

CHAPTER 8

SYSTEMS ACQUISITION AND PROGRAM SECURITY DOCUMENTS

A. INTRODUCTION

1. United States law and DoD Acquisition Management Process policies and procedures dictate the need for the documents discussed in this chapter. They are reviewed at the various milestone decision reviews that occur at critical program junctures in the acquisition process. See DoD Directive 5000.1, DoD Instruction 5000.2 and DoD's Defense Acquisition Guidebook (*references mm, nn, and ll*) for additional information on the structure of the acquisition process. The Technology Assessment/ Control Plan (TA/CP) and the Delegation of Disclosure Authority Letter (DDL) are also required in support of other programs (e.g., sales and coproduction) involving the release of classified information to foreign governments pursuant to DoD Directives 5230.11 (*reference dd*) and 5530.3 (*reference cc*).

2. The DoD policy on cooperative development in the acquisition process is based on law and necessity. In 1989, the Congress amended Title 10 (Armed Forces) of the U.S. Code by requiring the Department of Defense (DoD) conduct an analysis of cooperative opportunities at early decision points in the defense acquisition process for major defense acquisition programs (Public Law No. 101-189) (*reference hh*). The Department has implemented this by requiring a program proponent to consider potential foreign participation as part of the acquisition strategy approved at Milestone A and subsequent milestones for all major defense programs and to include similar analyses as an option in the development of the acquisition strategy for all other programs. The reduction in defense spending creates the necessity of considering cooperation in the development of defense systems.

3. Past practice and the economic picture suggest some involvement by allied nations may occur in all but the most sensitive acquisition programs, be it in the form of cooperative Research & Development (R&D), use of foreign contractors and subcontractors, Foreign Military Sales (FMS), direct commercial sales or follow-on support. Realistically, there are very few defense articles the United States will not sell or share with an ally sometime during the life-cycle of the article. Therefore, consideration and planning for some form of foreign participation must start at the earliest point in the acquisition process. A key aspect of this planning involves decisions on access to classified and critical unclassified technical data and protection of system capabilities and vulnerabilities, which are based on the underlying technology. DoD Directive 5000.1 specifically requires that acquisition managers shall identify classified and controlled unclassified research and technology information requiring protection early in the R&D, capability needs, and acquisition processes. Moreover, DoD Instruction 5000.2 states that all international cooperative programs shall fully comply with foreign disclosure and program

protection requirements, and that programs containing classified shall have a Delegation of Disclosure Authority Letter (DDL) or other written authorization issued by the DoD component's cognizant foreign disclosure office prior to entering into discussions with potential foreign partners.

B. CAPABILITY ANALYSIS AND ACQUISITION MANAGEMENT

1. Joint Capabilities Integration and Development System (JCIDS) Process. For major systems, the process normally begins with an analysis by the DoD Components of their capability to perform joint war-fighting missions, including interoperability, derived from top-down strategic guidance, such as national defense strategy, defense planning guidance, combatant command input, joint operations concepts and the intelligence threat. If capability gaps or needs are identified, the potential solution, or capability proposal, must consider the full range of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). A Functional Area Analysis (FAA) (identifies operational tasks, conditions and standards necessary to achieve military objectives), Functional Need Analysis (FNA) (assesses ability of current and projected capabilities to accomplish the tasks), and a Functional Solution Analysis (FSA) (assesses all DOTMLPF approaches and potential solutions are identified, and a capability need is identified) are prepared and they culminate in the preparation of an Initial Capabilities Document (ICD), which will be validated by the Joint Requirements Oversight Council (JROC), chaired by the Vice Chairman of the Joint Staff. The ICD describes a capability need requirement, in operational (not system) terms, that cannot be solved by a non-materiel solution (e.g., change to doctrine, organization, training, etc). For Major Defense Acquisition Programs (MDAPs), the JROC sends the ICD (prepared by the user) to the Defense Acquisition Executive (DAE) (the DAE is the Milestone Decision Authority (MDA) for Acquisition Category (ACAT) 1D programs) for a Concept Decision (CD) and, if the CD is approved, the designation of a lead Component. A plan for the Analysis of Alternatives (AoA) also is forwarded. If the MDA approves, the concept in the ICD is refined, the AoA is conducted, and the Technology Development Strategy (TDS) is developed, for approval at Milestone A. The Capability Development Document (CDD) is prepared during Technology Development and contains performance parameters and requirements and addresses cost for a proposed materiel solution. The Capability Production Document (CPD), which guides production, is prepared after a Milestone C decision.

