development is approved by the MDA.

(1) The Program Manager will provide the Acquisition Strategy and Program Baseline to include the program requirements, schedule, activities, program funding, and the assessment approach and intermediate decision points and criteria as the basis for this decision.

(2) The MDA will:

(a) Determine the feasibility of fielding the capability within the required timelines to include consideration of the technical maturity of the preferred solution(s).

(b) Review the Acquisition Strategy and Program Baseline and determine whether the preferred solution(s):

1. Can be fielded within 2 years.

2. Does not require substantial development effort.

3. Is based on technologies that are proven and available.

4. Can be acquired under a fixed price contract.

(c) Provide any exceptions necessary pursuant to section 804 (b)(3) of P.L. 111-383 (Reference (m)), including exceptions to the requirements of paragraphs 4b(2)(b)1 through 4b(2)(b)4.

(d) Approve initial quantities to be produced and assessed (to include required assessment and training articles).

(e) Approve the tailored Acquisition Strategy and Acquisition Program Baseline. These documents will be based on available information to be updated over time as directed by the MDA.

(f) Decide if RAA, in accordance with section 806(c) of P.L. 107-314 (Reference (cd)), should be requested from the Secretary of Defense or Deputy Secretary of Defense to expedite the fielding of the capability.

(g) Approve the planned testing approach. A normal Test and Evaluation Master Plan (TEMP) is generally not necessary. TEMPs are usually not appropriate for urgent capability acquisitions when there is minimal development work and minimal T&E to execute. Some test planning is usually required, however. In collaboration with the supporting operational test organization, a highly tailored and abbreviated test plan may be required by the MDA. The abbreviated test plan will describe a performance assessment approach that will include schedule, test types and environment, and assets required. An Operational Test Plan for the required pre-deployment performance assessment is generally adequate. If the defense urgent capability acquisition program is under DOT&E oversight, a TEMP is also not normally required; however, the Program Manager should prepare a combined operational and live fire test plan for DOT&E approval.

(h) Approve any appropriate waivers to statute or regulation. Specify any additional authority the Program Manager may use to modify the acquisition approach without the specific approval of the MDA.

(i) Authorize release of the RFP and related documents for development and any other MDA approved actions.

(j) Document these decisions in an ADM.

c. Development Activities

(1) Development includes an assessment of the performance, safety, suitability, and survivability of the capability, but does not require that all identified deficiencies including those related to safety be resolved prior to production or deployment. The MDA will, in consultation with the user and the requirements validation authority, determine which deficiencies must be resolved and what risks can be accepted.

(2) IT, including NSS, fielded under this enclosure require an Authority to Operate in accordance with DoD Instruction 8510.01 (Reference (bg)). DoD Component Chief Information Officers will establish processes consistent with DoD Instruction 8510.01 for designated approval authorities to expeditiously make the certification determinations and to issue Interim Authorization to Test or Authority to Operate.

d. P&D Milestone

(1) Entry into P&D is approved by the MDA.

(2) At the P&D Milestone review:

(a) The Program Manager will summarize the results of Development activity and the program assessment to date. The Program Manager will present plans to transport, deploy, and sustain the capability; to conduct Post-Deployment Assessments; and to train maintenance and operating personnel. This information will be provided to the MDA for approval.

(b) The MDA, in consultation with the supporting operational test organization, and with the concurrence of DOT&E for programs under DOT&E oversight, will determine:

1. Whether the capability has been adequately reviewed, performs satisfactorily, is supportable, and is ready for production and deployment.

2. When assessments of fielded capabilities are required.

(c) The MDA decides whether to produce and, in coordination with the requester/user, deploy (field) the system, approves the updated Acquisition Strategy (which will include the sustainment plan) and Program Baseline, and documents the Production Decision in an ADM.

(3) P&D Activities

(a) During P&D the acquiring organization provides the warfighter with the needed capability, to include any required training, spares, technical data, computer software, support equipment, maintenance, or other logistics support necessary for operation.

1. DoD Components will ensure that the capability and required support (e.g., field service representatives, training) are deployed by the most expeditious means possible and tracked through to their actual delivery to the user.

2. The DoD Components will coordinate with each other and the requiring activity to verify the total number of items required, considering necessary support and spares and training assets for deployed and/or pre-deployment training.

(b) Upon deployment, the capability will enter O&S.

e. O&S

(1) The Program Manager will execute a support program that meets materiel readiness and operational support performance requirements, and sustains the capability in the most cost-effective manner over its anticipated total life cycle. Planning for O&S will begin during Pre-Development and will be documented in the Acquisition Strategy.

(2) The capability is operated and supported consistent with the sustainment plan approved by the MDA at the Production Milestone.

(3) The Program Manager or the user may propose urgently needed improvements to the capability. If within the scope of the initial requirements document, procedures in this enclosure may be used to acquire the improvements. If improvements are outside the scope of the validated or approved requirements document, a new or amended requirements document may be required.

(4) In collaboration with the original requesting DoD Component, a post-deployment assessment will be conducted after deployment. If practical, this assessment will be conducted in the field by the supporting operational test organization. If not practical, the Program Manager may use alternate means for this assessment to include Program Manager or operational test agency assessment of user feedback or other DoD Component feedback. Post-deployment assessment approaches for all programs under DOT&E Oversight will be independently reviewed and approved by DOT&E.

