CHAPTER 8

SYSTEMS ACQUISITION AND PROGRAM SECURITY DOCUMENTS

A. INTRODUCTION

1. United States law and Department of Defense (DoD) Acquisition System policy and procedures dictate the need for the documents discussed in this chapter. These documents are to be reviewed at the milestone decision points occurring during the acquisition process. The Acquisition System establishes the process and provides the framework and documentary requirements for DoD to obtain materiel solutions to a documented and verified capability need (i.e., acquire new equipment). See DoD Directive 5000.01, DoD Instruction 5000.02 and the Defense Acquisition Guidebook *(references mm, nn, and lll)* for additional information on the structure of the Acquisition System process. Department of Defense capability requirements are identified during the Joint Capabilities Integration and Development System (JCIDS) process described in the current version of the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01 *(reference mmm)*. The analyses performed during the JCIDS process identify the capability need and result in documentation that also must be approved at the milestone decision points during the Acquisition System process.

2. The DoD policy on cooperative development with allies and other friendly nations in the acquisition process is based on law and necessity. In 1989, the United States (U.S.) Congress amended Title 10 (Armed Forces) of the U.S. Code, requiring the DoD conduct an analysis of cooperative opportunities early in the Acquisition System process for Major Defense Acquisition Programs (MDAPs) *(see* 10 U.S.C. 2350a *(reference a))*. 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 MDAPs and to include similar analyses as an option in the development of the acquisition strategy for all other acquisition programs.

3. Past practice, the need for the best technologies available, and economic considerations suggest some involvement by allied and other friendly nations may occur in all but the most sensitive acquisition programs. Cooperation may be in the form of cooperative research & development (R&D), the use of foreign contractors and subcontractors, Direct Commercial Sales (DCS), Foreign Military Sales (FMS), 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, planning for some form of foreign participation must start early in the acquisition process. A key aspect of this planning involves decisions on access to classified information and critical unclassified technical data and the protection of system capabilities and vulnerabilities, which are based on the underlying technology. The DoD

Directive 5000.01 specifically requires acquisition managers to identify classified and controlled unclassified research and technology information requiring protection early in the R&D, capability need, and acquisition processes. The DoD Instruction 5000.02 also requires the identification of Critical Program Information (CPI). Moreover, DoD Instruction 5000.02 states that all international cooperative programs shall fully comply with foreign disclosure and program protection requirements. Programs containing classified information 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.

4. This chapter uses the acquisition management system process described in DoD Instruction 5000.02 for MDAPs as the baseline for discussion, while also showing its relationship with the DoD Science and Technology (S&T) initiatives and the JCIDS process. The procedures for Major Automated Information Systems (MAISs) are similar, but are subject to other legal requirements and follow a different "chain of command". While this process is mandatory for MDAPs, DoD policy encourages its use for other DoD system acquisition programs. It should be noted that certain DoD Components which have acquisition authority (e.g., the Special Operations Command (SOCOM) and Missile Defense Agency) typically apply a more streamlined approach to systems acquisition. However, the basic legal and regulatory requirements must be satisfied and documented in some form. Moreover, while the CJCS 3170.01 series documents emphasize joint capabilities, joint capability documentations, and the role of the Combatant Commands and Functional Capability Boards (FCBs) in identifying joint capability needs, a simplified, baseline approach based on MDAPs is used in this chapter.

5. The key players in this process are the senior Acquisition Community officials who exercise Milestone Decision Authority (MDA) and management oversight; the Director, Defense Research and Engineering, the R&D site directors, and the DoD organizations engaged in non-traditional development activities (e.g., Advanced Concept Technology Demonstrations (ACTDs) and Advanced Technology Demonstrations (ATDs)); and the DoD Components with acquisition authority, the Combatant Commands, the Joint Requirements Oversight Council (JROC), and the Director for Program Analysis and Evaluation. The Defense Acquisition Executive (DAE) for DoD is the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)). This individual is also the MDA for Acquisition Category (ACAT) 1D programs (those MDAPs approved at the DAE level). Senior level advice is provided to the DAE by the Defense Acquisition Board (DAB). Other officials who may make acquisition decisions include the Component Acquisition Executive (CAE), the Program Executive Officer (PEO), and the Program Manager (PM). When a program manager has not been selected or, for example, work is performed in a DoD lab or in a non-traditional development effort, it is the responsible commander, program executive, or site director who is responsible for ensuring security and foreign disclosure implications are taken into consideration.