a. Initial Capabilities Document (ICD). The ICD normally will contain the following elements:

- (1) Joint Functional Area: includes functional areas, Joint Functional Concepts (JFCs) (i.e., how a joint force commander will integrate a set of related military tasks to attain capabilities for a range of military operations), range of military operations, and the timeframe under consideration.
- (2) Required Capability: includes the particular aspects of the JFCs that the ICD addresses and explains why the desired capabilities are essential to the joint force

- commander to achieve military objectives; references Capstone Requirement Documents (CRDs) (i.e., a requirements document that facilitates CDDs and CPDs for families of systems (FOS) and systems of systems (SOS)).
- (3) Concept of Operations Summary: describes the mission areas that the capability contributes to, the operational outcomes it provides, the affects it must produce to achieve the outcomes, how it compliments the integrated joint war-fighting force, and the enabling capabilities that are required to achieve the desired operational outcomes.
 - (4) Capability Gap: describes, in operational terms, the missions or functions that cannot be performed or are unacceptably limited; the attributes of the desired general capabilities are described in terms of desired effects (including measures of effectiveness, such as time, distance, effect, and obstacles).
 - (5) Threat/Operational Environment: describes, in general terms, the operational environment in which the capability must be exercised; summarizes the current and projected threat capabilities to be countered (referencing the validated Defense Intelligence Agency (DIA) or Service products used).
 - (6) Functional Solution Analysis Summary: summarizes the DOTMLPF analysis, and identifies and changes in U.S. or allied doctrine, operational concepts, tactics, organization, and training that were considered, and describes why such non-materiel changes are inadequate; lists any ideas for materiel approaches that were considered; summarizes the analysis of all materiel approaches (U.S. and allied, commercial or military) considered in addressing the capability gaps.
 - (7) Final Materiel Recommendations: describes the best materiel approaches based on an analysis of the relative cost, efficacy, performance, delivery timeframe, and risk.
- b. Analysis of Alternatives (AoA). There is a hierarchy of potential alternatives to be considered prior to a decision to commit to a new start acquisition program. These alternatives are:
- (1) Procurement or modification of commercially available products, services, and technologies, from domestic or international sources, or the development of dual-use technologies;
 - (2) The additional production/modification of previously-developed U.S. and/or Allied military systems or equipment;
 - (3) A cooperative development program with one or more Allied nations.
 - (4) Initiate a new, joint, DoD Component or Government Agency development program;
- or

(5) Initiate a new DoD Component-unique development program.

c. Technology Development Strategy (TDS). The TDS documents the following:

(1) The rationale for adopting an evolutionary strategy or a single-step-to-full-capability strategy. For an evolutionary strategy (either spiral or incremental) include a preliminary description of how the program will be divided into technology spirals and development increments, limitations on prototypes, how the units will be supported, and performance goals and exit criteria.

(2) A program strategy, including overall cost, schedule, and performance goals for the total research and development program.

(3) Specific cost, schedule, and performance goals, including exit criteria, for the first technology spiral demonstration.

(4) A test plan to ensure that the goals and exit criteria for the first technology spiral demonstration are met.

d. Capability Development Document (CDD). The CDD will normally contain the following information:

(1) Capability Discussion: provides an overview of the capability gap in terms of mission area, relevant range of military operations, and the timeframe under consideration; describes the capability that the program delivers and how the current increment contributes to the required capability.

(2) Analysis Summary: summarizes the analyses conducted (e.g., the AoA), including the alternatives, objective, criteria assumptions, recommendations and conclusions.

(3) Concept of Operations Summary: describes the mission areas related to the capability, the operational outcomes, the affects it must produce to achieve the outcomes, how it compliments the integrated joint war-fighting force and the enabling technologies that are required.

(4) Threat Summary: includes the projected threat environment and the specific threat capabilities to be countered, including the nature of the threat, threat tactics, and projected threat capabilities.