(5) Disposition Analysis. No later than 1 year after the program enters O&S (or earlier if directed by the DoD Component), the DoD Component will appoint an official to conduct a Disposition Analysis. Based on the analysis, the DoD Component head and the CAE will prepare a determination document for disposition of the system. The disposition analysis will consider the performance of the fielded system, long term operational needs, and the relationship of the capability to the Component's current and planned inventory of equipment. The analysis will also consider the continuation of non-materiel initiatives, the extension of science and technology developments related to the fielded capability, and the completion of MDA-approved and funded materiel improvements. The disposition official will recommend one of the following options:

(a) Termination: Demilitarization or Disposal. The system will be demilitarized and disposed of in accordance with all legal and regulatory requirements and policy related to safety (including explosive safety) and the environment. The recommendation will be coordinated with the DoD Component or, for JUONs and JEONs, the Combatant Commands.

(b) Sustainment for Current Contingency. Operation and sustainment of the system will continue for the current contingency. Multiple sustainment decisions may be made should the system require operations and support longer than 2 years; however, such sustainment decisions will be made and re-documented at least every 2 years. The sustained system will continue to receive the same priority of action as the original acquisition program. This recommendation will be coordinated with the DoD Component validation authority.

(c) Transition to Program of Record. If the system provides a needed, enduring capability, it may be transitioned to a program of record. The disposition official will recommend to the CAE the acquisition point of entry into the defense acquisition system, and whether the MDA should retain program authority or whether it should transition elsewhere. The requirements validation authority will specify the capability requirements documents required to support transition to a new or existing program of record. The disposition recommendation will be made to the DoD Component head for UONs, critical warfighter issues identified by the Warfighter SIG, or Secretary of Defense RAA determinations.

(6) The DoD Component head and the CAE will review the disposition official's recommendation and record the Component head's transition decision in a Disposition Determination. The Determination will specify the requirements documents required by the validation authority to support the transition. Programs of record will follow the procedures for such programs described in this instruction.

5. ADDITIONAL INFORMATION REQUIREMENTS. Table 11 provides the Information Requirements that replace or are in addition to the statutory or regulatory requirements in Tables 2 and 6 in Enclosure 1 that are applicable to ACAT II and ACAT III programs. For urgent capability acquisitions, the documentation procedures described in paragraph 4a(3)(d) will be applied to all information requirements unless otherwise prescribed in statute.

Table 11. Information Requirements Unique to the Urgent Capability Acquisition Process

INFORMATION REQUIREMENT	URGENT CAPABILITY ACQUISITION DECISION EVENTS		SOURCE
	Development	Production	
STATUTORY REQUIREMENTS			
ASSESSMENT APPROACH	•	•	10 U.S.C. 2366 (Ref. (h)) 10 U.S.C. 2399 (Ref. (h))
STATUTORY; only required for programs responding to urgently needed capabilities. - For programs under DOT&E oversight, combined operational and live fire test plans will be submitted to DOT&E for approval at the Development Milestone; post-deployment assessment plans will be submitted to DOT&E for approval at the Production and Deployment Milestone. DOT&E will ensure that testing is rigorous enough to rapidly evaluate critical operational issues. - Programs not under DOT&E oversight are approved at the Service level; the program may require a rapid and focused operational assessment and live fire testing (if applicable) prior to deploying an urgent need solution. The Acquisition Approach will identify any requirements to evaluate health, safety, or operational effectiveness, suitability, and survivability.			
COURSE OF ACTION ANALYSIS	•		Meets the assessment requirements of Subtitle III, Title 40, United States Code (Ref. (p)) (see Table 10 in Enclosure 1).
STATUTORY, replaces and serves as the AoA. Approved by the MDA. For JUONs, JEONs, critical warfighter issues identified by the Warfighter SIG, and Secretary of Defense RAA determinations, a copy is due to the Director, JRAC, within 3 business days of MDA approval.			
RAPID ACQUISITION AUTHORITY (RAA) RECOMMENDATION	•		SEC. 806, P.L. 107-314 (Ref. (cd))
STATUTORY. Optional request to the Secretary of Defense or Deputy Secretary of Defense for RAA. Considered as part of the development of the Acquisition Strategy. MDA approves the decision to request RAA at the Development Milestone.			
REGULATORY REQUIREMENT			
Disposition Authority's Report to the DoD Component Head			Para. 4e(5) of this enclosure
Regulatory. Based on the disposition official's recommendation in the Disposition Analysis, the Component Head will determine and document the disposition of the initiative and process it in accordance with applicable Component and requirements authority procedures. Due within 1 year of entering the Operations and Support Phase (or earlier, if directed).			

Table Notes:
1. A dot (•) in a cell indicates the specific applicability of the requirement to the life-cycle event
2. Documentation required for the identified events will be submitted no later than 45 calendar days before the planned review.
3. While these requirements are specific to programs responding to urgent needs, they are additive to the requirements identified in Tables 2 and 6 in Enclosure 1.

ENCLOSURE 13

CYBERSECURITY IN THE DEFENSE ACQUISITION SYSTEM

1. INTRODUCTION

a. Cyber Impact on Defense Acquisition

(1) Cybersecurity is a requirement for all DoD programs and must be fully considered and implemented in all aspects of acquisition programs across the life cycle. DoD program offices, systems, and networks, and supporting contractor facilities, and activities, are at risk of cyberattacks by state and non-state threat actors. Malicious activity by threat actors includes remote unauthorized activity against DoD to:

(a) Exfiltrate operational and classified data to compromise or disrupt critical DoD missions.

(b) Exfiltrate intellectual property, designs, or technical documentation to weaken DoD technological and military advantage.

(c) Insert compromised hardware or software to disrupt or degrade system performance.

(d) Subvert or compromise DoD networks, systems, support infrastructure, and employees through malicious actions.