6. This chapter will initially summarize the Acquisition System and JCIDS processes and identify the documentation that is required at each milestone decision point in the Acquisition System process. It will then identify the security documents that are to be prepared to satisfy the above stated requirements in DoD Directive 5000.01 and DoD Instruction 5000.02, identify the sources of information for the security documents, and suggest who should participate in the

preparation of the documents. It will emphasize protection of information must be a consideration in pre-acquisition activities and S&T projects.. Finally, it will emphasize the relationship between the Acquisition/JCIDS documentation and the security documents. It makes the argument that it is extremely difficult to prepare the security documents if required information is not properly documented during the Acquisition System and JCIDS processes.

B. THE ACQUISITION SYSTEM PROCESS

1. The Defense Acquisition Management System provides an event-based process where the acquisition process proceeds through a series of phases and milestones. The MDA (the DAE, CAE, PEO, or PM, depending on the size of the program in terms of development and production costs) must approve transition to the next phase based on entrance and exit criteria for each milestone. The phases and milestones are:

a. The Materiel Solution Analysis Phase. This phase begins with a Materiel Development Decision (MDD) by the MDA approving a broad, initial concept (the Initial Capabilities Document (ICD)) for a materiel solution to an operational capability need, and an Analysis of Alternatives (AoA) plan. The concept for satisfying the need will be refined by the lead DoD Component during this phase and a Technology Development Strategy (TDS) will be developed, based in part on the initial AoA. When an evolutionary strategy (i.e., deliver a capability in increments as technology is available) is used, the ICD may cover only the initial increment. The phase ends when the MDA approves a preferred solution.

b. The Technology Development phase is used to reduce technology risk and to determine the appropriate set of technologies to be integrated into a full system. It involves continuous technology discovery and development with close collaboration between the S&T community, the user, and the system developer; multiple technology development demonstrations may be necessary. The ICD and AoA guide this effort. During this phase a list of known or probable CPIs is developed. The user will prepare the Capability Development Document (CDD) to support program initiation, refine the integrated architecture, and clarify how the program will lead to a joint war-fighting capability. The CDD contains the performance parameters necessary to design the proposed system. It will also contain a minimum set of Key Performance Parameters (KPP), (i.e., a set of minimum essential attributes or characteristics that must be met) for the system or increment. This phase ends when an affordable increment of militarily-useful capability is identified, the technology for that increment is demonstrated, and a system can be developed for production within a short time-frame, or the MDA decides to terminate the effort. The completion of this phase leads to a Milestone B (the Engineering and Manufacturing Development (EMD) phase) decision.

2. The EMD phase is normally the beginning of “systems acquisition”. The purpose is to develop a system or increment of capability; reduce integration and manufacturing risks; ensure operational supportability with particular attention to reducing the logistics footprint; implement human resources integration; design for producibility; ensure affordability and the protection of

CPI; and demonstrate system integration, interoperability, safety, and utility. Two major efforts are system integration (i.e., integrate subsystems, complete detailed design, and reduce system-level risk) and system demonstration (i.e., demonstrate the ability of the system to operate in a useful way consistent with the approved KPPs). The completion of this phase leads to a Milestone C (the Production and Deployment phase) decision.

3. The Production and Deployment Phase authorizes entry into low-rate initial production, into production or procurement (for systems that do not require low-rate production) or into limited deployment for MAIS or software-intensive acquisition programs with no production components. The Production and Deployment Phase, based on the Capabilities Production Document (CPD), completes work to achieve an operational capability that satisfies mission needs.

4. The Operations and Support phase includes all elements necessary to maintain the readiness and operational capability of deployed systems, and covers eventual disposal. It generally includes such items as supply, maintenance, transportation, data management, systems engineering, configuration management, and training, among others. Follow-on operational test and evaluation (FOT&E) may be conducted to confirm that deficiencies in operational effectiveness, suitability, survivability, or interoperability have been remedied, as appropriate. At the end of its useful life, the system is withdrawn from service for demilitarization and disposal. The PM is responsible to plan for future demilitarization and disposal.

