BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE PAMPHLET 63-113

17 OCTOBER 2013

Acquisition

PROGRAM PROTECTION PLANNING FOR LIFE CYCLE MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: SAF/AQXA

Certified by: SAF/AQX (Mr. Richard Lombardi)

Supersedes: AFPAM 63-1701, 27 Mar 2003

Pages: 74

This publication provides procedures to implement program protection planning requirements in Air Force Policy Directive (AFPD) 63-1/20-1, *Integrated Life Cycle Management;* AFPD 71-1, *Criminal Investigations and Counterintelligence;* Department of Defense Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*; and DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN).* Additionally, this Air Force Pamphlet (AFPAM) provides procedures to implement guidance in Air Force Instruction (AFI) 63-101/20-101, *Integrated Life Cycle Management*; AFI 63-114, *Quick Reaction Capability Process;* AFI 63-131, *Modification Management*; AFI 71-101v4, *Counterintelligence*; AFI 61-204, *Disseminating Scientific and Technical Information;* AFI 33-200, *Information Assurance (IA) Management;* AFI 14-111, *Intelligence Support to the Acquisition Life-Cycle,* AFI 14-201, *Intelligence Production and Applications;* and AFI 10-701, *Operations Security (OPSEC).* This publication applies to all military and civilian Air Force (AF) personnel including major commands (MAJCOMS), direct reporting units (DRU) and field operating agencies (FOA); other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force (DAF). This publication applies to Air Force Reserve Command (AFRC) Units and to the Air National Guard (ANG).

This AFPAM provides procedures for the protection of programs and technology projects developed or procured under Department of Defense Instruction (DoDI) 5000.02, *Operation of the Defense Acquisition System,* as well as the protection of legacy systems identified in AFPD 10-9, *Lead Command Designation and Responsibilities for Weapon Systems*. If there is any conflicting guidance between this publication and *Chairman of the Joint Chiefs of Staff Instruction* (CJCSI) 3170.01 or DoDI 5000.02, the latter takes precedence.

To ensure standardization, any organization supplementing this pamphlet must send the implementing publication to SAF/AQX for review and coordination before publishing. Refer recommended changes and questions about this publication to SAF/AQXA using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through appropriate chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) maintained in the Air Force Records Information Management System (AFRIMS).

SUMMARY OF CHANGES

This is a new document providing procedures to implement new guidance established by AFI 63-101/20-101 based upon guidance from DoD CIO, USD (AT&L) and USD (I). It also consolidates information previously contained in Air Force Pamphlet (AFPAM) 63-1701, *Program Protection Planning*, 27 March 2003.

Chapter 1

INTRODUCTION

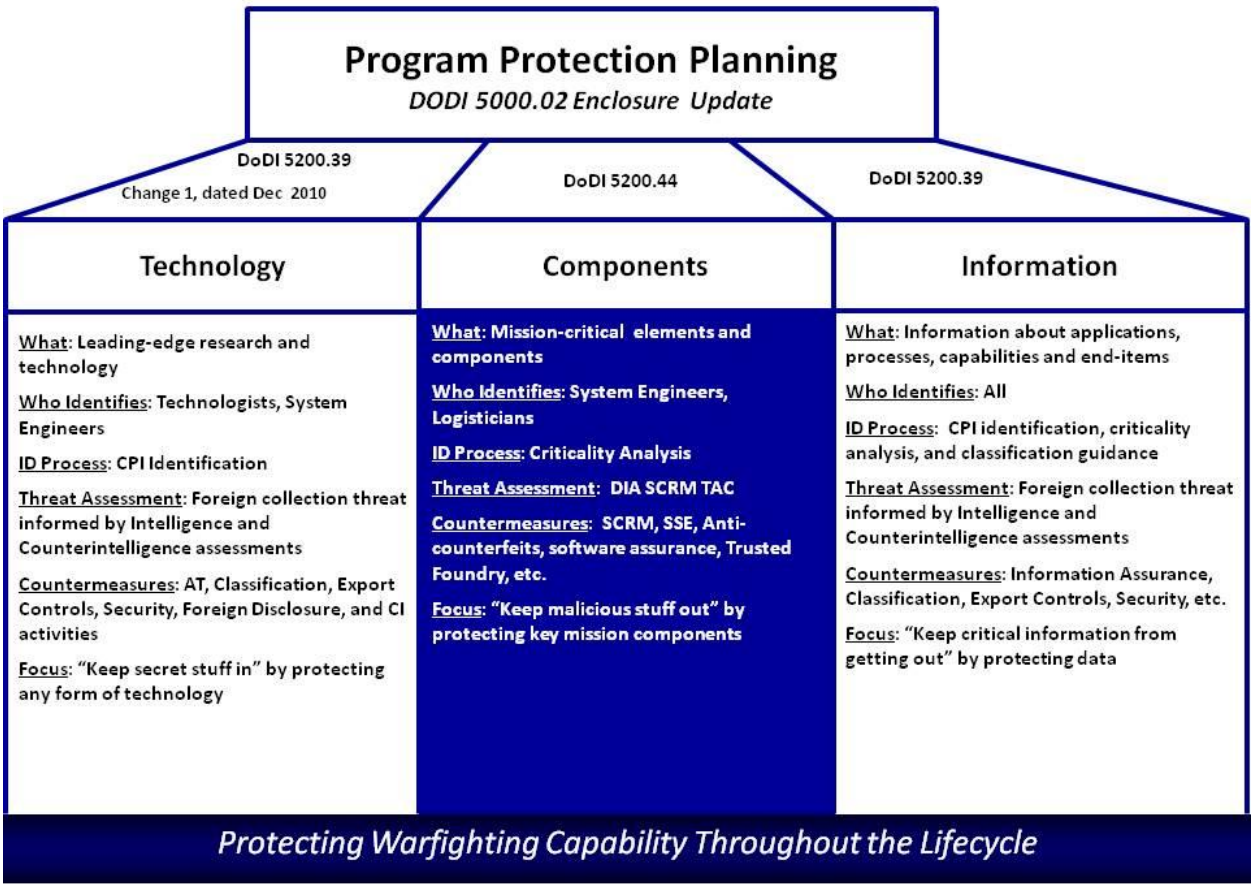
1.1. Overview. Program protection is a critical element of the Integrated Life Cycle Management (ILCM) of weapon systems and services. The Program Protection Plan (PPP) documents program decisions to ensure that technology, components, and information are adequately protected. For the latest PPP template reference Defense Acquisition Guidebook, Chapter 13. The protection planning process is intended to help program offices consciously think through what needs to be protected and to develop a plan that describes protection techniques as well as addresses the risk management for what cannot be adequately protected. Chapter 2 details the basic roles and responsibilities of key participants in implementing program protection. Chapter 3 of this pamphlet focuses on the process requirements that program managers should use for conducting sound program protection and covers all the functional parts of program protection. Chapter 4 shows the logical flow of procedures for program protection. Chapter 5 explains how program protection methods work throughout the life cycle of the acquisition framework. The PPP should be a current and useable reference (regardless of the life cycle phase) for understanding and managing the full spectrum of program and systems security activities. It is updated as the system develops, as the program's critical assets are identified, and as threats or vulnerabilities change (or are better understood).

1.2. Purpose. This pamphlet provides Program Managers (PM) with recommended protection planning activities for the integrated management of systems security risks. Risks to Air Force systems' advanced technology and mission-critical functionality can come from foreign intelligence services, design vulnerability, supply chain compromise, cyber or advanced persistent threats, or battlefield loss at any point in the system's life cycle. This pamphlet provides the procedures for the identification and protection of Critical Program Information (CPI) and critical components.

1.2.1. Technology and acquisition programs (including testing and sustainment activities) must be protected against hostile or criminal activities to keep technological advantages in and malicious or counterfeit content out.

1.2.2. In accordance with (IAW) DoDI 5200.39, DoDI O-5240.24, DoDI 3020.46, and DoDI 5200.44, program protection is focused on protecting CPI (leading edge research & technology and information about applications, processes, capabilities and end-items) and critical components. This is broken down as shown in Figure 1.1.

Figure 1.1. Comprehensive Program Protection Focus Areas.



1.3. Core Activities. PMs develop and apply comprehensive program protection in order to provide secure, uncompromised military systems to the warfighter. For the purposes of this pamphlet and the program protection process, the term program applies to technology, acquisition, sustainment activities and research and development projects; the term PM refers to the designated individual with responsibility for and authority to execute a program, including sustainment efforts. This pamphlet provides procedures to implement guidance for programs to preserve the effectiveness of military systems through appropriate protection and risk management strategies. Program protection activities consist of:

1.3.1. Designing in resilience and agility to maintain mission assurance if a system or sub-system is compromised. Redundancy, diversity, and distribution can enhance resilience; nimbleness and adaptability enhance agility.

1.3.2. Identifying critical components as well as inherited or organic CPI early in a technology or system life cycle and continuing to assess for CPI or critical components as part of the ILCM process IAW DoDI 5200.39. PMs are required to assess their programs for CPI and critical components any time there is a significant configuration change, or an actual or suspected compromise of the system or its industrial base.

1.3.3. Assessing and identifying threats and vulnerabilities to CPI and critical components.

1.3.4. Protecting and mitigating the compromise of CPI and critical components through the integrated and synchronized application of counterintelligence (CI), intelligence, security, systems engineering, information assurance, Anti-Tamper, and other defensive countermeasures to mitigate risks; then documenting program protection decisions in a PPP classified by content.

1.3.5. Conducting comparative analysis of similar program CPI, as well as cases of cyber attacks and CPI exfiltration, and aligning protection activities horizontally through the use of the DoD Acquisition Security Database (ASDB).

1.3.6. Minimizing and managing the risk that the program capability will be impaired due to malicious or criminal compromise of the supply chain. PMs are required to manage the risk that counterfeit or maliciously altered parts may enter and degrade a system or introduce unknown content. (see DoDI 5200.44)

1.3.7. Ensuring that contractual language requires contractors to participate in program protection.

1.4. Applicability. All programs are required to perform protection planning IAW DoDI 5000.02, *Operation of the Defense Acquisition System,* DoDI 5200.39, and AFI 63-101/20-101. This includes any modification IAW AFI 63-131, *Modification Program Management* for programs in the Operation and Sustainment (O&S) Phase. All new and legacy systems (regardless of whether they have CPI) must address mission critical functions and components requiring risk management to protect capabilities.

1.4.1. Acquisition Category (ACAT) programs. Per AFI 63-101/20-101, all ACATs require a PPP for Milestone Decision Authority (MDA) review and approval at every milestone (beginning at Milestone [MS] A). The PM updates the PPP at each subsequent milestone and the Full-Rate Production (FRP) decision. The PM should consider the impact of configuration changes and update the PPP as necessary. For legacy systems, PPP requirements for modifications can be satisfied by updating or annexing an existing PPP, creating a PPP for individual modification efforts, or creating a PPP for the entire weapon system addressing all modification protection measures with provisions for annexes to cover future modifications.

1.4.2. Technology Projects Planned for Transition. Technology projects requiring a formal Technology Transition Plan (TTP) should document CPI in a PPP. If an AT plan is required, it should be provided to the Transition Agent as a classified annex to the PPP. Research and technology projects that develop advanced or unique technology must develop a PPP.

1.4.3. Nuclear Systems. Nuclear components governed by DoDI 5030.55, *DOD procedures for Joint DOD-DOE Nuclear Weapon Life-Cycle Activities*, AFI 63-103, *Joint Air Force-National Nuclear Security Administration (AF-NNSA) Nuclear Weapons Life Cycle Management* and DoD-DoE and/or Air Force-National Nuclear Security Administration (AF-NNSA) agreements are exempt. All other components and information that are part of nuclear systems should use this pamphlet as a guide for program protection.

1.4.4. Special Access Programs (SAP). Special Access Programs (SAPs) are managed in accordance with DoDD 5205.07, DoDI 5205.11, AFPD 16-7, and AFI 16-701. SAP program managers are required to develop PPPs or an alternative document that combines program protection and other aspects of program security per DoDI 5205.11.

1.4.5. Defense Business Systems (DBS). PMs for DBS meeting any of the criteria in DoDI 5200.44 must identify critical components and document risk mitigations in a PPP.

1.4.6. Quick Reaction Capability (QRC) Programs. QRC programs are required to assess program protection requirements IAW AFI 63-114. The requirement for a full PPP is then assessed at the Capability Transition Review (CTR).