(2) Responsibility for cybersecurity extends beyond network operators, software developers, and chief information officers, to every member of the acquisition workforce. Attention must be paid to cybersecurity at all acquisition category levels and all classification levels, including unclassified, throughout the entire life cycle; this includes systems that reside on networks and stand-alone systems that are not persistently connected to networks during tactical and strategic operations.

b. Program Manager Responsibilities. Program managers, assisted by supporting organizations to the acquisition community, are responsible for the cybersecurity of their programs, systems, and information. This responsibility starts from the earliest exploratory phases of a program, with supporting technology maturation, through all phases of the acquisition. Acquisition activities include system concept trades, design, development, test and evaluation (T&E), production, fielding, sustainment, and disposal. Program managers will pay particular attention to the following areas where a cybersecurity breach or failure would jeopardize military technological advantage or functionality:

(1) Program Information. This includes, but is not limited to:

(a) Information about the acquisition program, personnel, and the system being acquired, such as planning data, requirements data, design data, test data, operational software data, and support data (e.g., training, maintenance data) for the system.

(b) Information that alone might not be damaging and might be unclassified, but that in combination with other information could allow an adversary to compromise, counter, clone, or defeat warfighting capability or to simply gain a cost and schedule advantage.

(2) Organizations and Personnel. This includes government program offices, manufacturing, testing, depot, and training organizations, as well as the prime contractors and subcontractors supporting those organizations.

(3) Enabling Networks. This includes government and government support activity unclassified and classified networks, contractor unclassified and classified networks, and interfaces among government and contractor networks.

(4) Systems, Enabling Systems, and Supporting Systems. This includes systems in acquisition, enabling systems that facilitate life cycle activities (e.g., manufacturing, testing, training, logistics, maintenance), and supporting systems that contribute directly to operational functions (e.g., interconnecting operational systems).

2. CYBERSECURITY RISKS. Cyber vulnerabilities provide potential exploitation points for adversaries to steal, alter, or destroy system functionality, information, or technology they seek. Program managers will pay particular attention to the program and system elements that are vulnerable and can be exposed to targeting. At a minimum, the program manager's technical risk and opportunity management will consider:

a. Government Program Organization. Poor cybersecurity practices, untrained personnel, undetected malicious insiders, insufficient or incorrect classification of information and dissemination handling control, and inadequate information network security can be used by threat actors to gain program and system knowledge.

b. Contractor Organizations and Environments. Contractor facilities, including design, development, and production environments, networks, supply chains, and personnel, can be used by threat actors as cyber pathways to access government program organizations or fielded systems to steal, alter, or destroy system functionality, information, or technology.

c. Software and Hardware. Software, including firmware, and microelectronics used in the system or incorporated into spares can be deliberately compromised while in the supply chain with the intent to use these compromises for cyber-attacks to trigger future system failures. Undiscovered weaknesses or flaws in system elements containing software or microelectronics, including spares, can provide the foundation for threat actors to defeat fielded systems through cyber-attacks.

d. System Interfaces. Poorly configured, inadequately maintained, undocumented, or unprotected network and system interfaces can be used by threat actors to gain unauthorized system access or deliver cyber-attacks in the form of malicious software or content.

e. Enabling and Support Equipment, Systems, and Facilities. Test, certification, maintenance, design, development, manufacturing, or training systems, equipment, and facilities can be used by threat actors to gain access to system functionality, information or technology for cyber-attacks.

f. Fielded Systems. Degradation of the cybersecurity configuration or poor cyber hygiene conditions can expose system functionality to unauthorized access that threat actors can potentially exploit to gain access to system functionality. Battlefield loss can expose critical program information (CPI) to cyber threats.

3. ACTIVITIES TO MITIGATE CYBERSECURITY RISKS. Program Managers will rely on existing cybersecurity standards tailored to reflect analysis of specific program risks and opportunities to determine the level of cyber protections needed for their program information, the system, enabling and support systems, and information types that reside in or transit the fielded system. Appropriate cyber threat protection measures include information safeguarding, designed in system protections, supply chain risk management (SCRM), software assurance, hardware assurance, anti-counterfeit practices, anti-tamper (AT), and program security related activities such as information security, operations security (OPSEC), personnel security, physical security, and industrial security.

a. Safeguard Program Information Against Cyber-Attack. Program Managers will:

(1) Safeguard digitized information, starting with the application of appropriate classification and marking guidance for all program data, with a key focus on classified information and unclassified covered defense information (CDI), which includes unclassified controlled technical information. Programs that contain classified information can contain unclassified CDI, and the compilation of CDI can become classified. PMs will assess the impact of the exposure of the unclassified program information that will be placed on unclassified networks, including information that is contained in solicitations, technical publications, and associated research and technology efforts.

(2) Promote a strong culture of cybersecurity awareness and behavior in program offices and among contractors. This includes practicing need to know, good network security, and OPSEC, as described in DoDD 5205.02E (Reference (cn)), whenever and wherever digital information and communications are concerned.

(3) Ensure Federal Acquisition Regulation (FAR) Clause 52.204-2 (Reference (ak)) is included in solicitations and contracts that may require access to classified information; conduct assessments of compromised classified information, and mitigate impacts as a result of the loss of information.

(4) Ensure FAR Clause 52.204-21 is included in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.

(5) Ensure Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 (Reference (al)) is included in all solicitations and contracts, including solicitations and contracts using Part 12 of the FAR procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of commercially available off-the-shelf items. Use other appropriate DFARS and FAR requirements for solicitations and contracts that include the clause; and if a cyber incident is reported, assess what unclassified CDI was compromised, and mitigate impacts as a result of the loss of CDI.