C. THE JCIDS PROCESS

1. 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. This capability analysis is based on a review of top-down strategic guidance, such as the National Defense Strategy, the National Military Strategy, Defense Planning Guidance, Combatant Command Concepts of Operation, , 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 identifies a need or gap), and a Functional Solution Analysis (FSA) assesses all DOTMLPF approaches and potential solutions are identified.

2. These analyses culminate in the preparation of an ICD, which will be validated by the 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). CJCSI 3170.01 (current issuance) provides guidance on the JCIDS process. For MDAPs, the JROC sends the ICD to the DAE (the DAE is the MDA for ACAT 1D programs) for a MDD and, if the ICD is approved, the designation of a lead DoD Component. A plan for the AoA also is forwarded at this time. If the MDA approves

the concept and the AoA plan, the concept in the ICD is refined, the AoA is conducted, and the TDS is developed, for approval at Milestone A. The CDD is prepared during the Technology Development phase and contains performance parameters and requirements and addresses cost for a proposed materiel solution. The CPD, which guides production, is prepared after a Milestone C decision. The latter document is not discussed in this chapter, because all of the security documents should have been prepared before this document is approved at Milestone C in the Acquisition System process. The other documents described in this paragraph are summarized below.

a. The Initial Capabilities Document. The ICD normally contains 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 complements 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. The Analysis of Alternatives. There is a hierarchy of potential alternatives to be considered prior to a decision to commit to a new start acquisition program. These alternatives, in order of priority, 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, which is the least desirable solution.

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

(1) The rationale for adopting an evolutionary strategy (the preferred approach) or a single-step-to-full-capability strategy (e.g., for common supply items or (Commercial Off-The-Shelf (COTS) items). For an evolutionary acquisition, the TDS shall include a preliminary description of how the materiel solution will be divided into acquisition increments based on mature technology and an appropriate limitation on the number of prototype units or engineering development models that may be produced in support of a Technology Development Phase;

(2) A preliminary acquisition 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 Technology Development Phase;

(4) A description of the approach that will be used to ensure data assets will be made visible, acceptable, and understandable to any potential user as early as possible (DoD Directive 8320.02 (*reference dddd*));

(5) A list of known or probable CPI and potential countermeasures such as anti-tamper in the preferred system concept and in the critical technologies and competitive prototypes to inform program protection (DoD Instruction 5200.39 (*reference oo*) and design integration during the Technology Development Phase;

(6) A time-phased workload assessment identifying the manpower and functional competency requirements for successful program execution and the associated staffing plan, including the roles of government and non-government personnel;

(7) A data management strategy; and

(8) A summary of the Cost Analysis Improvement Group (CAIG)-approved Cost and Software Data Reporting (CSDR) Plan(s) for the Technology Development Phase.

d. The Capability Development Document. 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 complements 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 DOTMLPF Considerations: discuss any additional DOTMLPF and policy implications 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.

3. In addition to the above discussion of the Acquisition System phases and related documentation, other activities are going on outside the traditional acquisition process. These activities are taking place in DoD laboratories, civilian universities and colleges, and industry where technologies are being developed or put to new uses. As these technologies mature they may be inserted into a program without going through the traditional acquisition phases.

D. The DoD SCIENCE &TECHNOLOGY EFFORTS

User needs and technology opportunities can occur at any time, and may occur prior to and outside the normal systems acquisition process. A technology opportunity may result from pre-acquisition activities, such as a JCTD or an ATD program. A technology opportunity may be represented by work performed in DoD S&T initiatives, such as in the DoD laboratories, in civilian universities and colleges, and in the contractor community. Much of the S&T work performed in these environments is considered to be fundamental research, and not subject to control. However, once the technology is applied to a military capability need, consideration must be given to the security and foreign disclosure implications of it being made publicly available or shared in international programs. Therefore, foreign disclosure and security requirements frequently are necessary before the start of new system acquisition effort.

E. THE SECURITY SUPPORT DOCUMENTS

The 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 of the 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 3170.01 and CJCS Manual (CJCSM) 3170.01 (*reference nnn*). Some information necessary to prepare these documents also may be available from similar or earlier legacy systems. All of these documents must be ready for a milestone B decision, when approval is given for system acquisition. However, they must be available, if only in preliminary or draft form before disclosures of classified information can take place. This may be necessary early in the process as the acquisition community begins to enter into exploratory discussions to ascertain the possibility of foreign availability of technology and foreign involvement in the development and processes. They are dynamic documents and must be updated at milestone review.