1.4.7. Foreign Military Sales (FMS) and Direct Commercial Sales (DCS). FMS and DCS programs should prepare a PPP and follow the guidance in this document.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Assistant Secretary of the Air Force for Acquisition (SAF/AQ). SAF/AQ has overall responsibility for acquiring systems for the Air Force and serves as the Service Acquisition Executive (SAE). SAF/AQ:

2.1.1. Serves as the AF focal point for all program protection matters pertaining to research, development, acquisition, and sustainment programs.

2.1.2. Establishes technical standards, procedures, and guidelines for implementing proper AT mechanisms for the protection of CPI. SAF/AQL reviews all Anti-Tamper (AT) plans.

2.2. The Administrative Assistant to the Secretary of the Air Force (SAF/AA). SAF/AA provides oversight and broad direction in conjunction with Headquarters Air Force (HAF) offices on plans, policies, and programs related to Air Force-wide information protection. SAF/AA establishes USAF security policy and manages the following security programs: personnel, industrial, and information. SAF/AA serves as the AF authority for the use and dissemination of classified information and Controlled Unclassified Information (CUI).

2.3. Deputy Under Secretary of the Air Force for International Affairs (SAF/IA). SAF/IA provides policy oversight and guidance to international programs supporting national security objectives through politico-military affairs, security assistance programs, technology and information disclosure, education and training, and cooperative research and development. Increasing reliance on foreign and global supply chains requires an international engagement strategy to ensure timely information and counter strategies. SAF/IAPD is the approval authority for delegated disclosure authority to the Foreign Disclosure Office (FDO) in support of both one-time and continuing disclosure requirements.

2.4. Secretary of the Air Force, Office of Information Dominance and Chief Information Officer (SAF/CIO A6). SAF/CIO A6 develops, documents, and implements the Air Force information assurance program to oversee the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in support of Air Force operations, missions, and business processes. SAF/CIO A6:

2.4.1. Serves as the approval authority for information assurance strategy documents.

2.4.2. Conducts cyber intrusion damage assessments to determine the overall impact of potential CPI and critical components compromises stemming from unauthorized cyber intrusions into unclassified Defense Industrial Base (DIB) information systems. These assessments should address impact on current and future Air Force weapons programs, scientific and research projects, and warfighting capabilities

2.4.3. Provides damage assessment reports to affected PMs and appropriate AF acquisition leadership IAW DoDI 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*.

2.4.4. Appoints a Senior Information Assurance Officer (SIAO) to carry out the AF CIO responsibilities IAW Federal and DoD mandates.

2.5. Air Force Office of Special Investigations (AFOSI). AFOSI provides overall CI support to technology and acquisition program activities IAW DoDI O-5240.24 and DoDI 5200.39. AFOSI:

2.5.1. Assigns a Trusted Systems and Networks (TSN) focal point IAW DoDI O-5240.24 and DoDI 5200.44 to coordinate with the Defense Intelligence Agency's (DIA) Supply Chain Risk Management (SCRM) Threat Analysis Center (TAC) and the MAJCOM (for AFMC and AFSPC) TSN focal points.

2.5.2. Assigns CI analysts to assist DIA in conducting threat analysis of suppliers of critical components IAW DoDI 5200.44, DoDI O-5240.24 and DoDI 5200.39.

2.5.3. Coordinates with DIA and the National Air and Space Intelligence Center (NASIC) on Technology Targeting Risk Assessments (TTRAs), Risk Assessment of Technology Transfers (RATTs), and supply chain threats.

2.5.4. Obtains and reviews Requests for Information (RFIs) sent to the DIA SCRM TAC by the AFMC or AFSPC TSN focal point.

2.5.5. Obtains and analyzes threat assessment reports from DIA's SCRM TAC.

2.5.6. Coordinates with the AFMC or AFSPC TSN focal point to provide DIA SCRM TAC reports and analysis to requesting PMs.

2.5.7. Notifies DIA of discovered or suspected supply chain exploitation for the purposes of further analysis and the development of enterprise remediation, as appropriate.

2.5.8. Works with PMs to develop the Counterintelligence Support Plan (CISP) responsive to risk, vulnerability, and threat assessments.

2.5.9. Provides PMs with Counterintelligence Threat Assessments (CITAs) in support of protection planning.

2.6. National Air and Space Intelligence Center (NASIC). NASIC, in cooperation with DIA and AFOSI, provides tailored intelligence products and analysis of threats in response to appropriate requests IAW DoDI O-5240.24, DoDI 5200.39, AFI 14-111, and AFI 14-201.

2.7. Air Force Materiel Command (AFMC) and Air Force Space Command (AFSPC). AFMC and AFSPC:

2.7.1. Assign AFMC and AFSPC TSN focal points IAW DoDI 5200.44, with access to all MAJCOM development and sustainment programs, in order to support required TSN activities such as prioritizing PM requests for intelligence to DIA's SCRM TAC.

2.7.2. Horizontally integrate program-level threat assessments, risk assessments, and mitigation strategies at the enterprise level.

2.7.3. Support execution of horizontal protection processes to include implementation and use of the ASDB.

2.7.4. Support research and development to provide tools for testing and verification of critical components.

2.8. Milestone Decision Authority (MDA). The MDA:

2.8.1. Validates that comprehensive program protection is addressed in appropriate program documents and contracts.

2.8.2. Validates CPI determinations, critical component determinations, and program protection approach when approving PPPs.

2.9. Program Executive Officer (PEO). The PEO:

2.9.1. Assigns an AT technical lead from PEO Engineering Staff to support program CPI (including Resident-CPI) validation and protection.

2.9.2. Horizontally integrates program-level threat assessments, risk assessments, and mitigation strategies at the portfolio level.

2.10. Program Manager (PM). The PM:

2.10.1. Determines program protection requirements for the program's inherited or organic CPI as well as the program's critical components.

2.10.2. Develops a PPP for all applicable programs. The PM is required to update the PPP at each subsequent milestone and the Full-Rate Production (FRP) decision per AFI 63-101/20-101. The PM updates the PPP based upon evolving system design, newly identified CPI and critical components, and recent threat data. The PM should also update the PPP after any compromise.

2.10.3. Develops cost estimates for all aspects of program protection, to include implementing protection requirements throughout the life cycle and incorporate into the budget submission.

2.10.4. Includes program protection requirements in applicable programmatic documentation and contract flow-down documentation. This includes placing the approved PPP on contract via DD Form 254 and delivering the PPP to the contractor.

2.10.5. Addresses CPI, critical component risks, and countermeasures during appropriate program reviews IAW DoDI 5000.02, DoD 5200.44, DoDI 5200.39, and AFI 63-101/20-101.

Chapter 3

PROGRAM PROTECTION REQUIREMENTS

3.1. Overview. The objective of program protection is to maintain military advantage. Program protection should also preserve information, property, and supply chain integrity to assure the intended capability for its life cycle. This chapter will focus on the key concepts and process requirements for conducting sound program protection. Each PM should determine the program's unique requirements and tailor a protection approach which both satisfies regulatory guidance and is, to the maximum extent possible, consistent with risk management and capability requirements.

3.1.1. Protection planning is a risk-based process for selecting cost-effective countermeasures to protect CPI and critical components. Protection is tailored to the program based on the manner in which the CPI and critical components manifest themselves (information, technology, or component). Program protection is discussed at technical and program reviews.

3.1.2. The PPP describes the program's mission-critical functions as well as its CPI and critical components providing, protecting, or having unrestricted access to mission-critical functions. The PPP documents the threats to, and vulnerabilities of its CPI and critical components; describes the program's risk management approach; details the selection, application, and estimated cost of countermeasures to mitigate associated risks; and describes all foreign involvement.

3.1.3. A PPP should reflect the current protection planning for each program's unique situation throughout the acquisition life cycle. Program protection requires close coordination among functional disciplines, user communities and contractors.

3.1.4. PPP development includes working with the Product Support Manager (PSM) and the logistics community to build in protection-related sustainment requirements.

3.1.5. A PPP template and detailed information on how program planning is accomplished beyond what is covered in this pamphlet is in the Defense Acquisition Guidebook (DAG) Chapter 13.

3.2. Tailoring. Tailoring provides the ability to integrate, consolidate, incorporate, and streamline strategies, oversight, reviews, decision levels, documentation, and information. MDAs should promote maximum flexibility in tailoring programs under their oversight to fit particular conditions of that program, consistent with applicable laws and regulations and the time sensitivity of the capability need. The MDA ensures PPPs are tailored to 1) provide the needed capability to the warfighter in the shortest practical time, 2) balance risk, 3) ensure affordability and supportability, and 4) provide adequate information for decision making. Reference AFPAM 63-128 for more information on tailoring.

3.2.1. The PM documents the tailoring strategy, including the supporting rationale and citation to the applicable statute or regulation in the Acquisition Strategy (AS) and/or Acquisition Decision Memorandum (ADM) for the MDA's approval.

3.2.2. MDAs and PMs should tailor within the scope of the applicable statute or regulation. MDAs have tailoring authority over programmatic execution requirements except where stated in statute or regulation.

3.2.3. Care should be taken to not waive requirements when the waiver authority resides outside MDA authority. Waiver authority, other than those explicitly defined, belongs to the publication or requirement owner. A waiver is an expressed or written statement to relinquish or provide exceptions to specific statutory or regulatory requirement.

3.3. Information Assurance (IA). The Information Assurance Strategy (IAS) is a required annex of the PPP that is submitted to meet the program's IA requirement for Clinger-Cohen Act compliance. If the program does not have IA requirements, the Annex should so state. Technology projects may document the IAS in accordance with local policy. See DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, DoDI 8500.2, *Information Assurance (IA) Implementation*, AFI 33-200, and AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)* for required IA processes.

3.3.1. Determine if the system has Platform IT (PIT), Platform IT Interconnections (PITI), or DoD Information Assurance Certification and Accreditation (DIACAP) requirements. See Attachment 9 for PIT Determination Checklist template. If the program is or contains PIT, ensure candidate PIT components are identified, systems security requirements are verified, and PIT determinations are documented in the Information Assurance Strategy (IAS) annex of the PPP IAW DoDI 8500.02, and AFI 33-210.

3.4. Software Assurance. Software Assurance must be addressed in the PPP. This encompasses not only development activities, but also the security of the processes used to handle software components during their sourcing, development and distribution. (See DoDI 5200.44) Specifically, the PPP should detail how software will be designed and tested to assure protection of critical functionality and CPI. PMs will monitor CPIs and Critical Intelligence Parameters as part of their Risk Management Plan (as defined in AFI 63-101/20-101).

3.5. Anti-Tamper (AT). AT measures are intended to prevent and/or delay exploitation of Resident CPI in U.S. weapon systems. SAF/AQLS serves as the USAF AT Lead. The office is responsible for reviewing AT Plans for horizontal protection and ensuring Resident CPI and provisos are protected from reverse-engineering. Provisos require AT protection only if required by the Tri-Service Committee or other National Disclosure Policy. Two main sources of reverse-engineering include Foreign Military Sales (including a company's Direct Commercial Sales), and battlefield losses. The USAF AT Lead approves Direct Commercial Sales AT Plans and coordinates on domestic and Foreign Military Sales (FMS) AT Plans. For further clarification on AT measures contact the USAF AT Lead.

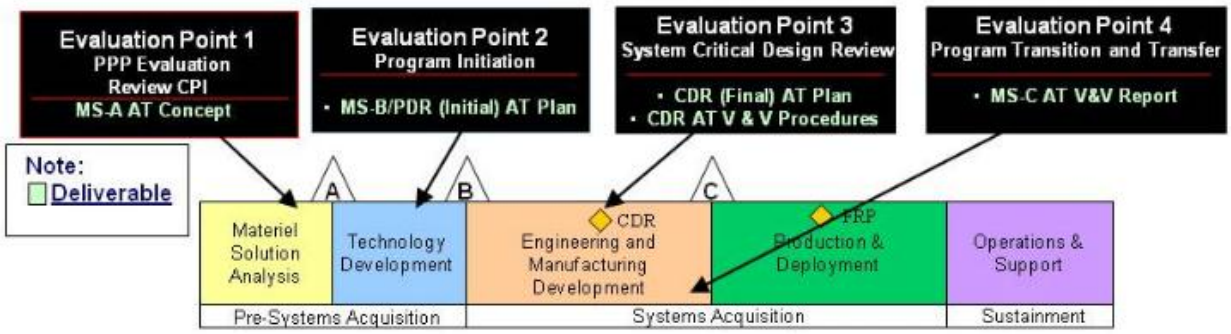
3.5.1. The PM must ensure all CPI is assessed and threats to CPI are continually monitored to determine if AT measures are required and appropriate. AT is incorporated into the program's systems engineering processes and should be discussed at system engineering technical reviews (see Figure 5.1 for examples of relevant reviews within the acquisition life cycle). Although not all programs will require an AT plan, the PM must consider application of AT measures to protect CPI resident on any system that has foreign participation (e.g. developed with allied partners), is likely to be sold or provided to U.S. allies and friendly foreign governments, or might fall into enemy hands on the battlefield. If a program has no

CPI or the PM believes the program has no AT requirements, then the PM should coordinate with SAF/AQL for a waiver recommendation letter to the MDA.