(5) Program Summary: summarizes the overall program strategy for reaching full capability and the relationship between the increment addressed by the current CDD and any other increments of the program, including the status of any previous increments.

(6) System Capabilities Required for the Current Increment: includes a description of each attribute or characteristic, with supporting rationale for the capability; each attribute must be in measurable terms.

- (7) Family of System and System of System Synchronization: describes how related solutions, specified in other CDDs and CPDs remain compatible and that the development is synchronized; solutions should be tied to a common ICD.
- (8) National Security System and Information Technology System (NSS and ITS) Supportability: for systems that receive or transmit information, provides an estimate of the expected bandwidth and quality of service requirements for support of the capability.
- (9) Intelligence Supportability: for programs that produce, consume, process, or handle intelligence data, provides requirements for intelligence support as a basis for certification.
- (10) Electromagnetic Environmental Effects and Spectrum Supportability: describes the electromagnetic environment in which the system must operate and coexist with other U.S., allied, coalition, government, and non-government systems.
- (11) Assets Required to Achieve Initial Operational Capability (IOC): describes the types and initial quantities of assets required to attain IOC.
- (12) Schedule and IOC/Full Operational Capability (FOC) Definitions: describes actions which, when complete, will constitute attainment of IOC and FOC of the current increment, as well as target date.
- (13) Other Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) Considerations: discusses any additional DOTMLPF consideration associated with fielding the system that have not already been addressed.
- (14) Other System Attributes: addresses any other attributes that tend to be design, cost, and risk drivers, including environmental quality, human systems integration, embedded instrumentation, electronic attack, information protection standards/information assurance, and wartime reserve mode requirements.
- (15) Program Affordability: describes costs as life-cycle costs, including all associated DOTMLPF costs.

2. The four security-related support documents that are the subject of this chapter all deal with access to program information and its protection. The preparation of all four documents must be the result of a team effort involving program management, technical, intelligence, security, and foreign disclosure staffs. Much of the information required for the security support documents is derived from the JCIDS documents generated pursuant to CJCSI 3170.01C and CJCSM 3170.01M. (*references mmm and nnn*).

C. COOPERATIVE OPPORTUNITIES DOCUMENT (COD)

1. DoD Instruction 5000.2 (*reference nn*) requires a discussion of opportunities to conduct cooperative R&D or production for Major Defense Acquisition Programs (MDAPs) with allies as a part of the development of the acquisition strategy, to include the considerations for foreign military sales, component codevelopment and incorporation of subsystems from allied sources. The acquisition strategy for non-major programs may include a similar analysis for consideration by DoD Component program review authorities. The COD is one way to present the results of this discussion. This discussion may also be found in the program's Acquisition Strategy.

2. A principal issue is that of evaluating and comparing the positive and negative impacts of the technology sharing that happens in any cooperative program. This information for this analysis will be based in part on information developed for the ICD, AoA, and the CDD. This same information will be used for other acquisition management related documents. Among such impacts are those involving program timing, development, life cycle costs and rationalization, standardization, interoperability (RSI). A standard format for the COD, which is found in the Public Law (*reference hh*), may be used which addresses the specific areas required by the current legislation.

a. Sections one and two of the format provide the background and description of the program under consideration. They must be compatible with the description in the ICD and CDD.

b. Section three requires answers to four questions.

(1) The first two questions get to the heart of the matter. They ask whether there are any similar projects in development or production by one or more major allies of the United States and whether that project could satisfy, or be modified in scope, so as to satisfy the U.S. military requirements. In addition to briefly describing similar projects (assuming there are some) and their similarities and differences, the answer to the second question is critical. The sense of the Congress indicates, and the legislation implies, that U.S. military requirements should also be considered for modification if, by doing so, it will result in fielding a better weapon with greater efficiency. The opposite side to this is that if the necessary modifications are too extensive and costly or the relaxation of the U.S. military requirement results in an ineffective system, cooperation is not a good choice in this instance.

(2) The third question requires a description of any options. The advantages and disadvantages of trying to structure a cooperative development program should be listed, covering at least:

(a) Program Timing,

(b) Development and Life Cycle Costs,

(c) Technology Sharing (cover the flow in both directions, what technology is involved, is it state of the art, will an exception to the National Disclosure Policy (NDP) be required, effect of compromise of U.S. Classified Military Information (CMI) or Controlled Unclassified Information (CUI), etc.), and

(d) Rationalization, Standardization and Interoperability (RSI).