1. The Cooperative Opportunities Document

   a. The DoD Instruction 5000.02 requires a discussion of opportunities to conduct cooperative R&D or production for MDAPs with allies as a part of the development of the acquisition strategy, to include the considerations for FMS, component co-development 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.

   b. 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 10 U.S.C. 2350a, may be used which addresses the specific areas required by the current legislation.

      (1) Section 1 of the format provides the background of the program under consideration. It must be compatible with the description in the ICD and CDD.

      (2) Section 2 is a description of the program under consideration. This section also must be compatible with the ICD and CDD.

      (3) Section 3 requires answers to three questions:

(a) The first question asks whether there are any similar projects in development or production by one or more major allies of the U.S. and whether that project could satisfy, or be modified in scope, so as to satisfy the U.S. military requirements.

(b) 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.

(c) 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:

- Program Timing,
- Development and Life Cycle Costs,
- 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
- Rationalization, Standardization and Interoperability.

(d) Section 4 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 three items as 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.

2. The Security Classification Guide (SCG)

The classification guide will identify the elements of information that are classified, the level of classification, and the downgrading and declassification instructions. It will be prepared in accordance with DoD Regulation 5200.1-R *(reference j).* The preparation of the SCG requires collaboration among the program technical staff and security professionals. The SCG is one of the most important tools in preparing the other security documents. These other documents require knowing the elements of classified information in the anticipated program and the levels of classification. Frequently, a previous SCG from a similar program can be used as a baseline. The Defense Technical Information Center (DTIC) maintains a record of SCGs. A

comprehensive SCG is critical to the preparation of subsequent security and export documentation.

3. The Program Protection Plan (PPP)

a. The DoD Directive 5000.01 requires the identification of classified and controlled unclassified research and technology information requiring additional counter intelligence and security support (i.e., CPI) early in the research and development, capability needs, and acquisition processes. The PPP required by DoD Instruction 5200.39 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.

b. 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.

c. The scope of the PPP is driven by CPI that 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 SCG. The DoD 5200.1R 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.

d. 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.

e. The PPP for an international program will include as attachments the SCG, a systems security engineering plan, anti-tamper plan, a Technology Assessment/Control Plan (TA/CP) and a DDL. The format for the PPP can be found in DoD Instruction 5200.39.

4. The Technology Assessment/Control Plan

a. 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. The DoD Directive 5530.3 (*reference dd*) requires a TA/CP as part of the package requesting authority to negotiate (RAN) an international coproduction agreement. It supports the Request for Authority to Develop (RAD) international program agreements, as well as subsequent decisions during the life of the program, and is to be submitted with a Request for Authority to Conclude (RAC) the agreement. The DoD Directive 5230.11 (*reference ee*) also requires a TA/CP be developed early in the all programs involving technology disclosures. The DoD Instruction 5000.02 requires all international cooperative programs to fully comply with foreign disclosure and program protection requirements – this in effect means the preparation of a TA/CP. As a practical matter, most programs will eventually have some foreign involvement, if it is only foreign sales. The DoD Instruction 5200.39 also requires the preparation of a TA/CP as part of the PPP preparation.

b. 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. This includes identification of CPI and the need for anti-tamper planning.. 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.

(1) 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 cooperative R&D 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.

(2) 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:

(a) Type of program (e.g., cooperative R&D, coproduction, system acquisition).

(b) Describe the country(ies) participating, extent of participation, foreign commercial participants if known, and extent of commitment.

(c) Program phases, in terms of development, production, and testing.

(d) Summary of projected benefits to the U.S. and to other participants, if applicable, in terms of technology, production base, and military capability.

(e) Points of contact, including program management and security/foreign disclosure officials that are involved in the preparation of the TA/CP.

(f) Major milestones or dates when the assessment will require review or revision.