3.5.2. Early in the program's life cycle (MS A), (Fig 3.1.), PMs will follow published AT guidance or direction provided by SAF/AQLS for planning, validation, and documentation of AT effectiveness measures. The USAF AT Lead provides a suite of CPI identification tools to help determine if a program has Resident CPI. To register for CPI Tools, contact your local AT Representative. An approved initial AT Plan must have concurrence by USAF AT Lead for all Foreign Military Sales (FMS), while the initial AT Plan must be approved for Direct Commercial Sales programs.

3.5.3. The USAF AT Lead provides assessment reports of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS) products used in the protection of R-CPI. The USAF AT Lead also provides information on what the other Services are doing relative to AT practices, and of associated costs.

Figure 3.1. Anti-Tamper Evaluation Points (EP) for Programs.



3.5.4. AT Plans should be submitted NLT 60 days (and, to allow for Formal OUSD PPP coordination, 90 days for ACAT ID programs) before corresponding acquisition program milestone and ideally 120 days prior. The MS-A AT Concept (EP 1) includes a technical approach and cost estimate to initially price AT for the program. The MS-B/PDR AT Plan (EP 2) includes an updated resident CPI list and AT protection implementations. The CDR AT Plan and CDR AT V&V Procedures (EP 3) detail AT implementation. The MS-C AT V&V Report (EP 4) describes step by step AT V&V completion to ensure AT has been implemented properly.

3.5.5. The Acquisition Security Database (ASDB) is used to store USAF (and other Services') AT Plans. Upload and submit SECRET (collateral) domestic, FMS, and Direct Commercial Sales AT Plans via the ASDB. All AT Plans must be at least SECRET (collateral) per AT Security Classification Guide (SCG). Contact SAF/AQLS to submit plans classified higher than SECRET (collateral). ASDB Accounts are available on Secret Internet Protocol Router Network (SIPRNET).

3.5.6. The PM should document the analysis and recommendation to use or not to use anti-tamper measures in a classified annex to the PPP, and report findings to the MDA at Milestone A and subsequent decision points in the life of the program. The USAF AT Lead will provide an AT recommendation. The MDA will review the AT recommendation from

SAF/AQLS to reach an approval decision concerning the PM's recommended AT measures in the classified annex of the PPP.

3.5.7. The PM should reassess AT implementation for configuration changes.

3.6. Horizontal Protection. Horizontal Protection ensures that effective common countermeasures are used by programs that utilize similar CPI, yielding cost-effective applications of technology protection efforts. PEO AT Leads should assist the PEO Director of Engineering in validating each FMS and DCS program's R-CPI. Whenever possible, PMs should leverage the risk mitigation efforts of like programs in developing their own countermeasures. The ASDB is DoD's tool for the horizontal protection process. The PM should:

3.6.1. Review CPI data in the DoD ASDB and utilize the database to address any horizontal protection issues. See Chapter 4 for further details regarding the ASDB.

3.6.2. Coordinate with other affected program(s) when disputes involving the level of risk mitigation applied to shared or similar CPI arise. The PM's goal should be to understand, document, and communicate unacceptable risk mitigation differences to the affected program(s). If risk mitigation results in unacceptable or potentially unacceptable mission impact, the PM should report this to the MDA and courtesy copy the findings to affected program's (s') MDA and MAJCOM program protection POC for further action. Identical countermeasures are not necessarily required in each program. The PM's goal should be to achieve a commensurate level of risk mitigation acceptable by affected programs.

3.6.3. Coordinate with counterintelligence elements on horizontal protection and analysis issues involving the protection of CPI.

3.6.4. Maintain continuity of protection with respect to inherited CPI. Inherited CPI is CPI from other acquisition programs, subsystems, or projects that are being incorporated or implemented into another program.

3.7. Trusted Systems and Networks (TSN). TSN requirements have been developed (reference DoDI 5200.44) to minimize the risk that mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's critical functions or critical components by foreign intelligence, terrorists, malicious insiders, and other hostile or criminal elements. TSN strategy integrates robust systems engineering, Supply Chain Risk Management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust. SCRM is a subset of program protection that identifies susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and develops mitigation strategies to combat those threats. TSN requirements must be incorporated into the program's acquisition, systems engineering, and information assurance processes. TSN processes such as critical function analysis and protection is a discussion item at System Engineering Technical Reviews (SETR).

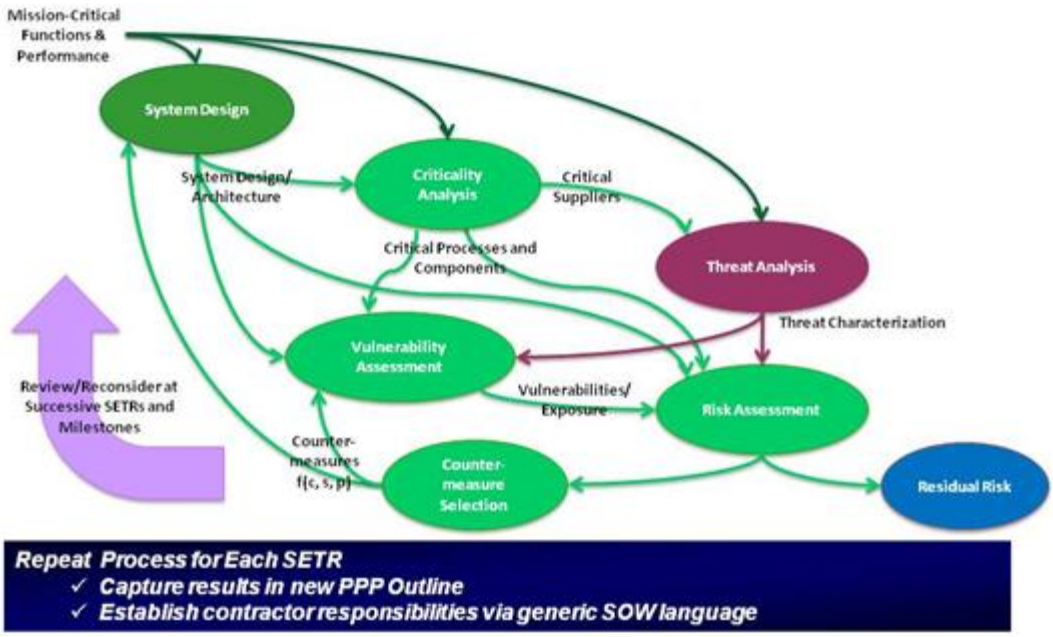
3.7.1. PM Implementation Activities:

3.7.1.1. Conduct comprehensive program protection analysis and mitigation to identify and protect critical components and information. PMs should assess threats and mitigate system security risks using cost-effective best practices such as secure system design.

3.7.1.2. Employ enhanced vulnerability detection tools when available. Continually assess mitigations and respond to new threats and vulnerabilities in critical components (e.g. cyber threats to programmable logic elements). As the system design evolves, criticality analysis, vulnerability assessment, risk assessment, threat analysis, and countermeasure selection must be reconsidered to reflect the current threat picture IAW DoDI 5200.39. (See Figure 3.2)

3.7.1.3. Contact the AFMC or AFSPC TSN focal point when critical components have been identified.

Figure 3.2. Criticality Analysis and Vulnerability Assessment Methodology.



3.7.2. TSN Focal Point Activities. The MAJCOM TSN focal point will provide the PM the appropriate threat information and potential mitigation options. The AFMC and AFSPC MAJCOM TSN focal points:

3.7.2.1. Coordinate and prioritize RFIs to the DIA SCRM TAC for threats to suppliers of critical components.

3.7.2.2. Coordinate with AFOSI to obtain assessments of suppliers of critical components and provide analysis of critical component supplier intelligence to the PM.

3.7.2.3. Provide PMs with key practices, and recommended strategies for vulnerability detection and risk mitigation to protect critical components upon request.

3.7.3. Mitigations. The PM should use intelligence assessments (such as SCRM TAC reports) on critical components to inform risk management decisions, including source selection. The PM should ensure the use of risk mitigations, such as SCRM Key Practices,

during the design of critical functions and prior to the acquisition of critical components or their integration within a system.

3.7.3.1. Secure System Design. Early in the system development life cycle, PMs should consider systems designs that reduce vulnerabilities of critical functions. PMs should apply assurance principles such as minimizing user privileges, reducing vulnerabilities, standardizing and simplifying architectures, increasing redundancy, diversity, and distribution for survivability, increasing agility through adaptability and reconstitution. PMs should consider, prioritize, and evaluate security attributes as part of overall system trade studies. PMs and Lead Systems Engineer should consider designs that mitigate supplier risk of a component. MIL-HDBK-1785, *Systems Security Engineering Program Management Requirements*, defines systems security engineering tasks and provides implementation guidance. See Chapter 5.

3.7.3.2. Key Practices. PMs will decide how to implement key practices obtained from the AFMC or AFSPC MAJCOM TSN focal point. These include, but are not limited to, diversifying sources including second and third tier suppliers, buying all supplies up front, limiting delivery times, and increasing supply chain transparency. For more information, reference DoDI 5200.44, the DoD SCRM Key Practices and Implementation Guide, and the DoD PPP Guidance in the Defense Acquisition Guide (DAG).

3.7.3.3. Trusted Suppliers. In accordance with DoDI 5200.44, in applicable systems, integrated circuit-related products and services are required to be procured from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use. The PM may also use accredited suppliers as best practice and risk mitigation concerns dictate. Specifically this direction applies to circuits which are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application specific integrated circuits or ASICS).

3.7.3.4. Use of the AF Network-Centric Solutions (NETCENTS) Contracts . The Air Force has established a series of Indefinite Delivery, Indefinite Quantity (ID/IQ) contracts to ensure adherence to Air Force Enterprise Architecture and allow for SCRM control mechanisms. PMs should use the NETCENTS contracts in the acquisition strategy of any ICT products or services when feasible and where it achieves an effective acquisition strategy. The NETCENTS-2 ID/IQ contracts include the following categories of ICT products and services in their scope: COTS Net-centric Products, Network Operations (NETOPS) and Infrastructure Solutions, Application Services, Enterprise Integration and Service Management (EISM) Advisory and Assistance Services (A&AS), and IT Professional Support and Engineering Services (ITPS) A&AS. NETCENTS-2 includes the following best practices to mitigate supply chain risk:

3.7.3.4.1. Requires refurbished products to be clearly identified as such.

3.7.3.4.2. Directs delivery orders to be TEMPEST compliant when required IAW Air Force Intelligence, Surveillance and Reconnaissance (ISR) Agency Instruction (AFISRAI) Checklist 90-203; AFISRAI 33-203, National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95; and National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, Annex B.

3.7.3.4.3. Requires the contractor to maintain a supplier inspection system.

3.7.3.4.4. Directs vendors to follow all Trade Agreements.

3.7.3.4.5. Requires all IA or IA-enabled IT products to be National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) compliant.

3.7.3.4.6. Requires the vendor to provide all associated software and associated peripherals as provided by the Original Equipment Manufacturer (OEM).

3.7.4. Documentation. Current DoD PPP direction requires the PM to l document the results of the criticality analysis and all TSN protection activities in the PPP. This includes:

3.7.4.1. Mission critical functions.

3.7.4.2. Critical components.

3.7.4.3. Criticality Levels (I, II, III, IV) for each identified critical component. Criticality is assessed by the relative impact on the system's ability to complete its mission if the component fails. Level I is total mission failure, Level II is significant/unacceptable degradation, Level III is partial/acceptable, and Level IV is negligible. See Appendix C of the PPP Outline and Guidance.

3.7.4.4. TSN planning and mitigation activities, including supplier risk decisions.

3.7.4.5. Significant threats that cannot be reasonably addressed through technical mitigation and countermeasures, and for which procedures have not been established.