(3) The fourth question requires the consideration of alternative forms of cooperation such as FMS, coproduction, licensed production, component/sub-component codevelopment or incorporation of subsystems from allied sources and follow-on support. If a substantial possibility for cooperation exists, list the advantages and disadvantages in the same four items 3.b.(2)(a) through (4) above, as a minimum.

c. All of the factors raised in the COD should be considered and a conclusion drawn. Keep the focus on the cooperative issues and not the technical issues that will need to be resolved regardless of the outcome of the analysis.

D. PROGRAM PROTECTION PLAN (PPP)

1. DoD Instruction 5000.2 (*reference nn*) requires that sensitive information and technologies (i.e., Critical Program Information or CPI) be identified early in the acquisition process and be protected from inadvertent or unauthorized disclosure. The Program Protection Plan (PPP) required by DoD Directive 5200.39 (*reference oo*) serves this purpose, which is to protect defense items and technical data and the program from hostile collection efforts and unauthorized disclosure during the acquisition process.

2. The PPP addresses the protection of CPI throughout the acquisition cycle of the item. CPI are those elements of information that if compromised would degrade the combat effectiveness of the system, shorten its combat life, significantly alter program direction, or permit another to kill, counter or clone the U.S. system. If the program does not contain CPI, a PPP is not required. The PPP must consider system vulnerabilities, specific threats, and which countermeasures to employ to protect the item. The plan should counter only recognized vulnerabilities using selected countermeasures from the various security disciplines. The program manager can design a cost effective plan using a judicious combination of the security disciplines, counterintelligence assets and operations security (OPSEC) specialists. The governing directive contains the elements of information to be covered, but does not specify a particular format for the PPP. If a program does not contain classified or unclassified CPI, a PPP is not necessary.

3. The scope of the PPP is driven by which CPI needs protection, the threat and vulnerabilities, and system security engineering necessary for life-cycle protection. This serves as the basis for information security-related decisions in drafting the Security Classification Guide (SCG). DoD 5200-1R (*reference j*) requires a SCG for all classified systems, programs, plans, or projects. The SCG should identify sensitive (controlled) unclassified information and time-phase the

security guidance over the life of the item. The previously prepared documents, i.e., the ICD, CDD, AoA, and COD should be consulted in preparing the PPP.

4. The PPP can include the system security management plan as an annex. This annex concentrates on the protection of the system in its operational environment. The system security management plan draws upon a portion of system security engineering as described in MIL-STD-1785 (*reference ooo*). System security addresses the use of engineering measures to protect the system physically or to limit actions that compromise its war-fighting or support capabilities. The plan must include an evaluation of the use of anti-tamper capabilities, particularly if the program will involve cooperative development; there is the possibility of foreign sales or loss in combat.
5. The PPP for an international program will include a TA/CP and DDL.

E. TECHNOLOGY ASSESSMENT/CONTROL PLAN (TA/CP)

1. The Deputy Secretary of Defense, in June 1990, directed that the TA/CP requirement be implemented to accelerate the planning process for decisions on the foreign release of sensitive information involved in cooperative programs and sales of military equipment. He directed that the foreign disclosure and security planning should start at the beginning of the weapon system acquisition process. DoD Directive 5530.3 (*reference cc*) requires a TA/CP as part of the package requesting authority to negotiate (RAN) an international coproduction agreement. DoD Directive 5230.11 (*reference dd*) also requires a TA/CP be developed early in the all programs involving technology disclosures. DoD Instruction 5000.2 (*reference nn*) requires that all international cooperative programs will fully comply with foreign disclosure and program protection requirements – this in effect means the preparation of a TA/CP. As a practical matter, all programs will eventually have some foreign involvement. Program managers will likely be involved in North Atlantic Treaty Organization (NATO) and other bilateral data exchanges. Foreign sales or coproduction of the resulting systems, more often than not, will occur. The TA/CP prepared for acquisition programs identifies the technical data that warrants special protection in an international program and specifies the controls that are necessary. It also, can support the Request for Authority to Develop (RAD) for international program agreements, as well as subsequent decisions during the life of the program. The information used in the ICD, AoA, CDD, COD, and PPP will be used in preparing the TA/CP. Program managers, together with the team that developed it, should therefore review and update the TA/CP before each acquisition milestone, at each phase of cooperative programs, and when there are significant system improvements. A TA/CP also should be prepared for programs that are already in development to support sales and follow-on support decisions. When a TA/CP is prepared to support an international program, the U.S. prime contractor may provide assistance in technical aspects of the TA/CP. The TA/CP consists of the following four parts.