(3) 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 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. The analysis must identify any critical military capability, information, or technology that requires protection. It must evaluate the risk of compromise based on the capability of the recipients or purchaser to protect the information. It may reveal that certain information should not be shared or 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 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. The analysis should address the following:

(a) Sensitive Technical Data or Technologies: Describe the hardware, software, technical data and technologies or processes (classified and unclassified) that will or

are expected to provide the desired system capabilities and identify those which, if known to potential adversaries, would give them the capability to neutralize, counter, or copy the U.S. system. If the TA/CP is to be used for a cooperative acquisition program, also describe any information that would give a potential adversary the capability to take action to disrupt or cause a change in the course of the program. Information that reveals program or system vulnerabilities and susceptibilities should be included. The Militarily Critical Technologies List (MCTL) may be used as a baseline for identifying the technical data and technologies, but should not be the sole basis for deciding what data and technologies need to be protected; i.e., the technical data or technology must be related to the program or project and loss or compromise would give an advantage to a potential adversary (e.g., neutralize or counter the system). If the required information is not fully known during the early stages of an initiative (e.g., cooperative research and development, when exploratory research is being pursued), describe the technology area based on the MCTL and the nature of capability to be achieved by the effort in terms of its contribution to military operational use. Program or project scientists and engineers, and any contractors already participating, should provide most of the input for this item.

(b) Susceptibility to Exploitation**:** Indicate the susceptibility to diversion, exploitation and reverse engineering of any U.S. hardware, software, or technology that is provided to the program, the capability and likelihood of the other participating countries and others to exploit the susceptibilities, and the capability of the participating countries and others to benefit from exploiting the susceptibilities. Program scientists and engineers should provide the information; supporting counterintelligence and intelligence personnel should be consulted for information on foreign availability and foreign collection efforts.

(c) Classification/NDP Category: The information required for this section is the list of information, technical data and technology to be provided to or generated in the program, which should have resulted from the analysis in subparagraph A., above, the eight NDP-1 categories, and the three classification levels (TOP SECRET, SECRET, or CONFIDENTIAL). The input on the classification of information will come from the classification guide for the program, if one exists. A classification guide for legacy systems or similar systems may be consulted if a classification guide for the initiative at issue is yet to be developed. Information on CUI will come from program scientists and engineers and any contractors that may be involved and, for acquisition programs, from the user organization that developed the capability need during the JCIDS analyses that led to the acquisition requirement. If any of the information could be CPI, it must be identified as such.

(d) Comparable Foreign Systems: For any U.S. system or hardware or software that is involved, provide an assessment of foreign systems that have essentially comparable capabilities, including information on the capabilities and susceptibilities and vulnerabilities of the foreign systems and the level of technology involved. If a system is not involved (e.g., as in the case of cooperative research and development), provide an assessment of the status of the participating countries' and other countries'

capabilities with respect to comparable technologies, R&D capabilities, and production processes in relation to that of the United States. Identify the source of the information that is provided. This information should be available from knowledge gained by participation in Data Exchange Agreements (DEAs), Information Exchange Programs (IEPs), The Technical Cooperation Program (TTCP), and NATO programs by DoD scientists and engineers, and from the intelligence community.

(e) Prior Disclosures: Identify any previous disclosures to foreign entities, via U.S. Government or commercial programs (sales, co-production, cooperative R&D, information exchange program, personnel exchange program, etc.), of comparable systems or technologies. This information should be available from the Foreign Disclosure System (FDS), the Foreign Visits System (FVS), and the Exception to National Disclosure Policy (ENDP) and the USXPORTS data bases in the Security Policy Automation Network (SPAN), from records maintained for projects under such cooperative R&D programs as the DEAs, IEPs, and TTCP, and from the FMS data base.

(f) Impact on U.S. and Foreign Military Capability:

(1) U.S. Military Capability: Identify the specific expected foreign contributions to the initiative. Describe advances in U.S. military capability or contributions to the U.S. technology base that will result from the foreign contributions to the initiative. The DoD sponsor of the initiative should provide this information.

(2) Foreign Military Capability: Identify the specific U.S. contributions to the initiative. Describe the advances to the military capabilities of the other countries or the advances to their technology base as the result of the U.S. contributions. The DoD sponsor of the initiative should provide this information.

(g) Risk of Compromise: Describe the specific damage to U.S. military capabilities and the U.S. technology base that would result from any loss or compromise of the U.S. hardware, software, technical data or technologies that are to be provided under the initiative, as well as the impact on the program or project, and the system to be developed and its capability. This assessment is to be made without reference to the intended foreign participant(s) or their security or export control programs. The purpose of this paragraph is to place a value on the U.S. contributions to the program or project as well as the product expected to result from the program or project, and postulate the impact on the United States should the program or project, the research effort, or the system to be developed be compromised. If it is stated that no damage will result from the initiative, the reason(s) for such response will be provided. The program manager, DoD Component operational personnel, and the organization that prepared the capability requirement documentation (for acquisition programs) or identified the need should provide this information.