3.8. Counterfeit Prevention. The objective of the AF counterfeit parts prevention capability is to ensure appropriate risk mitigations and protection of components in AF weapon systems and information systems throughout their life cycles. Per DoDI 5200.44, PMs are required to identify critical components vulnerable to counterfeiting, and maintain an updated list throughout the system life cycle. The term component includes software and hardware articles. As part of program protection, counterfeit prevention should be assessed at program reviews. PMs should ensure that contracts include language requiring prime contractors to take preventative steps at all levels of the supply chain based on risk to system integrity and to commit suppliers to provide authentic hardware, software, and firmware. The Defense Contract Management Agency (DCMA) works directly with DoD suppliers to ensure compliance with contractual terms and conditions. See the USD (AT&L) Supply Chain Integration website and DoDI 4140.01, *DoD Supply Chain Materiel Management Policy*, for further guidance on counterfeit materiel management. The PM should implement the following actions to mitigate the risk of incorporating any counterfeit parts into any systems:

3.8.1. Planning and Preventative Actions. Establish planning and preventative measures to mitigate counterfeiting risks and manage residual risk throughout the life cycle. See MIL-STD-3018, DoD *Standard Practice for Parts Management*, Standardization Document (SD)-19, *Parts Management Guide*, and SD-22, *Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook.*

3.8.1.1. Collaborate with contractor to implement security business practices in engineering, component purchasing, test and evaluation, manufacturing, and sustainment to mitigate threats to the supply chain of weapon systems.

3.8.1.2. Include robust design features to minimize vulnerabilities.

3.8.1.3. Define criteria for determining critical components vulnerable to counterfeiting (e.g., critical points of operational failure, rankings of risk and consequences of component failure based on criticality analysis).

3.8.1.4. Determine critical components that have a global supply chain. Consider using emerging industry standards such as those from the Independent Distributors of Electronics Association (IDEA) and the Society for Automotive Engineers (SAE) for practices and methods to mitigate risks from counterfeit electronic parts. Consider requiring contractual compliance with the standard adopted by DoD for counterfeit electronics, SAE Aerospace Standard (AS) 5553, *Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*, for critical components with a global supply chain.

3.8.1.5. Define triggers for alerts on counterfeits during fielding, pre-fielding, and inventory receipt processing (duplicate serial numbers in systems, physical inspection).

3.8.1.6. Determine life cycle events which provide opportunities for reviewing program protection efforts to prevent counterfeit materiel from entering a system's supply chain (technical reviews, milestone reviews, sustainment planning).

3.8.1.7. Determine how much risk is acceptable commensurate with threat, vulnerability, and consequences and adjust procurement strategy accordingly.

3.8.1.8. Avoid risky suppliers when possible.

3.8.1.9. Use original manufacturers or trusted suppliers whenever possible.

3.8.1.10. Require suppliers and contractors to provide notification when critical items are not obtained from the Original Equipment Manufacturer or an authorized distributor, particularly when electronic parts are included. This requirement should apply to suppliers below the prime contract as well.

3.8.1.11. Establish testing and verification requirements for items not received from an original equipment manufacturer, or authorized distributor that are identified as having high risk for counterfeit potential. These requirements apply to prime contracts, and to subcontracts or suppliers below the prime contracts.

3.8.1.12. Require traceability of parts origination and distribution.

3.8.1.13. Require product support providers (organic and contractors) to identify obsolete components.

3.8.1.14. Require that all personnel involved in the program receive initial training on anti-counterfeiting techniques and that those involved in the management of parts and DMSMS programs receive detailed training in anti-counterfeiting techniques. Further guidance is available at the USD (AT&L) Supply Chain Integration website.

3.8.1.15. Ensure CPI and critical components are documented in the PPP. Catalog critical components by National Stock Number (NSN), if applicable, with associated inventory indicative data. CPI and critical components may require specialized item management and/or inventory control. This approach should be discussed in the Systems Engineering Plan (SEP) or the Life Cycle Sustainment Plan (LCSP). The Item Unique

Identification (IUID) Implementation Plan includes the identified items. Reference DoDI 8320.04, *Item Unique Identification (IUID) Standards for Tangible Personal Property*.

3.8.1.16. Specify flow-down of applicable requirements regarding counterfeit parts to lower tier suppliers and maintain processes to verify such requirements.

3.8.1.17. Require static testing for critical software components.

3.8.1.18. Ensure software development contractors use sanitized compilers and testing tools.

3.8.1.19. Establish processes and procedures that ensures all software (including updates) originates from an authentic supplier. Validated CDs should be used to the maximum extent possible for software uploads. Website usage should be discouraged as counterfeit software suppliers are proficient at creating legitimate-appearing sites. When website downloads cannot be avoided, processes and procedures should be established to ensure downloaded code is appropriately validated.

3.8.2. Supplier Control Actions. Determine supplier control measures and actions including the following minimum set of counterfeit control measures:

3.8.2.1. Distributor assessments.

3.8.2.2. Product assurance processes.

3.8.2.2.1. Authenticity verification techniques.

3.8.2.2.2. Counterfeit material detection processes.

3.8.2.3. Materiel control processes. Determine the materiel control processes required for those who store, handle, or ship program materiel. Materiel control processes should ensure effectiveness in preventing counterfeit materiel and materials from entering the program's life cycle at any point in the acquisition process. The PM should ensure determination is made for the following activities:

3.8.2.3.1. Storage.

3.8.2.3.2. Handling.

3.8.2.3.3. Shipping.

3.8.2.4. Counterfeit materiel disposition processes. Implement a counterfeit materiel disposition process to ensure counterfeit materiel is removed once discovered. The chain of custody must be preserved. The materiel and relevant data should be sequestered for analysis by cognizant security personnel.

3.8.2.5. Reporting processes. PMs should ensure all instances of counterfeit or suspect counterfeit parts are reported in the Government and Industry Data Exchange Program (GIDEP) database and to the MAJCOM TSN focal point.

3.8.2.6. Feedback Loop. Monitor, report, investigate, and eliminate known and suspected breaches to in-service inventory assets.

3.8.3. Consequence Management Actions. Retain possession of confirmed or suspect counterfeit items. Manage infiltration of suspected or confirmed counterfeit parts into your supply chain IAW AFMAN 23-110, *USAF Supply Manual*, Chapter 16, "Management of

Suspect Counterfeit and Counterfeit Materiel." Reference AFI 51-1101, *The Air Force Procurement Fraud Remedies Program* and AFI 91-202, *The U.S. Air Force Mishap Prevention Program*. Programs should immediately notify their supporting contracting officer of confirmed or suspected counterfeit parts. Additionally, report suspected or confirmed counterfeit items discovered by DoD activities in the Government-Industry Data Exchange Program (GIDEP) using the Product Quality Deficiency Reporting process as appropriate.

3.9. Compromised CPI. The PM is required to provide written notification of any actual or potential compromise of US Government information designated as CPI (classified or unclassified) to local AFOSI CI and security officials IAW DoDD O-5240.02, *Counterintelligence*, DoDI 5240.04, *Counterintelligence (CI) Investigations*, DoDI 5200.39, DoDM 5200.01 v1, *DoD Information Security Program*, DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, and AFI 31-401, *Information Security Program Management*. This reporting ensures incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of the loss or compromise of CPI, and to preclude recurrence.

3.9.1. Incidents involving the Defense Industrial Base (DIB) or proprietary information where CPI is present will be managed under the provisions of DoDI 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities* (for DIB CS/IA Framework Agreement signatories only) and AFI 33-200.

3.9.2. Incidents involving the AF Global Information Grid (GIG) where CPI is present will be managed under the provisions of AFI 10-712, Telecommunications Monitoring and Assessment Program (TMAP) to initiate a Cyber Operations Risk Assessment (CORA).

3.9.3. Incidents involving electronic communication of classified information and/or Communications Security (COMSEC) equipment, whether test, evaluation or operational use should be reported IAW AFI33-200 and the supporting AFMAN 33-283, COMSEC, or AFMAN 33-386, TEMPEST Security, as appropriate.

3.10. Compromised Critical Components. The PM is required to provide written notification of any actual or potential compromise of an item identified as a "critical component" (classified or unclassified) to local AFOSI CI and security officials IAW guidance cited above. If there is a suspected or confirmed compromise of critical components, then the PM must assume there has been a potentially damaging malicious insertion into the system. However, criminal or malicious determination is not a PM's decision. Reference DoDI 5200.44, the DoD SCRM Key Practices and Implementation Guide (Key Practice 30) and the DoD PPP Guidance in the DAG.

3.11. Foreign Involvement. The PM should, with the support of DIA and TSN focal points, assess all suppliers of critical components for Foreign Ownership, Control, or Influence (FOCI). The PM should assess all items being considered for export or foreign involvement, including operation or testing, to determine if any additional protection countermeasures need to be designed-in or implemented to protect CPI and critical components. The PM should review all items, components, test activities, and data support packages for CPI and critical components and protect accordingly, to include working with the contracting officer to determine if contract changes are required. SAF/IAPD is the approval authority for delegated disclosure authority to the Foreign Disclosure Office (FDO) in support of both one-time and continuing disclosure requirements. Programs with foreign involvement are required to comply with the following

activities IAW DoDD 5530.3, *International Agreements*; DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*; DoDI 2040.02, *International Transfers of Technology, Articles, and Services;* Defense Security Cooperation Agency (DSCA) 5105.38-M, *Security Assistance Management Manual (SAMM)*; DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM); and AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*:

3.11.1. When it has been determined there will be foreign involvement (e.g. cooperative research and development, production, test, maintenance, training), or work performed for the US by companies under FOCI, the PM is required to prepare a Technology Assessment/Control Plan (TA/CP), Delegation of Disclosure Authority Letter (DDL), and Program Security Instruction (PSI) prior to formal engagement. (Reference DoDD 5530.03) The TA/CP annex to the PPP identifies security arrangements for international programs and is used to:

3.11.1.1. Document all FMS transactions or international agreements and cooperation involving the transfer of CPI to specific countries.

3.11.1.2. Assess the feasibility of the United States' participation in joint programs from a foreign disclosure and technical security perspective.

3.11.1.3. Prepare negotiation guidance on the transfer of classified information and Resident CPI involved in the negotiation of international agreements.

3.11.1.4. Draft the DDL that provides specific guidance on proposed disclosures.

3.11.1.5. Plan for Foreign Military Sales (FMS), Hybrid FMS-Direct Commercial Sales, and co-production or licensed production of the system or international cooperative agreements involving U.S. technology or processes.

3.11.1.6. Recommend the extent and timing of foreign involvement in the program, foreign sales, and access to program information by foreign entities.

3.11.2. The PM is required to adhere to overall systems protection requirements during the disclosure of CPI to foreign governments and international organizations in support of international programs.

3.11.3. The PM should confirm Air Force information authorized in the DDL is representative of the item being sold or considered for sale, development, or transfer.

3.11.4. The PM should develop a PSI prior to formal engagement (NOTE: The PSI is only required for foreign co-development programs).

3.11.5. The PM must document all FMS transactions or international agreements and cooperation involving the transfer of CPI to specific countries in the PPP’s TA/CP annex. The TA/CP annex will take into account the review of all export provisions already in place i.e. DDL's commercial, and other DoD service exports.

3.11.6. The PM must confirm CPI protective countermeasures are adequate prior to the export of the CPI to foreign governments and international organizations.

3.11.7. The PM should provide the FMS Case Manager or international agreement Project Officer with protection guidance, including countermeasures, for all items/components that will include CPI or critical components.

3.11.8. The PM must conduct and document a follow-on support analysis, normally as part of the foreign sales portion of the TA/CP, to ensure compliance with protection considerations.

3.11.9. The PM should address information assurance and protection of critical U.S. systems giving special consideration to vulnerabilities resulting from reliance on the information support infrastructure and the risk of their loss, damage, or destruction.

3.12. Counterintelligence Support. PMs must seek counterintelligence support for all CPI and critical components threat determinations. AFOSI provides the following CI support to assist the PM in assessing threats and developing appropriate countermeasures IAW DoDI O-5240.24:

3.12.1. Supporting the PM with development and implementation of a CI Support Plan (CISP). The CISP describes CI activities in support of the program.

3.12.2. Preparing Counterintelligence Threat Assessment (CITA). Programs must request CITAs upon initial identification of CPI and critical components and upon any programmatic changes affecting CPI and critical components (i.e., locations, system configurations, contractor involvement). PMs will ensure their local CI support is consulted regarding need to update existing CITAs.

3.12.3. Providing analytical studies or risk assessment products from the Defense Security Service (DSS) on foreign threats from Foreign Ownership, Control and Influenced (FOCI) risks or Committee on Foreign Investment in the United States (CFIUS) cases.

3.12.4. Supporting DIA and NASIC analysis of foreign need, intent, capability, targeting, and collection pertaining to CPI and critical components.

3.12.5. Providing PMs, via TSN focal point, with DIA SCRM TAC assessments of critical components.

3.13. Intelligence Support. PMs should seek appropriate intelligence for Technology Targeting Risk Assessments (TTRA) when requesting intelligence production. Center Intelligence Officers or program intelligence representatives facilitate the PM in assessing threats and developing countermeasures by providing the following:

3.13.1. Forecasts of the military technology needs of threat countries and potential development areas that could impact program protection (CPI and critical component).