(6) Assess unclassified controlled technical information losses associated with cyber incidents reported under contracts that contain DFARS Clause 252.204–7012. Refer to the Guidance to Stakeholders for Implementing DFARS Clause 252.204-7012 for detailed guidance on these assessments. Use the Joint Acquisition Protection and Exploitation Cell (JAPEC) to assist in tracking and correlating threat intelligence reports to further inform courses of action.

(7) Encourage contractor and industry participation in public-private information sharing activities, such as those described in DoDIs 8500.01 (Reference (x)) and 5205.13 (Reference (co)), and codified in Part 236 of Title 32, Code of Federal Regulations (Reference (cp)) or those developed under Executive Order (E.O.) 13691 (Reference (cq)).

b. Design for Cyber Threat Environments. In order to design, develop, and acquire systems that can operate in applicable cyber threat environments, Program Managers will:

(1) Derive cybersecurity and other system requirements into system performance specifications and product support needs as follows:

(a) Use the draft or validated capability development document (CDD) or equivalent capability requirements document, the concept of operations, the operational mode summary/mission profiles, and the assessed threats to the military capability provided by the Defense Intelligence Agency (DIA) or DoD Component intelligence and counterintelligence activities to inform requirements derivation activities.

(b) Ensure KPPs and attributes establish system survivability and sustainment measures, and may establish information system security measures, such as cryptography and key distribution, based on confidentiality, integrity, and availability needs.

(c) Use requirements derivation methods, such as system modeling and analysis, security use and abuse or misuse cases, criticality analysis, and vulnerability analysis to determine cybersecurity requirements that are sufficient to minimize vulnerabilities introduced by design, implementation, system interfaces, and access points.

(2) Allocate cybersecurity and related system security requirements to the system architecture and design, and assess for vulnerabilities.

(a) The system architecture and design will address, at a minimum, how the system:

1. Manages access to and use of the system and system resources.

2. Is structured to protect and preserve system functions or resources, e.g., through segmentation, separation, isolation, or partitioning.

3. Maintains priority system functions under adverse conditions.

4. Is configured to minimize exposure of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides, and patch management in the development environment (including integration and T&E), in production and throughout sustainment.

5. Monitors, detects, and responds to security anomalies.

6. Interfaces with DoD Information Network (DoDIN) or other external security services.

(b) Identify the digitized T&E data that will contribute to assessing progress toward achieving cybersecurity requirements. The T&E strategy should include not only the explicit cybersecurity requirements, but also all key interfaces. This is the key first step of the T&E planning process to support design and development. To support the architecture and design considerations in paragraph 3b(2)(a) of this enclosure, determine the avenues and means by which the system and supporting infrastructure may be exploited for cyber-attack and use this information to design T&E activities and scenarios.

(c) Apply DoDIs 8500.01 (Reference (x)) and 8510.01 (Reference (bg)) in accordance with DoD Component implementation and governance procedures. Program Managers will use program protection planning, system security engineering, developmental test and evaluation (DT&E), sustainment activities, and cybersecurity capabilities or services external to the system (e.g., common controls) to meet risk management framework for DoD IT objectives. Program Managers will collaborate with designated authorizing officials from program inception and throughout the life cycle, to ensure system and organizational cybersecurity operations are in alignment, and to avoid costly changes late in a program's development.

(3) Ensure cybersecurity and related system security requirements, design characteristics, and verification methods to demonstrate the achievement of those requirements are included in the technical baseline and maintain bi-directional traceability among requirements throughout the system life cycle.

(4) Include cybersecurity and related system security in the conduct of technical risk management activities and change management processes to address risk identification, analysis, mitigation planning, mitigation implementation, and tracking. Use evolving program and system

threats to inform operational impacts. The goal is to mitigate risks that could have an impact on meeting performance objectives as well as thresholds. Program risks, and opportunities as applicable, will be assessed at technical reviews and will include specific cybersecurity cost and schedule implications.

(5) Use evolving program and system threat assessments to continuously assess cybersecurity risks to the program and system.

(6) Identify and protect CPI, capabilities that contribute to the warfighters' technical advantage, throughout the life cycle in accordance with DoDI 5200.39 (Reference (ai)). Program Managers will:

(a) Identify and implement AT and exportability features as appropriate to protect CPI in U.S. systems when outside of U.S. control in accordance with DoDI 5200.39.

(b) Coordinate with the applicable DoD Component office of primary responsibility for AT, for programs with CPI. Submit an AT concept before Milestone A and AT plans before Milestones B and C; the DoD Executive Agent for Anti-Tamper must concur with the concept and plans, and the MDA must approve the concept and plans as an element of the Program Protection Plan (PPP) in accordance with Enclosure 3 of this instruction and DoDI 5200.39.

(7) Use trusted suppliers or appropriate SCRM countermeasures for system elements that perform mission-critical functions. Cyber protection measures for mission-critical functions and critical components must, at a minimum, include software assurance, hardware assurance, procurement strategies, and anti-counterfeit practices in accordance with DoDI 5200.44 (Reference (aj)).

(8) Use validated cybersecurity solutions, products, and services when available and cost effective.

(9) Establish, implement, and sustain security configuration parameters (e.g., Defense Security Technical Implementation Guides or Security Requirements Guides) for the system.

(10) Implement a cyber system vulnerability discovery and remediation process that spans research, development, production, and sustainment and integrates activities by both the government and contractors.

(11) Request assistance, when appropriate, from the Joint Federated Assurance Center, established in accordance with Section 937 of Public Law 113-66 (Reference (j)) to support software and hardware assurance requirements.