- a. **Program Concept.** This section requires a concise description of the program concept. It must describe in as few words as possible the purpose of the program and the threat or military or technical requirement that created the need for the program. When applied to

R&D cooperative programs not related to specific systems, it should define the technical objectives and limits of the cooperative effort and the need for this effort. This section must be consistent with other supporting program documentation. In short, this section describes briefly "what" is to be done and "why." The program manager and technical staff are primarily responsible for this section.

b. Nature and Scope of the Effort or Objectives. This section also should be concise and to the point. It describes "how" the technical and/or military operational objectives will be satisfied; "how" the program will be organized or phased, and "how" the effort will benefit the U.S. It also describes "who" is responsible, including program management. The program manager and technical staff also have primary responsibility for its preparation. It can be brief when prepared initially to support a coproduction program since the participants and program parameters are not known in advance. When the TA/CP is prepared to support a cooperative R&D program, this section will necessitate a more detailed discussion on courses of action and phasing. For a TA/CP prepared in support of a new-start acquisition program, this section also will involve a detailed discussion of the courses of action and phasing. This information will be used later to determine the extent and timing of possible foreign involvement. Foreign involvement is not a consideration for a new-start program at this point in the TA/CP. However, as a result of the analysis discussed in paragraph c. below, Technology Assessment, conclusions drawn can lead to potential foreign involvement. Factors to be covered in this section are:

- (1) Type of program (e.g., cooperative R&D, coproduction, system acquisition).
- (2) Describe the country(ies) participating, extent of participation, foreign commercial participants if known, and extent of commitment.
- (3) Program phases, in terms of development, production, and testing.
- (4) Summary of projected benefits to the U.S. and to other participants, if applicable, in terms of technology, production base, and military capability.
- (5) Points of contact, including program management and security/foreign disclosure officials that are involved in the preparation of the TA/CP.
- (6) Major milestones or dates when the assessment will require review or revision.

c. Technology Assessment. This is the most important part of the TA/CP. Its preparation will require a joint effort involving experts from program management, technical staff, security, intelligence and foreign disclosure.

- (1) This assessment requires the preparer to identify U.S. technologies involved, place a value on the U.S. technical contributions to the program, fully assess the benefits to accrue to the United States and perform a risk versus gain analysis. The preparer must also assess the value of any foreign government contributions. In all cases this analysis must result in clearly defined operational or technological benefits to the United States.

These benefits must clearly outweigh any damage that might occur, if there should be a compromise or unauthorized transfer. The benefits must be described fully in layman's terms.

(2) The analysis must identify any critical military capability, information, or technology that requires protection. It may reveal that an adjustment to program phasing is necessary to preclude the release of critical information before it is absolutely needed. The analysis should identify the need for any special security requirements. It must evaluate the risk of compromise based on the capability of the recipients or purchaser to protect the information. It must discuss any known foreign availability of the information, system and technology involved, and previous releases to the participants and to other countries.

(3) Whether preparing a TA/CP in support of a cooperative or coproduction program or a PPP for a new-start program, emphasis should be placed on the value of the technology and system in terms of military capability and technology, susceptibility to compromise, foreign availability, and likely damage in the event of compromise. It should draw conclusions regarding the need for protective security measures; the advantages and disadvantages of foreign participation in the program, in whole or in part, foreign sales, and follow-on support. Concerning foreign sales and cooperative R&D, the assessment must consider phasing of releases of classified and unclassified information.

d. **Control Plan.** The Control Plan will identify measures to minimize the potential risks and damage to the U.S. through loss, diversion or compromise. Development of this section also requires a team effort. It describes "how" the security requirements to be set forth in the pertinent agreement will be satisfied for cooperative R&D and coproduction programs.