3.13.2. Intelligence on the current state of foreign technologies contrasting the market forecast of competitive countries with U.S. technology efforts in each CPI.

3.13.3. Predictive intelligence on foreign cyber capabilities and intent.

3.14. Reviews. Program protection requirements and measures should be reviewed for risk mitigations during program and SETRs (see Figure 5.1). The following reviews (at a minimum) provide the PM opportunities to confirm that the program has addressed the adequacy of the comprehensive program protection approach:

3.14.1. Alternative System Review (ASR)

3.14.2. System Requirements Review (SRR)

3.14.3. System Functional Review (SFR)

3.14.4. Preliminary Design Review (PDR)

3.14.5. Critical Design Review (CDR)

3.15. Contractual Considerations. Contractual provisions must be in place to support the approved PPP. Solicitations, requirements documents, and contracts with industry must require the protection of CPI and critical components outlined in the PPP and placed on contract via the DD 254, *Contract Security Classification Specification*. (See DoDI 5200.44) PMs should ensure that requirements documents require prime contractors and subcontractors, as applicable, to:

3.15.1. Support the PM's identification and protection of CPI and critical components. Protection should be based on security requirements and selected countermeasures. See Chapter 5 of this document.

3.15.2. Produce and use a Program Protection Implementation Plan (PPIP) or appropriate deliverable to document the contractor's measures to protect CPI and critical components at their facilities and supplier locations consistent with the Government's PPP.

3.15.3. Properly identify, mark, and protect all controlled unclassified information. Comply with the provisions of DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems*, as applicable.

3.15.4. Communicate program protection requirements to subcontractors who are also responsible for identifying, accessing, marking, handling, and protecting CPI or critical components.

3.15.5. Assess the security practices of subcontractors or suppliers and continually monitor their compliance with protection measures. Contracts should include clauses to ensure software assurance and static and dynamic code reviews on software developed for delivery to the Government.

3.15.6. Implement, and as appropriate require subcontractors to implement, supply chain risk management and information assurance best practices. This should include identifying potential suppliers of critical components and identifying processes to control access by foreign nationals to software, hardware, and associated classified and unclassified information used to integrate commercial technology. Additionally, the PM must ensure the implementation of processes to protect classified and controlled unclassified DoD information.

3.15.7. Require counterfeit prevention processes and requirements for all levels of subcontractors. Include DFARS clause 252.246-7003, Notification of Potential Safety Issues, in contracts for critical components Ensure contractor and subcontractor reports of suspected or confirmed counterfeit items are entered into the Government-Industry Data Exchange Program (GIDEP) system, which will serve as the DoD central reporting repository.

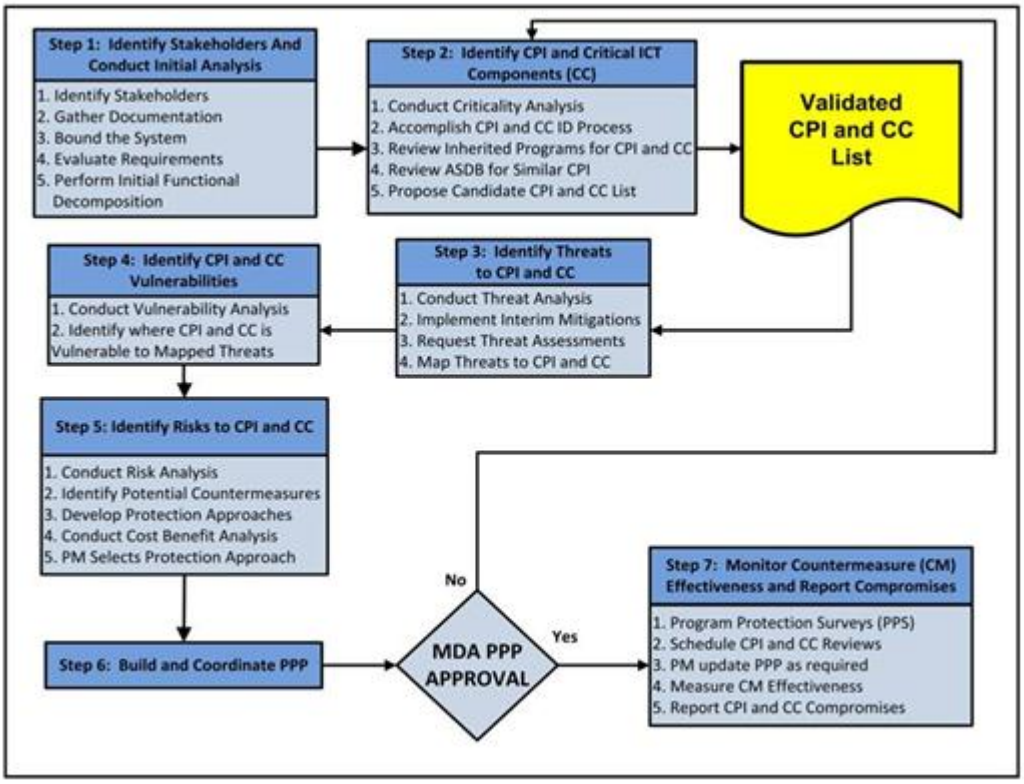
3.15.8. Allow Government personnel or designee access to prime contractor and subcontractor facilities to enable surveys, assessments, and inspections to verify the successful implementation of protection activities.

Chapter 4

PROGRAM PROTECTION PROCEDURES

4.1. Overview. This chapter outlines the procedures to gather all the inputs and analysis required as part of program protection. Figure 4.1 presents the seven suggested program protection steps to follow which are detailed in this chapter. PMs may tailor these steps to meet the program's circumstances.

Figure 4.1. Program Protection Procedures.



4.2. Step 1: Identify Stakeholders and Conduct Initial Analysis. This step includes identifying stakeholders and functional experts, gathering relevant program documentation, bounding the system, evaluating the requirements, and performing an initial functional decomposition. The PM identifies stakeholders and subject matter experts from the operational, scientific, acquisition, logistics, sustainment, engineering, security, intelligence, and information protection communities. Consider forming and chartering an Integrated Process Team, which can be useful to the PM as a management approach. See Attachment 2 for scope of membership and activities.

4.3. Step 2: Identify Critical Program Information (CPI) and Critical Components. The PM must continually evaluate system security risks in relation to cost, schedule, and performance. CPI and critical components (whether technology, components, or information) must be identified to prioritize and manage system security risks. Helpful program documentation, if available, includes, but is not limited to: Systems Requirements Document,

Capability Development Document, system schematics such as Operational Activity Models, Work Breakdown Structure, and Information Support Plan (ISP) (Operational View (OV)-5 and associated activity models, if available).

4.3.1. Conduct Criticality Analysis. IAW DoDI 5200.44, criticality analysis is an end-to-end functional decomposition performed to identify mission-critical functions and components. It includes identification of missions, a decomposition of each mission set into the functions to perform those missions, and the traceability to the hardware, software, and firmware components that implement those functions, protect those functions, or have unmitigated access to those functions. Criticality is assessed in terms of relative impact on the system's ability to complete its mission if the component fails or is compromised. Criticality analysis determines:

4.3.1.1. Mission criticality and prioritization of mission capability.

4.3.1.2. Critical functions that support the prioritized mission capabilities and the prioritization of those functions.

4.3.1.3. Critical components that support the prioritized critical functions. The list of all critical components in applicable systems is documented in the PPP.

4.3.2. Accomplish CPI and Critical Component Identification Process. PMs should identify CPI and critical components early in the development, to include the Materiel Solution Analysis Phase. Technologies transitioned or inherited from another program should also be evaluated. Once initial analysis from Step 1 has been completed, system decomposition should be performed in order to apply the CPI Identification Survey and Decision Aid (See Attachment 8). The PM should determine which items will have the CPI Decision Aid applied to them. The system should be decomposed to the lowest possible level in order to identify potential CPI and critical components with sufficient granularity. Identifying CPI and critical components at the lowest sub-system or component level possible is a critical enabler of focusing countermeasures. How far a system is decomposed will vary based on the nature and complexity of the system. For example, a radar receiver group might be decomposed to specific device or part. In such a case, identifying the entire suite as potential CPI or critical components versus a piece part could have significant impact (cost and schedule) to the program in the application of countermeasures.

4.3.2.1. ACAT PMs should use the CPI Identification Survey and Decision Aid found in Attachment 8 to quickly identify if a program has the potential for containing CPI.

4.3.2.2. The PM should document in the PPP the list of critical functions and critical components identified during the criticality analysis. The PM should build the PPP for these components whether or not he or she determines the program has CPI. The level of decomposition will depend upon the maturity of the program, however it should complete prior to the Critical Design Review (CDR). See DoD PPP Outline and Guidance in the Defense Acquisition Guide (DAG) Chapter 13.

4.3.2.3. The PM documents the methodology for identification of CPI, critical components, and mission critical functions in the PPP.

4.3.3. Identify Inherited CPI. Inherited CPI is technology, components, or information not originating from or organic to the program. Review CPI and protection measures of any

program or technology which is being incorporated into, interfaces with, or is a sub-system of the parent program. Inherited CPI protection measures can aid in the selection of appropriate CPI protection measures or to recommend changes in existing protection measures. The receiving PM is responsible for ensuring inherited CPI protective measures are adopted to meet horizontal protection requirements and protection methodology intent. Protection should be based upon its role in the inheriting system and its original role (horizontal protection). Also review CPI and/or protection measures for programs sharing like capabilities to ensure horizontal protection is maintained.

4.3.4. Review ASDB for Similar CPI. The Acquisition Security Database (ASDB) is DoD's tool for implementing horizontal protection. The ASDB is only used for CPI.

4.3.4.1. Once CPI has been identified PMs should review ASDB for other programs' existing or similar CPI.

4.3.4.2. PMs should review the ASDB at least once every three (3) years during the PPP review cycle or more often if there are changes in the program causing a review of CPI or critical components.

4.3.4.3. PMs should check for the presence of unidentified inherited CPI.

4.3.4.4. In cases where CPI for like programs exists outside the ASDB, review those programs for inherited CPI.

4.3.4.5. Horizontal Protection Adjudication. If an inconsistency in classification or protection countermeasures exists for the program's CPI or related CPI, the PMs should use the horizontal protection adjudication process to resolve or mitigate the risk.

4.3.4.5.1. PMs should determine, based upon a comparative analysis of levels of protection, if countermeasures involving another program's CPI will result in relatively equal protection afforded to the CPI by each program.

4.3.4.5.2. If there are disagreements regarding classification of CPI and/or related information which cannot be resolved informally, formal Original Classification Authority challenging procedures should be followed for resolution.

4.3.4.5.3. Horizontal protection adjudication should be performed at the lowest common level of authority for the programs involved. For example, disputes between programs with the same MDA should be resolved by that MDA. Disputes between AF programs with different MDAs should be resolved by the SAE. Disputes across Services should be resolved by Under Secretary of Defense for Acquisition, Technology, and Logistics, USD (AT&L), as noted below.

4.3.4.5.4. After the horizontal protection process has been adjudicated, each of the programs should update their PPPs and the ASDB to record the results of the adjudication. This will likely include either updating (adding or modifying) the CPI list and/or updating the countermeasures that will be implemented to protect the CPI. If classification level of CPI changes based on horizontal protection adjudication process, ensure the SCG is updated to reflect the change.

NOTE: If USD (AT&L) becomes aware that there is a contradiction in the identification and/or protection of CPI between two programs that are being executed by different Service organizations, then USD (AT&L) will first inform the two programs of the issue and request that

they work together to resolve the issue. If the Services cannot come to an agreement on the resolution, the USD (AT&L) decision authority will adjudicate the issue and make the final decision.

4.3.5. Propose Candidate CPI and Critical Components Lists. The most fundamental decisions in the entire process are the CPI baseline and critical components determinations. These determinations should be approved by the PM and validated by the PEO prior to further PPP development in order to begin CPI and critical components protection immediately. The CPI and critical components determinations will be further validated by the MDA upon approval of the PPP (see Figure 4.1).

4.3.5.1. Validate CPI and Critical Components List. The PM should approve the CPI and critical components lists, obtain PEO validation, then ensure entry of new CPI into the ASDB within 15 days of CPI determination. Ensure CPI and associated information is marked/classified IAW the appropriate SCG. Prior to ASDB entry, CPI will be evaluated for classification using the program's SCG.