(h) Conclusions: Drawing on the responses in subparagraphs (a) through (g), above, summarize the hardware, software, technical data, and/or technology to be provided

for the type initiative that is to be pursued (as described in Sections 1 and 2, above) and the impact of permitting foreign involvement in the program or project or access to the hardware, software, technical data, or technology provided to or generated in the program or project. If any of the information is CPI, it must be specifically identified including the reasons for characterizing the information as CPI. Address whether anti-tamper measures should be adopted for an acquisition program. The description must summarize both the advantages and disadvantages of the foreign involvement or access, taking into consideration the risks and damage described in subparagraphs (f) and (g), above. If the analysis in this section leads to the conclusion that anti-tamper measures should be adopted, explain the requirement. This summary must support the security and control measures described in the Control Plan in subparagraph (4), below. The bottom line is to identify technical data and other information which may be shared, that which must be withheld, that for which release authority must be obtained from other departments or agencies, or industry (proprietary information), whether phased releases should be adopted, whether anti-tamper measures are recommended, and whether an export variant should be considered.

(4) 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.

(a) 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 DDL.

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

- Identification of information that will not be shared under any circumstances.

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

- 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.

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

- How to handle foreign government information and proprietary information.

5. The Delegation of Disclosure Authority Letter

a. The DoD Directive 5230.11 provides the format for a DDL. The DoD Directive 5530.3 requires a DDL as part of the package requesting authority to conclude an international coproduction agreement. The DoD Directive 5000.02 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.

b. A DDL is required for a cooperative acquisition program as soon as classified information is identified during the Acquisition System/JCIDS processes. This may occur prior to the MDD approval. If an initial DDL is prepared during the early stages of those processes, it must be reviewed and updated at each milestone decision point.

(1) The DDL should be prepared in collaboration with the Program Manager (PM) and is issued by a Principal Disclosure Authority (PDA) or Designated Disclosure Authority (DDA). 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.

(2) It provides disclosure guidance to disclosure officials in subordinate commands and agencies and, when applicable, to DoD contractors. The DDAs are responsible for reporting in the FDS all disclosures of CMI made under their delegation. (Note: Chapter 3.E.8. has detailed information on the FDS.)

(3) The MDA, in coordination with the Component PDA or DDA, approves the DDL prepared to support the defense acquisition process.

(4) 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 (e) and (f) by major subsystems to enhance the usefulness of the DDL

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

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

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

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

(e) 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, and the identification of items releasable only as finished and tested items). The description must be specific with respect to oral, visual and documentary information that is authorized for disclosure or release. General descriptions are to be avoided.

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

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

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

6. The Program Security Instruction

a. Many international agreements for cooperative arms programs contain a requirement for the preparation of a PSI. 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, generated in the international program, and transferred among the participants. It also can be used to obligate participating foreign governments on any security requirements that are documented in the PPP.

b. The content of the PSI is based on an analysis of the program structure, the number of governments and contractors participating in the program, the complexity of the program, and the range of security procedures that are anticipated for use during the program. With regard to the latter point, questions to be addressed are, for example: Will there be a need to hand carry classified documents? Will secure communications be needed? Will there be frequent, recurring visits? Will commercial freight be used? Will there be a need to identify, mark, and handle various categories of information? The answers to such questions will identify the need for government approval of plans or procedures to accomplish the requirements. The plans and procedures are documented in the PSI.

c. The PSI is an extension of the program international agreement. As such, it must be approved by the National Security Authorities or Designated Security Authorities of the Participating governments (Note: The approving authority for the Department of Defense is the Deputy Under Secretary of Defense (Technology Security Policy and National Disclosure Policy). The PM, technical staff, and participating contractors must assist in identifying the requirements, since they will be managing the program and using the procedures. The PSI will represent a rationalization of the security procedures of all participating governments. Hence, the only efficient method of preparing it is to assemble a working group composed of

security professionals from the participating countries and task that group to prepare the document. The PM is ultimately responsible for ensuring its preparation for a Milestone B decision. However, it should be completed before there is any exchange of classified information under the program. A sample PSI is at Appendix N of this Handbook.