(12) Incorporate automated software vulnerability analysis tools throughout the life cycle to evaluate software vulnerabilities, as required by Section 933 of Public Law 112-239 (Reference (l)). When appropriate, use software vulnerability analysis enterprise licenses provided by the Joint Federated Assurance Center.

(13) Plan for and resource cybersecurity T&E in order to identify and eliminate as many cybersecurity shortfalls as early in the program as possible. Refer to the "Department of Defense Cybersecurity Test and Evaluation Guidebook" (Reference (cr)) and the Director of Operational Test and Evaluation (DOT&E) "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," (Reference (cs)) for detailed guidance on cybersecurity T&E planning. Beginning early, before Milestone A, work closely with the Chief Developmental Tester as well as the T&E WIPT to plan, as described in paragraph 3b(2), this enclosure, and conduct cybersecurity T&E, as described in paragraphs 3b(13)(a) and 3b(13)(b), this enclosure, to provide feedback to design and engineering teams. This will help avoid costly and difficult system modifications late in the acquisition life cycle. Cybersecurity T&E spans the entire material life cycle of the program, and each phase builds off the completion of the prior phase. T&E activities should be planned for and documented in the Test and Evaluation Master Plan (TEMP), including the T&E Strategy, evaluation frameworks (DT&E and operational T&E), and resource requirements. Cybersecurity T&E will include:

(a) Developmental Testing

1. Cooperative Vulnerability Identification. Conduct T&E activities to collect data needed to identify vulnerabilities and plan the means to mitigate or resolve them, including system scans, analysis, and architectural reviews.

2. Adversarial Cybersecurity DT&E. Conduct a cybersecurity DT&E event using realistic threat exploitation techniques in representative operating environments and scenarios to exercise critical missions within a cyber-contested environment to identify any vulnerabilities.

(b) Operational Testing. Two phases of cybersecurity testing are required as part of operational testing for all systems under the oversight of the Director of Operational Test and Evaluation. Program Managers should coordinate with the appropriate operational test agency to prepare their systems for these assessments by conducting comprehensive cybersecurity testing during system development.

1. Cooperative Vulnerability and Penetration Assessment. This phase consists of an overt examination of the system to identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities. This assessment is conducted in cooperation with the system's Program Manager. It is a comprehensive characterization of the cybersecurity status of a system in a fully operational context, and may be used to substitute for reconnaissance activities in support of adversarial testing when necessary. The assessment should consider the operational implications of vulnerabilities as they affect the capability to protect system data, detect unauthorized activity, react to system compromise, and restore system capabilities. This testing may be integrated with DT&E activities if conducted in a realistic operational environment, and if the DOT&E approves the testing in advance.

2. Adversarial Assessment. This phase assesses the ability of a unit equipped with a system to support its mission while withstanding cyber threat activity representative of an actual adversary. In addition to assessing the effect on mission execution, the test must evaluate

the ability to protect the system and data, detect threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity. This test phase should be conducted by an operational test agency employing a National Security Agency-certified adversarial team to act as a cyber aggressor presenting multiple cyber intrusion vectors consistent with the expected threat. The assessment should characterize the system's vulnerability as a function of an adversary's cyber experience level, relevant threat vectors, and other pertinent factors.

(14) Ensure that cybersecurity and system security requirements are incorporated in contracts.

c. Manage Cybersecurity Impacts to Information Types and System Interfaces to the DoDIN. Information types include specific categories of information resident in or transiting fielded systems (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management), defined by an organization or, in some instances, by a public law, E.O., directive, policy, or regulation. Program Managers will:

(1) Use applicable DoD and Component issuances, and specific program situations to tailor cybersecurity activities and guide collaboration throughout the system life cycle between the Program Manager team and the entities responsible for ensuring an acceptable cybersecurity posture during operations.

(2) Incorporate Federal Information Processing Standards, or National Security Agency/Central Security Service (NSA/CSS)-certified cryptographic products and technologies into systems in order to protect information types at rest and in transit. Programs with certain cryptographic requirements, as determined by the information type or other protection considerations, must coordinate development efforts with NSA/CSS Information Assurance Directorate.

d. Protect the System Against Cyber Attacks From Enabling and Supporting Systems. Program Managers will:

(1) Identify all system interfaces to all enabling and supporting systems and assess cybersecurity vulnerabilities. Program Managers will review vulnerabilities introduced by enabling and supporting systems and support activities, including engineering, simulation, and test tools and environments, third party certification and assessment activities, logistics, maintenance and training support activities, and all interoperable or ancillary equipment which the system operates or interfaces.

(2) Use threat intelligence from DIA, DoD Component intelligence and counterintelligence activities, the Defense Security Service, and the JAPEC to assess the trustworthiness of third party service providers and environments, (e.g., training, testing, logistics, or certification).

e. Protect Fielded Systems. Cybersecurity and related system security measures implemented throughout the system development effort do not ensure security is maintained

throughout operations. Once systems are fielded, they become exposed to a changing cyber threat environment and potentially more vulnerabilities. Planning for maintaining the cybersecurity of the system must be considered early and throughout the life cycle. Program Managers will:

(1) Plan for and implement effective software configuration updates and software management, to include software patch management during sustainment to mitigate newly discovered vulnerabilities. For high impact mission critical functions as established in accordance with DoDI 5200.44 (Reference (aj)), consider having a user representative as part of the software configuration management risk acceptance process.