4.3.5.2. Reassess the CPI and Critical Components Determination. CPI and critical components will be assessed at each milestone, modification, or as directed by the MDA or equivalent decision authority. In addition to all PPP updates for milestones, the PM should assess all modifications and configuration changes for impact to CPI and critical components and the PPP should be updated accordingly. Protection assessment results should be included as part of the PM's configuration management process. For further guidance see Attachments 5 and 6.

4.4. Step 3: Identify Threats to CPI and Critical Components. A threat is anything that impacts the ability to protect technology, information, and components from unintended use. Threats to systems may result in loss or degradation of CPI or critical components. Threats are not static, and the program must be diligently monitored for changes in threat. A program's CPI and critical components and critical functionality face many types of threats. A threat may also arise from a natural event. Multiple resources should be used to develop a comprehensive picture of the threat environment to include the probability of a threat occurring. Attachment 3 provides threat identification methodology, threat assessment options, and procedures. When a threat has been identified, the PM should:

4.4.1. Conduct Threat Analysis. During initial threat analysis events, the PM may not be fully informed by specific intelligence and should therefore focus on deciding what kinds of threats may exist and what type of intelligence will be required. After receiving specific intelligence, further threat analysis must occur. Identifying threats must be accomplished throughout the life cycle. Multiple threat analysis events should be planned.

4.4.2. Implement Interim Mitigations. Interim mitigations or countermeasures should be implemented immediately for CPI and critical components.

4.4.3. Request Threat Assessments.

4.4.3.1. Contact the servicing AFOSI detachment to request a Counterintelligence Threat Assessment (CITA) on the program's CPI list.

4.4.3.2. For supply chain risk issues, contact the AFMC or AFSPC MAJCOM TSN focal point to request DIA SCRM TAC reports on the program's critical components list, and

for submitting RFIs on critical components. Reference Attachment 3. PMs should work through the Center Intelligence office to request additional intelligence support as needed to identify threats.

4.4.3.3. PMs is required to request updated threat assessments for existing CPI and critical components every three years per DoDI O-5240.24.

4.4.4. Map threats to each CPI and Critical Component**.** Conduct additional threat analysis events as new intelligence becomes available.

4.5. Step 4: Identify CPI and Critical Component Vulnerabilities. Identification of CPI and critical components vulnerabilities should occur as an independent process. For efficiency they can be sequenced to occur concurrently with threat identification. These vulnerabilities may include aspects of the technology development environment, the systems design, or the methods used to procure the component. Attack vectors should be determined based upon how the system is vulnerable to threats. Attachment 4 provides detailed information on vulnerability analysis methodology and procedures.

4.5.1.1. Conduct Vulnerability Analysis.

4.5.1.2. Document concept, technology, or system security vulnerabilities as well as perceived value to adversaries.

4.5.1.3. Identify impacts to criticality of mission success in deployment.

4.5.1.4. For systems with distinct electromagnetic or acoustic emissions, identify the susceptibility that an outside agency may be able to collect these emissions and the impact of such collection.

4.5.2. Identify where CPI or Critical Components are vulnerable to mapped threats. This should be informed by likely adversarial attack vectors.

4.5.3. Contractual Language. Contractual language should require contractors to assist in identifying CPI and critical components and produce a Program Protection Implementation Plan (PPIP) or other appropriate deliverable consistent with the Government's PPP. If CPI is identified after contract award (e.g. during technology development in a laboratory effort), ensure a security survey is conducted within 90 days after CPI is identified and ensure the contract is amended to include the PPP requirement at the next contract update or within one year (whichever is sooner).

4.6. Step 5: Identify Risks to CPI and Critical Components. Compliance based protection measures, potentially classified components, and critical infrastructure requirements must be identified at the earliest time to be included in the comprehensive program protection scheme. System security engineering methodology is critical to the development of systems that are designed to address protection concerns. See Chapter 5 and Attachment 5 for further guidance to accomplish the following activities:

4.6.1. Conduct Risk Analysis. Determine where the interaction of threats and vulnerabilities creates risk.

4.6.1.1. Assess the probability that an adversary can exploit the vulnerability.

4.6.1.2. Assess the consequence to the system, mission, or personnel if an adversary successfully exploits the vulnerability.

4.6.1.3. Determine residual risk based on probability and consequence.

4.6.1.4. Develop mitigations and countermeasures for all moderate or higher risks.

4.6.2. Identify Potential Countermeasures. Nominate potential countermeasures based upon the perceived attack vectors identified during threat analysis and vulnerability analysis.

4.6.3. Develop Protection Approaches. Assess countermeasure effectiveness without respect to cost.

4.6.4. Conduct Cost Benefit Analysis. Estimate cost of countermeasures for cost/benefit analysis. Risk tolerance is also an important consideration during risk analysis.

4.6.5. PM Selects Protection Approach. Develop final countermeasures for consideration and approval by the PM. Risk mitigations selected for implementation should include countermeasures that the program can use to protect against the highest priority attack vectors. Final countermeasures should be identified as a change to process documentation, system requirements, or other contractual document change (e.g. Statement of Work (SOW)).

4.6.6. PMs should assess residual risk to each identified risk/vulnerability based upon the proposed countermeasure and perceived effectiveness.

4.7. Step 6: Build and Coordinate a Program Protection Plan. The program protection work/decisions/outcomes will be captured in the PPP and associated annexes. Information collection to finalize PPP development begins with the results of the criticality analysis and the identification of CPI and critical components. Supporting documentation of the analysis and decision-making processes is critical to acceptance of the plan by the approval authority. Required attachments are determined by the nature of the program. Reference Attachment 7.

4.8. Step 7: Monitor Countermeasure Effectiveness and Report Compromises. The PM should monitor the effectiveness of the program protection approach. Countermeasures can eliminate or reduce the projected vulnerabilities and, within the parameters of risk management principles, negate an adversary's ability to exploit any vulnerability. To ensure countermeasure effectiveness, personnel with access to CPI and critical components must understand procedures and methods to protect the CPI and critical components. If countermeasures are determined to be less effective than required, then the countermeasures and/or risk assessment should be re-examined. For further information see Attachment 6.

4.8.1. Program Protection Surveys (PPSs). The PM is responsible for ensuring that a PPS is conducted on contractor and sub-contractor facilities supporting ACAT I and II programs containing CPI or critical components at least once during each integrated life cycle phase. See Attachment 6 of this document and DoD 5200.1-M. The PPS must be a contract requirement.

4.8.2. CPI and Critical Components Reviews. PMs should assess CPI and critical components to confirm validity of the CPI and critical components determinations and related protection countermeasures. These reviews should address all of the above program protection process steps. These reviews should occur:

4.8.2.1. Every three years.

4.8.2.2. Upon receipt of updated threat assessments for existing CPI and critical components.

4.8.2.3. When there are significant changes in the configuration of the program.

4.8.2.4. When monitoring identifies degradation in effectiveness of countermeasures.

4.8.3. Updates to PPPs. The PM should review the PPP for currency at least once every three (3) years. This includes requesting updated threat assessments for the program's CPI and critical components throughout the life cycle of the program and at each milestone. Sustainment programs should follow the same process identified in Section 4.8.2 for the review of CPI and critical components and the update to the PPP. Also, systems in Sustainment undergoing modifications should follow the same process for CPI and critical components identification and update the PPP to ensure protection of upgrades to the system.

4.8.3.1. Countermeasures should be modified or terminated when no longer required or determined to be ineffective. Changes to CPI countermeasures should be reflected in the ASDB.

4.8.3.2. PPP updates during the life cycle of the system, to include sustainment and at each milestone, should be coordinated with MAJCOM users to ensure synchronization with MAJCOM requirements documentation, funding, training, testing, certification, sustainment, installation security planning, and operational risk acceptance decisions prior to operational transition.

4.8.3.3. The technical content and currency of the PPP should be validated before any portfolio transfer or transition to the operational and/or sustainment organization. CPI and critical components supporting artifacts should be included with the transition.

4.8.3.4. Upon completing the PPP and threat assessment review, the PM should:

4.8.3.4.1. Document the results of the PPP review confirming that recent threat assessments did not reveal any change in threat to the program's CPI or critical components; or

4.8.3.4.2. Update the PPP because there has been a change in the program's CPI, critical components, and/or a change in the threat confirmed by the results of the threat assessments.

4.8.4. Measure Countermeasure Effectiveness. Measures of effectiveness should be developed. The PM uses measures of effectiveness to monitor countermeasure performance and perform a reassessment of CPI and critical components protection measures.

4.8.5. Report Compromises. Procedures for handling compromises should be developed and included in the PPP. The loss or theft of CPI or critical components presents a threat to the warfighter's capability and DoD's technological superiority. Reports of loss or theft ensure such incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects and to preclude recurrence.

4.8.5.1. Compromise. Any potential compromise of CPI or critical components is required to be immediately reported to the PM. The PM is required to provide written notification of any actual or potential compromise of US Government information designated as CPI (classified or unclassified) to the servicing CI and security officials IAW DoDD O-5240.02, *Counterintelligence*, DoDI 5240.04, *Counterintelligence (CI) Investigations*, DoDI 5200.39, DoD 5200.01 v1, *Information Security*, DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, and AFI 31-401,

Information Security Program Management. In addition, the PM should review the ASDB to determine if there is a possible impact to other programs. The PM should inform the servicing intelligence and AFOSI detachment if other programs may be affected. AFOSI should review the ASDB to determine if there is a possible impact to other programs. The PM should take the following actions upon discovery of a compromised critical component:

4.8.5.1.1. Protect the fact of a compromised critical component as CONFIDENTIAL information or at a higher classification if directed by the program Security Classification Guide.

4.8.5.1.2. Retain possession of all compromised critical components.

4.8.5.1.3. Notify the local AFOSI official not later than 72 hours after discovery.

4.8.5.1.4. Contact the AFMC or AFSPC TSN focal point for potential mitigations.

4.8.5.1.5. Notify the COMSEC Responsible Officer or COMSEC Account Manager (CAM) within 24 hours for incidents involving electronic communication of classified information and/or Communications Security (COMSEC) equipment, whether test, evaluation or operational use.

4.8.5.2. Theft. Upon indication of theft of CPI, whether involving unclassified or classified, contractor proprietary, or Air Force/DoD data, PMs should notify the PEO with either proposed countermeasures and/or mitigation strategies or indicate a proposed acceptance of the threat risk and the rationale. PMs should present initial mitigation plan to the PEO within 30 days. If adequate countermeasures or mitigation strategies cannot be put in place or the risk is unacceptable, the PM should determine and document if protection of the CPI and critical components is still warranted for the program. This determination should include impact on other affected programs through horizontal analysis. If protection is no longer warranted and there is no impact to other programs, the PM should take action to end protection countermeasures in future program and contracting actions.

4.8.5.3. Damage Assessments.

4.8.5.3.1. Damage assessments are conducted by SAF/CIO A6 for DIB CS/IA Framework Agreement signatory companies only. Damage assessments for classified information are conducted by the Original Classification Authority (OCA). When CI authorities suspect or confirm the involvement of criminal(s), and/or foreign entity(s), including foreign intelligence service(s), in a compromise incident, the PM will provide notification of the incident to the PEO, the servicing Information Protection Office, the Original Classification Authority (OCA) for classified compromises, and the Designated Accrediting Authority.

4.8.5.3.2. PMs will fully cooperate with the damage assessment process to include providing subject matter experts to assist in the evaluation of the incident's impact and development of countermeasures.

4.8.5.3.3. Within 30 days of the damage assessment report, the PM should provide the PEO a written response to the damage findings along with proposed countermeasures and/or revised mitigation strategies that nullify the advantages

gained by an adversary from the captured information, or propose acceptance of the threat risk and rationale.

4.8.5.4. ASDB Updates. PMs will update the ASDB after each confirmed compromise of CPI.

Chapter 5

PROGRAM PROTECTION THROUGHOUT THE LIFE CYCLE

5.1. Overview. Program protection may require systems security engineering or secure systems design to control system vulnerabilities and contain risks through sound engineering principles. These methods eliminate or reduce the vulnerability of Critical Program Information (CPI) or critical components to loss or compromise, and include any method (e.g., anti-tamper techniques, or information assurance) that effectively negates a foreign interest capability to exploit CPI vulnerability. Reference MIL-HDBK 1785 for more on recommended systems security activities. The secure systems designer:

5.1.1. Identifies, designs, develops, and tests security features in Air Force weapons systems until protection is no longer required (e.g., the system is demilitarized, or the technology is approved for release to the public).

5.1.2. Develops and implements systems engineering countermeasures to reduce vulnerabilities.

5.1.3. Considers possible enemy capture of the system.

5.1.4. Considers potential foreign involvement and defense exportability features so that the system is cost effectively designed and will facilitate security cooperation from international research, development, and acquisition through foreign military sales with partner nations.