(1) The Control Plan, together with the Technology Assessment, will form the basis for the following: agreement negotiating guidance, identifying the technical and security aspects of the program, disclosure guidelines development, and security arrangements for subsequent foreign participation in the program. Ultimately, it will be used in the preparation of the Delegation of Disclosure Authority Letter (DDL).

(2) Consider the following points in developing the Control Plan.

(a) Phasing the release of information on a just-in-time basis over the course of the project.

(b) Plan for modified or FMS versions of particularly critical components, or the release of them as completed, tested items. This is particularly important as the United States moves to smarter weapons.

(c) Consider the possible development of special security procedures to handle and control access to program information (e.g., prepare a Program Security Instruction (PSI)).

(d) Plan for controls on access to information by foreign nationals at U.S. facilities and the release of information by U.S. persons at foreign facilities.

2. A sample TA/CP is at Appendix H.

F. DELEGATION OF DISCLOSURE AUTHORITY LETTER (DDL)

1. DoD Directive 5230.11 (*reference dd*) provides the format for a DDL. DoD Directive 5530.3 (*reference bb*) requires a DDL as part of the package requesting authority to conclude an international coproduction agreement. DoD Instruction 5000.2 (*reference nn*) specifies that a DDL or other similar written guidance shall be prepared for all international acquisition programs that involve classified information. The DDL uses, as its basis, the guidelines and restrictions in the Control Plan of the relevant TA/CP, if one has been prepared. The DDL also is required by DoD Directive 5230.20 (*reference ff*) for certain visits and assignments of foreign nationals.

a. The DDL should be prepared in collaboration with the Program Manager (PM) and is issued by a Principal or Designated Disclosure Authority. It explains classification levels, categories, scope, and limitations on information that may be disclosed to a foreign recipient. This document will be used by foreign disclosure and licensing personnel to carry out their functions.

b. It provides disclosure guidance to disclosure officials in subordinate commands and agencies and, when applicable, to DoD contractors. Delegated disclosure authorities are responsible for reporting in the Foreign Disclosure System (FDS) all disclosures of CMI made under their delegation.

c. The Milestone Decision Authority in coordination with the Component Principal or Designated Disclosure Authority approves the DDL prepared to support the defense acquisition process.

d. The DDL must conform to the content of paragraphs 3. (Technology Assessment) and 4. (Control Plan) of the TA/CP. While all elements identified below should be provided in the general order shown, information should be presented in the clearest and easiest-to-use manner. For complex systems give consideration to breaking out items (5) and (6) by major subsystems to enhance the usefulness of the DDL.

(1) **CLASSIFICATION:** Identify the highest level of classification of the U.S. information involved in the program.

(2) **DISCLOSURE METHODS:** Identify the approved methods of disclosure, e.g., oral, visual or documentary.

(3) **CATEGORIES OF CMI PERMITTED:** Specify which of the eight categories of CMI may be disclosed or released.

(4) **SCOPE:** Specify who is authorized to release material or information, and to whom disclosure is authorized.

(5) **AUTHORIZED FOR RELEASE/DISCLOSURE:** Describe the material or information that can be released or disclosed. Specify any conditions or limitations to be imposed (e.g., time-phasing of release, allowable forms of software, identification of items releasable only as finished and tested items).

(6) **NOT AUTHORIZED FOR RELEASE/DISCLOSURE:** Describe material or information that cannot be released or disclosed.

(7) **PROCEDURES:** Specify review and transfer procedures, special security procedures or protective measures to be imposed. Include coordination requirements.

(8) **REDELEGATION:** Specify the extent of redelegation of authority, if any, permitted to subordinate activities.

G. PROGRAM SECURITY INSTRUCTION (PSI)

Many international agreements for cooperative programs contain a requirement for the preparation of a PSI by the PM. It is to be made binding on participating contractors through the contract. The PSI is used to rationalize the security requirements of the various participating governments and establish standard security procedures for the program. The PSI deals with the handling and protection of classified and controlled unclassified information furnished by the participants or generated in the international program. Preparation of the PSI must involve all participating governments and, to be effective, should be prepared and approved prior to the exchange of classified information. However, the PM is ultimately responsible for ensuring its preparation. A sample PSI is at Appendix N.