(2) Plan, define, and document roles and responsibilities in the appropriate logistics documentation, (e.g., software support plan, operational technical manuals, planned maintenance support), for monitoring, maintaining, and reassessing cybersecurity and related program security risks as it relates to in-service usage, problem reports, configuration management, patch management, plan for Diminishing Manufacturing Sources and Materiel Shortages, and SCRM, to include counterfeits of critical components. This must include plans for coordinating cyber threat intelligence support throughout operations to ensure cybersecurity and related program security risk management accounts for changes to threats.

(3) Conduct periodic reassessments of cyber vulnerabilities to the system and support systems. These reassessments must be conducted, at a minimum, for any engineering modifications or technology refreshes. Technical and process mitigations will be incorporated into engineering and logistics documentation, and related solicitations and contracts.

(4) Ensure program and system information are protected and cyber vulnerabilities introduced by depot and other sustainment activities are minimized.

(5) Ensure identified CPI is protected from cyber-attack through disposal.

f. Independent Acquisition, Engineering, and Technical Assessments. For acquisition category I programs, DoD Component heads will conduct independent assessments of system designs and interfaces for cyber vulnerabilities. The results must inform technical baselines, and T&E plans and procedures.

4. PROTECTION PLANNING

a. Systems Engineering Plan (SEP). Program Managers will ensure the SEP, developed in accordance with Enclosure 3 of this instruction, describes the program's overall technical approach to cybersecurity and related program security, including technical risk, processes, resources, organization, metrics, and design considerations.

b. PPP. In accordance with Enclosure 3 of this instruction, Program Managers will prepare a PPP as a management tool to guide the program and systems security engineering, to include

cybersecurity, activities across the life cycle. The PPP will be submitted for MDA approval at each milestone review, beginning with Milestone A.

(1) Program Managers should ensure the PPP is included in requests for proposals (RFPs) and prepare updates to the PPP after any contract award to reflect the contractor's approved technical approach, and after identification of any significant threat activity or compromise.

(2) After the full rate production or full deployment decision, the PPP will transition to the Program Manager responsible for system sustainment and disposal.

c. TEMP. Ensure planned cybersecurity T&E as described in the TEMP, developed in accordance with Enclosures 4 and 5 of this instruction, includes activities that produce data to support engineering, risk management and acquisition decisions. Include within the T&E strategy those elements and interfaces of the system that, based on criticality and vulnerability analysis, need specific attention in T&E events. Vulnerability testing and evaluation must be planned for and described within the TEMP, and included as appropriate in RFPs and government DT&E.

d. Risk Management Framework for DoD IT Security Plan and Cybersecurity Strategy. As tailored to specific program situations, Program Managers will prepare plans and strategies in accordance with DoDI 8510.01 (Reference (bg)) and applicable DoD Component issuances.

5. PROGRAM MANAGEMENT AND COMPONENT ACTIONS TO IMPLEMENT CYBERSECURITY AND RELATED PROGRAM SECURITY ACROSS THE MATERIEL LIFE CYCLE

a. Before Materiel Development Decisions. Research, development, test, and evaluation (RDT&E) organizations and Program Managers will:

(1) Request cyber threat information from DIA or DoD Component intelligence and counterintelligence activities and use threat assessments to inform cyber protection planning.

(2) Protect digitized information from adversary targeting during basic and applied research, advanced technology development (including technology demonstrations and prototyping), and capabilities-based assessments.

(3) Identify CPI from science and technology (S&T) programs and initiate life-cycle cyber protection measures.

(4) Support the requirements community in the formulation of cybersecurity performance and affordability parameters and the identification of security-relevant critical intelligence parameters, and ensure key technical requirements are measurable and testable.

(5) Initiate all aspects of cyber related program protection planning, e.g., counterintelligence, information security classification, and OPSEC.

b. Materiel Solutions Analysis (MSA) Phase. During the MSA phase, RDT&E organizations and Program Managers will:

(1) Request information on cyber threats targeting program information and the system from DIA or DoD Component intelligence/counterintelligence activities and use updated threat assessments to inform the Analysis of Alternatives (AoA), early systems engineering analyses, selection of a preferred materiel solution and development of the draft CDD (or equivalent requirements document).

(2) Protect S&T, program, and system information from adversary cyber threat targeting during the MSA phase, including AoA, analyses and program such as formulation of the acquisition strategy and in requests for information or proposals.

(3) Manage technical risks and opportunities to include cybersecurity and related program security across the life cycle and informs all aspects of program security and cybersecurity planning.

(4) Establish program and system cybersecurity and related program security metrics and implement an enduring monitoring and assessment capability.

(5) Identify CPI and initiate life-cycle protection measures.

(6) Evaluate materiel solution alternatives for cybersecurity requirements, including but not limited to interfaces, performance, and sustainability, to support the AoA.

(7) Support the formulation of cybersecurity performance and affordability parameters and the identification of security-relevant critical intelligence parameters for the draft CDD.

(8) Update and integrate all cybersecurity related aspects of the program protection planning, to include but not limited to information security, OPSEC and life-cycle support.

(9) Define system cybersecurity entrance and exit criteria for all technical reviews, and document in the SEP along with related system security metrics for the program and system.

(10) Develop a cybersecurity T&E methodology based on derived system requirements and draft system performance specifications. Compile and analyze the system security requirements, identifying the data needed to support engineering, risk management, and acquisition decisions. Ensure the key system elements and interfaces identified through criticality and vulnerability analysis are tested during T&E. Document T&E planning in the TEMP. Identify the cybersecurity T&E resources, (e.g., cyber ranges) for each T&E activity.