5.1.5. Is part of new developments (including off-the-shelf and non-developmental items) and modifications of existing systems to minimize the operational costs of protecting deployed systems.

5.2. Context of Program Protection within SE. In order to be cost-efficient and technically effective, system security engineering must be integrated into the program's systems engineering approach. The PPP should describe the linkage between system security engineering and the Systems Engineering Plan and describe how the system security design considerations will be addressed. PMs must consider program protection throughout the system life cycle as part of systems engineering to provide a comprehensive, iterative, systems engineering approach. The systems engineer:

5.2.1. Specifies, predicts, and evaluates the vulnerability of the system to security threats.

5.2.2. Identifies and minimizes vulnerabilities to known or postulated threats.

5.2.3. Characterizes security risks to the system in the operational environment.

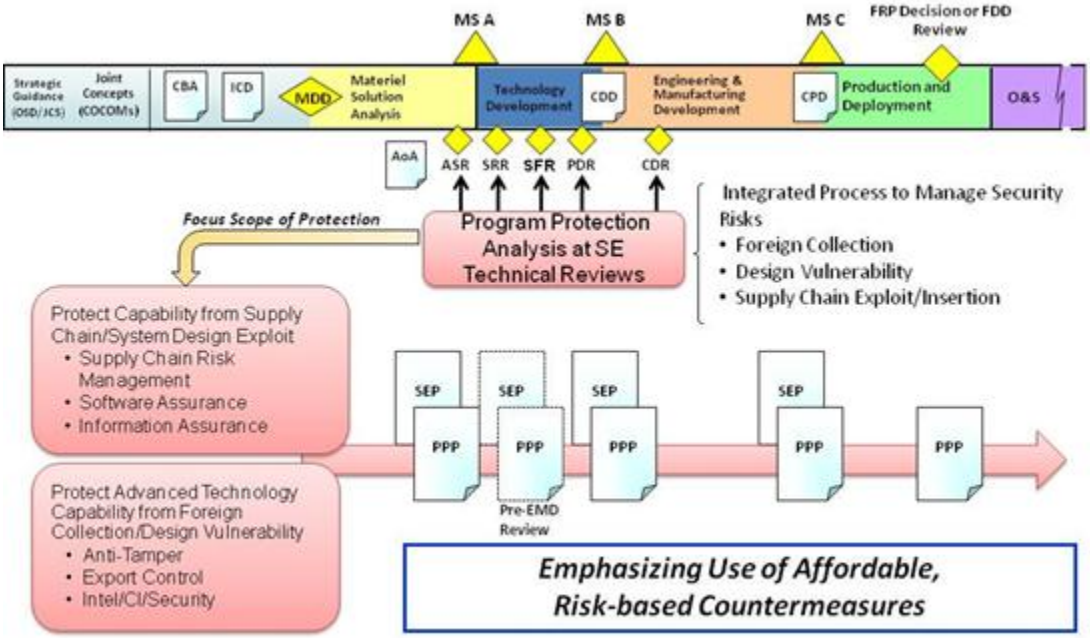
5.2.4. Develops risk mitigation approaches.

5.2.5. Develops a comprehensive security risk management program.

5.2.6. Translates mission needs and vulnerabilities into system security requirements for development, Test & Evaluation (T&E), manufacturing, verification, deployment, operations, support, training, and disposal.

5.2.7. Reduces technical acquisition risks through early identification of security requirements and their associated costs and effectiveness.

Figure 5.1. Program Protection in the Acquisition Life Cycle.



5.3. Program Protection in the Acquisition Life Cycle. The tasks detailed in this section should be applicable throughout the system life cycle for any pre-Milestone A effort, new acquisition program, upgrade, modification, resolution of deficiency, or technology refresh. Activities can be specified for each of the phases leading up to a major program milestone. See Figure 5.1.

5.3.1. Material Solutions Analysis. System security engineering should be used in early concept development to evaluate mission threads, identify system functions, and analyze notional system architectures to identify mission critical functions. The Capstone Threat Assessment (CTA) is the authoritative threat document for pre-milestone acquisition activities.

5.3.1.1. Development planning efforts should evaluate protection concepts.

5.3.1.2. An Analysis of Alternatives (AoA) decision includes weighing the relative costs and benefits of implementing different system protection features.

5.3.1.3. Technology Development Phase (or equivalent). Security activities during this phase are developed based on the System Threat Assessment Report (STAR) if available, Counterintelligence Threat Assessment (CITA), Capstone Threat Assessments (CTAs), other threat assessments as appropriate for the program, and the Acquisition Strategy (as it relates to international partnering and potential for foreign military sales). See Attachment 10 for specific program protection tasks that should be performed in the Technical Development phase.

5.3.1.4. Designing in System Security. The system designer should analyze protection requirements for the system's critical functions and components. Portions of the system may need to be re-designed to minimize compromising the system or its technologies.

The PM should ensure the following program protection activities take place during the Technology Development Phase:

5.3.1.4.1. Update or refine PPP from the previous phase.

5.3.1.4.2. Define or refine system specifications.

5.3.1.4.3. Update or refine the security vulnerability analysis.

5.3.1.4.4. Identify product security requirements.

5.3.1.4.5. Conduct cost benefit analysis and trade studies.

5.3.1.4.6. Conduct systems security risk analysis and studies.

5.3.1.4.7. Update or refine certification and accreditation requirements. (Reference AFI 33-210, DoDI 8510.01)

5.3.1.5. Allocating System Security Requirements. The Government and contractor should both directly support the allocation of system security requirements into program documentation and activities in preparation for the Milestone B Decision. PMs should ensure system security requirements are contained in:

5.3.1.5.1. Request for Proposal (RFP) - security requirements for the contractor.

5.3.1.5.2. Statement of Objective (SOO), SOW, System Requirements Document (SRD), or system specification as appropriate.

5.3.1.5.3. Contract Data Requirements List (CDRL).

5.3.1.5.4. DD Form 254, Contract Security Classification Specification.

5.3.1.5.5. Applicable Data Item Descriptions (DID).

5.3.1.5.6. Source Selection Planning.

5.3.1.5.7. Wartime Reserve Modes (WARM). For systems with distinct electromagnetic or acoustic emissions, evaluate the potential for WARM. WARM are characteristics and operating procedures of sensors, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance.

5.3.1.5.8. Planning Instruments.

5.3.1.5.8.1. Information Assurance Risk Analysis.

5.3.1.5.8.2. Communication Security (COMSEC) Equipment Plans.

5.3.1.5.8.3. Security Classification Guide.

5.3.1.5.8.4. Security System Concepts.

5.3.1.5.8.5. Demilitarization and Disposal Plan.

5.3.2. Engineering and Manufacturing Development Phase. The PM should continue the integration of system security design/countermeasure features based on the work done in the previous phase.

5.3.2.1. Designing in System Security. The PM should ensure the steps followed in 5.3.1 of this document are followed as applicable during the Engineering and Manufacturing Development Phase.

5.3.2.2. Allocating System Security Requirements. The Government and contractor should both directly support the allocation of system security requirements into program documentation and activities in preparation for the Milestone C Decision. PMs should ensure system security requirements are updated and included in the documents cited in 5.3.1.5. of this document.

5.3.2.3. Performing or Updating Key Program Protection Tasks. If not previously accomplished, or if the program is undergoing modification or other changes in design, implementation, or operation, PMs should reference Attachment 10 for specific program protection tasks that should be performed in the Engineering and Manufacturing Development phase.

5.3.3. Production & Deployment Phase. Production-related security will usually be the responsibility of the government's industry partners. For industry security procedures, see DoD 5220.22-M. The following is a list of activities required for program protection during this phase:

5.3.3.1. Update or refine system/subsystems interface specifications, vulnerability analysis, system architecture, and threat analysis.

5.3.3.2. Update or refine systems security concepts.

5.3.3.3. Finalize product security requirements and include in the RFP for this phase.

5.3.3.4. Include system security design characteristics in product configuration and document in the product specifications.

5.3.3.5. Performing or Updating Key Program Protection Tasks. If not previously accomplished, or if the program is undergoing modification or other changes in design, implementation, or operation, PMs should reference Attachment 10 for specific program protection tasks that should be performed in the Production and Deployment phase.

5.3.4. Operations & Support Phase. In the event of modifications the PM should ensure security design elements are maintained and determine if the modifications require additional design and/or countermeasures. The PPP should, as warranted, be updated to reflect modifications. The PM should manage ACAT-designated system modifications as acquisition efforts with milestones IAW AFI 63-131.

5.3.4.1. Secure system design documentation, plans, and analyses for sustainment are updated for system modifications or upgrades and changes in threat.

5.3.4.2. If the CPI or critical components no longer need protection, document the rationale for this in an updated PPP. Otherwise protect the system from losing its military advantages and from incorporating malicious or counterfeit content until system demilitarization.

5.3.4.3. Incorporate processes for the continual monitoring on the effectiveness of implemented security controls and safeguards to ensure the desired level of protection is being provided.

5.3.4.4. Performing or Updating Key Program Protection Tasks. If not previously accomplished, or if the program is undergoing modification or other changes in design, implementation, or operation, PMs should reference Attachment 10 for specific program protection tasks that should be performed in the Operations and Support phase.

5.3.4.5. PM must manage supply chain risk during the operational phase by supporting the incident reporting processes.

5.3.5. Demilitarization. Ensure the security measures outlined in the Demilitarization and Disposal Plan are followed as well as any other required safeguards for restricted technology (e.g. ITAR, export controlled) designated either to be placed in storage or for disposal. PM should ensure PPP is provided to Aerospace Maintenance and Regeneration Group or Defense Reutilization and Marketing Office as applicable. (Reference DoD 4160.21-M, *Defense Materiel Disposition Manual*).

5.3.6. Testing Across Acquisition Life Cycle Phases. System security requirements and countermeasures should be integrated into the program's T&E activities. Systems and facilities should be formally tested, evaluated, and certified as to the effectiveness of the system's information and physical security. Security system training plans should be prepared and implemented. Operational system security engineering support activities should be initiated. The following should be considered during the testing phase:

5.3.6.1. Information Assurance (IA) Test, Certification, and Accreditation Processes. Systems and facilities should be formally tested, evaluated, and certified as to the effectiveness of the system's information and physical security. The PM should develop an IA strategy and IA test plans that are fully integrated into the other T&E activities of the program. System security requirements, assessment methods (i.e., analysis, inspection, demonstration, test, and evaluation), and deficiency reporting must be described in the Test and Evaluation Master Plan (TEMP). The accreditation process should use a common risk management methodology. Reference AFI 99-103, *Capabilities-Based Test and Evaluation* and AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP).*

5.3.6.2. Electronic security/emission control (EMSEC, including TEMPEST). Especially during testing, the PM must ensure the selective and controlled use of any distinct electromagnetic or acoustic emissions to deny unauthorized persons information of value. WARM must not be used if it is incorporated into the system.

5.3.6.3. Test results from Developmental Test and Evaluation (DT&E), Operational Test and Evaluation (OT&E), and IA testing should be reviewed to ascertain whether desired system security requirements have been achieved.

5.3.6.4. Clear guidance via the PPP will initiate protection efforts throughout T&E. The PM must coordinate DT&E, OT&E, live-fire (LFT&E), family-of-systems interoperability, information assurance, and modeling and simulation (M&S) testing with the user and the appropriate T&E community to ensure CPI and critical components are protected and remain uncompromised during testing. See Chapter 7 of DoD 5200.1-M.

5.4. Threats and Vulnerabilities. PMs should assess their program(s) for security threats and vulnerabilities to the program's CPI and critical components as early as possible (before Milestone A) and throughout the life cycle of the program to reduce the likelihood of damage,

compromise, or destruction to the system (Steps 3 and 4 of the PPP procedures in Chapter 4). Specifically, PMs should:

5.4.1. Identify CPI and critical components and map their threats and vulnerabilities. Tailor individual security disciplines to program development efforts as cost-effectively as possible.

5.4.2. Map threats that can be neutralized or minimized through system design and countermeasures.

5.4.3. Identify necessary actions to minimize or contain system or component vulnerabilities.

5.4.4. Prioritize based upon the consequences if CPI or critical components are lost or compromised. Factors to consider include the impact on combat effectiveness, combat-effective lifetime, and the costs associated with any modifications required to compensate for loss.

5.4.5. Optimize life cycle security costs, while improving overall survivability of the system or component.

5.5. Protection Requirements. PMs must respond to protection requirements generated in an evolving threat environment throughout the life cycle of the system. The operational and support MAJCOMs, field operating agencies, and supporting security disciplines can provide guidance and assistance as follows:

5.5.1. Preparing Systems Security Concepts (SSC) and Protection Level designations.

5.5.2. Including security requirements in the Initial Capabilities Document (ICD), the Capabilities Development Document (CDD), the Capabilities Production Document (CPD), as well as in the AF Form 1067 (*Modification Proposal),* Problem Statements, and other requirements documentation.