(11) For programs requiring a DoD IT Authorization to Operate, in accordance with DoDIs 8500.01 (Reference (x)) and 8510.01 (Reference (bg)) in accordance with applicable DoD

Component issuances, coordinate authorization planning in accordance with DoD Component implementation and governance procedures.

c. Technology Maturation and Risk Reduction (TMRR) Phase. During the TMRR phase, Program Managers will:

(1) Request cyber threat information from DIA or DoD Component intelligence and counterintelligence activities and make use of updated cyber threat assessments to inform systems engineering trade-off analyses to support requirements, investment, and acquisition decisions. The analysis results should be reassessed over the life cycle as system requirements, design, manufacturing, test, and logistics activities evolve and mature.

(2) Protect digitized program and system information, CPI, and other system elements from adversary targeting during TMRR activities including system definition, design and test, contracting, and competitive prototyping.

(3) Analyze system requirements and design to ensure the system as described in the functional and allocated baselines meets cybersecurity performance requirements for operations in applicable cyber threat environments.

(4) Establish cybersecurity-relevant technical performance parameters and update the technical review entrance and exit criteria in the SEP.

(5) Update and integrate all cyber related aspects of the program protection planning, to include but not limited to information security, OPSEC, and life-cycle support. For T&E, understand the cyber-attack surfaces and refine the T&E planning and activities for cybersecurity; include updates in the Milestone B TEMP. Identify the cybersecurity T&E resources, such as cyber ranges, for each T&E activity. Ensure that an adversarial cybersecurity DT&E event is planned in a mission context.

(6) Incorporate cyber protection of program and system information, CPI, system elements (e.g., hardware assurance and software assurance) and cybersecurity performance requirements in the development RFP.

(7) Employ need to know principles and criteria when structuring contracting activities to minimize release of digitized program and system information. Include system security evaluation factors and subfactors that are tied to significant RFP security requirements and objectives that will have an impact on the source selection decision and are expected to be discriminators, e.g., implementation of safeguarding information on the contractors unclassified owned and operated network.

d. Engineering and Manufacturing Development (EMD) Phase. During the EMD phase, Program Managers will:

(1) Request cyber threat information on threats targeting program information and the system from DIA or DoD Component intelligence and counterintelligence activities and use

updated threat assessments to inform development of the detailed design, T&E criteria, system-level security risk, and assessment of readiness to begin production and deployment.

(2) Protect digitized program, system, and test information, CPI, and system elements from adversary targeting during design, test, and manufacturing and production readiness.

(3) Update cybersecurity and system security entrance and exit criteria for all technical reviews and document in the SEP.

(4) Update and integrate all aspects of the program protection planning, to include but not limited to information security, OPSEC, and life-cycle support.

(5) Conduct cybersecurity vulnerability and penetration testing and evaluation at the component, subsystem, interface, and integration levels in order to verify system requirements are met, and use results to inform the engineering activities, including technical risk and opportunity management.

(6) Incorporate recommendations from security T&E of EMD test articles and ensure the system as described in the production baseline is configured to established cybersecurity parameters and satisfies performance requirements for operations in applicable cyber threat environments. Ensure an adversarial cybersecurity DT&E event is conducted to evaluate the system's cybersecurity performance within a mission context. Use realistic threat exploitation techniques in representative operating environments and scenarios.

e. Production and Deployment Phase. During the production and deployment phase, Program Managers will:

(1) Request cyber threat information on threats targeting program information and the system from DIA or DoD Component intelligence/counterintelligence activities and make use of updated threat assessments to inform production and deployment activities such as, manufacturing, training spares.

(2) Protect digitized program and system information, CPI, and the system from adversary targeting during initial production, operational T&E, and initial fielding.

(3) Ensure the final product baseline includes cybersecurity design and configuration.

(4) Ensure system documentation addresses how to operate the system securely and how to manage and preserve the system security configuration.

(5) Ensure the system is deployed in a secure configuration.

(6) Update all aspects of program protection planning for the program and the system as cyber threats and the system evolve.

(7) Test the system for cybersecurity vulnerabilities using realistic threat exploitation techniques in an operational environment and remediate as appropriate.

(a) Coordinate with the appropriate operational test agency to support the execution of a cybersecurity cooperative vulnerability and penetration assessment. This assessment must include the enumeration of all significant vulnerabilities and the identification of exploits which may be employed against those vulnerabilities.

(b) Coordinate with the appropriate operational test agency to support the execution of a cybersecurity adversarial assessment, following the cooperative vulnerability and penetration assessment, to examine and characterize the operational impact of the vulnerabilities and exploits previously identified.

f. Operations and Support Phase. During the operations and support phase, Program Managers will:

(1) Request cyber threat information on threats targeting program information and systems in operation from DIA or DoD Component intelligence and counterintelligence activities and make use of updated threat assessments to inform impact to operational systems, technology refresh and disposal plans.

(2) Protect digitized program and system information, CPI, and system from adversary targeting during fielding and sustainment activities such as maintenance, training and operational exercises.

(3) Protect support systems and system spares from impairing cyber threats mission critical system functions.

(4) Respond to vulnerability alerts and apply security patches promptly.

(5) Periodically assess cybersecurity and other program security risks during system upgrades (e.g., technology refresh, modifications, engineering changes or future increments).

(6) Update all aspects of program protection planning for the program and the system as cyber threats and systems evolve.

(7) Before system disposal, remove all CPI and system data.

6. RESOURCES FOR EXECUTING CYBERSECURITY AND RELATED PROGRAM SECURITY ACTIVITIES. Table 12 lists and describes various resources and publications available for the Program Manager to use in executing cybersecurity and related program security procedures detailed in this enclosure.

Table 12. Cybersecurity and Related Program Security Resources and Publications

Category	Title of Resource and Description
Information Protection	FAR Clause 52.204-2 (Reference (ak)) This clause applies to the extent that the contract involves access to information classified Confidential, Secret, or Top Secret. The clause is related to compliance with the National Industrial Security Operating Manual and any revisions to that manual for which notice has been furnished to a contractor.
Protection of Information on Networks	FAR Clause 52.204-21 (Reference (ak)) This clause applies to information not intended for public release that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Websites) or simple transactional information, such as necessary to process payments.
	DFARS Clause 252.204-7012 (Reference (al)) The clause requires a company to safeguard CDI, as defined in the Clause, and to report to the DoD the possible exfiltration, manipulation, or other loss or compromise of unclassified CDI; or other activities that allow unauthorized access to the contractor's unclassified information system on which unclassified CDI is resident or transiting. The company must submit the malware to DoD if the company is able to isolate it and send it safely. For more information on implementing this clause, also see "Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012," (Reference (ct)) released by the Office of the Deputy Assistant Secretary of Defense for Systems Engineering.
	DoD Instruction 5205.13 (Reference (co)) - Establishes an approach for protecting unclassified DoD information transiting or residing on unclassified defense industrial base information systems and networks. - Increases DoD and defense industrial base situational awareness. - Establishes a DoD and defense industrial base collaborative information sharing environment. - DoD CIO manages the Defense Industrial Base Cyber Security/ Information Assurance Program. - Codified in Part 236 of Title 32, Code of Federal Regulations (Reference (cp)).
	E.O. 13691 (Reference (cq)) Encourages and promotes sharing of cybersecurity threat information within the private sector and between the private sector and government.
OPSEC	DoD Directive 5205.02E (Reference (cn)) Establishes process for identifying critical information and analyzing friendly actions attendant to military operations and other activities to: - Identify those actions that can be observed by adversary intelligence systems. - Determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk. - Select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.
Protection of IT and Information Systems	DoD Instruction 8500.01 (Reference (x)) Establishes a DoD cybersecurity program to protect and defend DoD information and information technology.
	DoD Instruction 8510.01 (Reference (bg)) Establishes the DoD decision process for managing cybersecurity risk to DoD information technology.

Table 12. Cybersecurity and Related Program Security Resources and Publications, Continued

Category	Title of Resource and Description
System Protection	DoDI 5200.39 (Reference (ai)) Provides policy and procedures for protecting CPI. CPI includes U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermine U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.
	DoDI 5200.44 (Reference (aj)) Establishes policy and procedures for managing supply chain risk. A supply chain is at risk when an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.
	Section 933 of the National Defense Authorization Act for Fiscal Year 2013, Public Law 112-239 (Reference (l)) Requires use of appropriate automated vulnerability analysis tools in computer software code during the entire life cycle, including during development, operational testing, operations and sustainment phases, and retirement.
	Section 937 of Public Law 113-66 (Reference (bj)) Requires the DoD to establish a joint federation of capabilities to support trusted defense system needs to ensure the security of software and hardware developed, maintained, and used by the DoD.
	DoD Instruction 8530.01 (Reference (cu)) Establishes policy and assigns responsibilities to protect the DoDIN against unauthorized activity, vulnerabilities, or threats.
	Joint Federated Assurance Center, chartered under Section 937 of Public law 113-66 (Reference (bj)) Federation of subject matter experts and capabilities to support program hardware and software assurance needs.
	National Cyber Range (NCR) The NCR is institutionally funded by AT&L Test Resource Management Center to provide cybersecurity T&E as a service to DoD Customers. The NCR provides secure facilities, computing resources, repeatable processes and skilled workforce as a service to Program Managers. The NCR Team helps the Program Manager plan and execute a wide range of event types including S&T experimentation, architectural evaluations, security control assessments, cooperative vulnerability, adversarial assessments, training and mission rehearsal. The NCR creates hi-fidelity, mission representative cyberspace environments and also facilitates the integration of cyberspace T&E infrastructure through partnerships with key stakeholders across DoD, the Department of Homeland Security, industry, and academia.

Table 12. Cybersecurity and Related Program Security Resources and Publications, Continued

Category	Title of Resource and Description
Threat Assessment and Integration	Defense Intelligence Agency Produces intelligence and counterintelligence assessments, to include assessment of supplier threats to acquisition programs providing critical weapons, information systems, or service capabilities, and system threat intelligence reports.
	Defense Security Service Provides cleared U.S. defense industry with information about foreign intelligence threats and ensures that cleared U.S. defense industry safeguards the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts.
	JAPEC Collaboration among the acquisition, intelligence, counterintelligence, law enforcement, and operations communities to prevent, mitigate, and respond to data loss.
Risk, Issue, and Opportunity Management	"Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs" (Reference (cv)) A guidance document that addresses the significant relationship between program success and effective risk management.
Cybersecurity T&E	DOT&E, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" (Reference (cs)) A guidance document that describes approaches for operational cybersecurity testing.
	"Department of Defense Cybersecurity Test and Evaluation Guidebook" (Reference (cr)) A guidance document that addresses planning, analysis, and implementation of cybersecurity T&E for chief developmental testers, lead DT&E organizations, operational test agencies, and the larger test community.

GLOSSARY

A complete Glossary of acquisition terms and common acquisition acronyms is maintained on the Defense Acquisition University website (Reference (ce)). The DAU Glossary (Reference (cf)) may be found at https://dap.dau.mil/glossary/Pages/Default.aspx.