5.5.3. Coordinating command or agency security requirements for systems scheduled to undergo depot maintenance.

5.5.4. Establishing program protection support to ensure security for systems undergoing maintenance or modification.

5.5.5. Developing security countermeasures based on threat analyses.

5.5.6. Coordinating with other MAJCOMs and agencies to ensure adequate, continual security arrangements exist.

5.5.7. Assessing the security impact of change proposals, deviations, and waivers through the system life cycle.

5.5.8. Assisting in security planning.

CHARLES R. DAVIS, LtGen, USAF
Military Deputy, Office of Assistant Secretary
of the Air Force (Acquisition)

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 10-9, *Lead Command Designation and Responsibilities for Weapon Systems*, 8 Mar 2007

AFPD 16-7, *Special Access Programs*, 29 Dec 2010

AFPD 63-1/20-1, *Integrated Life Cycle Management*, 03 Jul 2012

AFPD 71-1, *Criminal Investigations and Counterintelligence*, 6 Jan 2010

AFI 10-701, *Operations Security (OPSEC),* 8 Jun 2011

AFI 14-111, *Intelligence Support to the Acquisition Life-Cycle*, 18 May 2012

AFI 14-201, *Intelligence Production and Applications*, 1 Dec 2002

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*, 01 Dec 2004

AFI 16-701, *Special Access Programs*, 01 Nov 1995

AFI 31-101, *Integrated Defense,* 8 Oct 2009

AFI 31-401, *Information Security Program Management*, 1 Nov 2005

AFI31-501, *Personnel Security Program Management,* 29 Nov 2012

AFI 31-601, *Industrial Security Program*, 29 Jun 2005

AFI 33-200, *Information Assurance (IA) Management*, 23 Dec 2008

AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*, 23 Dec 2008

AFI 51-1101, *The Air Force Procurement Fraud Remedies Program,* 21 Oct 2003

AFI 61-204, *Disseminating Scientific and Technical Information*, 30 Aug 2002

AFI 63-101/20-101, *Integrated Life Cycle Management,* 7 Mar 2013

AFI 63-103, *Joint Air Force-National Nuclear Security Administration (AF-NNSA) Nuclear Weapons Life Cycle Management,* 24 Sep 2008

AFI 63-114, *Quick Reaction Capability Process*, 4 Jan 2011

AFI 63-131, *Modification Management*, 19 March 2013

AFI 71-101v4, *Counterintelligence*, 8 Nov 2011

AFI 91-202, *The Air Force Mishap Prevention Program*, 05 Aug 2011

AFI 99-103, *Capabilities-Based Test and Evaluation*, 28 Feb 2008

AFMAN 23-110, *USAF Supply Manual*, 1 Apr 2009

AFMAN 33-363, *Management of Records*, 1 Mar 2008

CJCSI 3170.01H, *Joint Capabilities Integration and Development System*, 10 Jan 2012

Defense Acquisition Guidebook

DOD Anti-Tamper (AT) Guidelines Version 2.0, 1 Apr 2010 (Secret)

DoD 4160.21-M, *Defense Materiel Disposition Manual*, 18 Aug 1997

DoD 5200.1-M, *Acquisition Systems Protection Program*, 16 Mar 1994

DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, 28 Feb 2006

DoD 5400.7-R_AFMAN 33-302, *Freedom Of Information Act Program*, 21 Oct 2010

DoDD 5000.01, *The Defense Acquisition System*, 12 May 2003

DoDD 5205.07, *Special Access Program (SAP) Policy*, 1 Jul 2010

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, 16 Jun 1992

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, 18 Aug 1995

DoDD O-5240.02, *Counterintelligence*, 30 Dec 2010

DoDD 5530.3, *International Agreements*, 11 Jun 1987

DoDD 8500.01E, *Information Assurance (IA)*, 24 Oct 2002

DoDI 2040.02, *International Transfers of Technology, Articles, and Services*, 10 Jul 2008

DoDI 3020.46, *The Militarily Critical Technologies List (MCTL)*, 24 Oct 2008

DoDI 4140.01, *DoD Supply Chain Materiel Management Policy*, 14 Dec 2011

DoDI 5000.02, *Operation of the Defense Acquisition System*, 8 Dec 2008

DoDI 5030.55, *DOD procedures for Joint DOD-DOE Nuclear Weapon Life-Cycle Activities*, 25 Jan 2001

DoDI 5200.01, *DOD Information Security Program and Protection of Sensitive Compartmented Information*, 13 Jun 2011

DoDI 5200.39, *Critical Program Information (CPI) Protection within the Department of Defense*, 28 Dec 2010

DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, 5 Nov 2012

DoDI 5205.11, *Management, Administration and Oversight of DoD Special Access Programs (SAPs)*, 6 Feb 2013

DoDI 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA)*

Activities, 29 Jan 2010

DoDI 5220.22, *National Industrial Security Program (NISP)*, 18 Mar 2011

DoDI 5230.24, *Distribution Statements on Technical Documents*, 23 Aug 2012

DoDI 5240.04, *Counterintelligence (CI) Investigations*, 2 Feb 2009

DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*, 8 Jun 2011

DoDI 8320.04, *Item Unique Identification (IUID) Standards for Tangible Personal Property*, 16 Jun 2008

DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 Feb 2003

DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, 9 July 2004

DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems*, 6 June 2012

DoDM 5200.01, *DoD Information Security Program*, 24 Feb 2012

DSCA 5105.38-M, *Security Assistance Management Manual (SAMM)*, 30 Apr 2012

DTM 09-019, *Policy Guidance for Foreign Ownership, Control, or Influence (FOCI)*, 1 Dec 2011

Executive Order 13526, *Classified National Security Information*, 29 Dec 2009

Federal Acquisition Regulation (FAR)

MIL-STD-881C, *Work Breakdown Structures for Defense Materiel Items*, 3 Oct 2011

MIL HDBK-1785, *Systems Security Engineering Program Management Requirements*, 1 Aug 1995

MIL-STD-3018, *Parts Management*, 27 Oct 2011

NSTISSP No. 11, *National Information Assurance Acquisition Policy*, Jul 2003

Risk Management Guide for DoD Acquisition, 6th Edition, Aug 2006

SAE Aerospace Standard (AS) 5553, *Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*, April 2009

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, 22 Sep 2009

AF Form 1067, *Modification Proposal*, 1 Nov 1999

Abbreviations and Acronyms

ACAT—Acquisition Category

ADM—Acquisition Decision Memorandum

AF—(U.S.) Air Force

AF—NNSA— Air Force –National Nuclear Security Administration

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFOSI—Air Force Office of Special Investigations

AFPAM—Air Force Pamphlet

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFRL—Air Force Research Laboratory

AFSPC—Air Force Space Command

AIS—Automated Information System

ANG—Air National Guard

AoA—Analysis of Alternatives

ASDB—Acquisition Security Database

ASR—Alternate System Review

AT—Anti-Tamper

AT&L—Acquisition, Technology and Logistics

C&A—Certification & Accreditation

CD—Capabilities Directorate

CDD—Capabilities Development Document

CDR—Critical Design Review

CFIUS—Committee on Foreign Investment in the United States

CI—Counterintelligence

CIO—Chief Information Officer

CISP—Counterintelligence Support Plan

CITA—Counterintelligence Threat Assessment

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

COA—Course of Action

COMSEC—Communications Security

COTS—Commercial Off The Shelf

CPD—Capability Production Document

CPI—Critical Program Information

CTE—Critical Technology Elements

CTTA—Certified Tempest Technical Authority

CUI—Controlled Unclassified Information

DAE—Defense Acquisition Executive

DAG—Defense Acquisition Guide

DDL—Delegation of Disclosure Letter

DIA—Defense Intelligence Agency

DIACAP—Department of Defense Information Assurance Certification and Accreditation Process

DIB—Defense Industrial Base

DID—Data Item Description

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DOE—Department of Energy

DRU—Direct Report Unit

DSCA—Defense Security Cooperation Agency

DSS—Defense Security Service

DT&E—Developmental Test and Evaluation

FAR—Federal Acquisition Regulation

FMS—Foreign Military Sales

FOCI—Foreign Ownership, Control and Influence

FOIA—Freedom of Information Act

FOUO—For Official Use Only

HAF—Headquarters Air Force

HUMINT—Human Intelligence

IAW—In Accordance With

ICD—Initial Capabilities Document

ICT—Information and Communications Technology

IDEA—Independent Distributors of Electronics Association

ILCM—Integrated Life Cycle Management

IT—Information Technology

JCIDS—Joint Capabilities Integration and Development System

MAC—Mission Assurance Category

MAJCOM—Major Command

MDA—Milestone Decision Authority

MS—Milestone

NASIC—National Air and Space Intelligence Center

NETCENTS—2—Network-Centric Solutions-2

NID—National Interest Determination

NISP—National Industrial Security Program

NISPOM—National Industrial Security Program Operating Manual

NNSA—National Nuclear Security Administration

NSA—National Security Agency

NSS—National Security Systems

NSTCA—Nuclear Security Threat Capabilities Assessment

OPR—Office of Primary Responsibility

OPSEC—Operations Security

O&S—Operation and Sustainment

OSD—Office of the Secretary of Defense

OT&E—Operational Test and Evaluation

PDR—Preliminary Design Review

PEO—Program Executive Officer

PIT—Platform Information Technology

PITI—Platform Information Technology Interconnections

PM—Program Manager

PPIP—Program Protection Implementation Plan

PPP—Program Protection Plan

PPS—Program Protection Survey

PSI—Program Security Instruction

PSM—Product Support Manager

PSR—Program Support Review

RATT—Risk Assessment of Technology Transfers

R&D—Research and Development

RDA—Research, Development, and Acquisition

RDT&E—Research, Development, Test, and Evaluation

RFI—Request for Information

RFP—Request for Proposal

SAE—Service Acquisition Executive

SAE—Society of Automotive Engineers

SAF—Secretary of the Air Force

SAF/CIO A6—Chief of Warfighting Integration and Chief Information Officer (CIO)

SAF/AQ—Assistant Secretary of the Air Force (Acquisition)

SAF/AQL—Special Programs

SAF/AQX—Deputy Assistant Secretary for Acquisition Integration

SAF/IA—Deputy Under Secretary of the Air Force for International Affairs

SAF/IG—Inspector General of the Air Force

SAF/IGX—Directorate of Special Investigations

SAP—Special Access Program

SCG—Security Classification Guide

SCI—Sensitive Compartmented Information

SCRM—Supply Chain Risk Management

SE—Systems Engineering

SEP—Systems Engineering Plan

SETR—System Engineering Technical Review

SFR—System Functional Review

SIAO—Senior Information Assurance Officer

SIPRNET—Secret Internet Protocol Router Network

SOO—Statement of Objectives

SRR—System Requirements Review

SSC—System Security Concept

SSE—Systems Security Engineering

SSO—Special Security Office

STA—System Threat Assessment

STAR—System Threat Assessment Report

TAC—Threat Analysis Center

TA/CP—Technology Assessment/Control Plan

T&E—Test & Evaluation

TEMP—Test and Evaluation Master Plan

TPWG—Technology Protection Working Group

TSN—Trusted Systems and Networks

TTRA—Technology Targeting Risk Assessments

USAF—United States Air Force

USD—Under Secretary of Defense

USD (AT&L)—Under Secretary of Defense (Acquisition, Technology and Logistics)

USD (I)—Under Secretary of Defense for Intelligence

WARM—Wartime Reserve Mode

WBS—Work Breakdown Structure

Terms

Agility—Nimbleness and adaptability; enabled by dynamic, reconfigurable architectures such as internet protocol hopping at the network layer.

Anti-Tamper (AT)—Anti-Tamper is defined as the systems engineering activities intended to prevent and/or delay exploitation of Resident CPI in U.S. weapon systems.

Center Intelligence Office—The singular focal point at each center specifically dedicated to supporting research, development, test, evaluation, and sustainment activities with analytical services and intelligence products and information.

Compromise—The unauthorized access to or inadvertent disclosure, destruction, transfer, alteration, or loss of CPI or critical components. The release of classified CPI to a person who does not have a need to know or does not meet the requirements for access to classified (i.e. a valid security clearance). A compromise must be assumed when CPI or critical components is found not protected as stated in the PPP or when the network on which CPI or critical components is connected to was compromised. Further, a compromise must be assumed when CPI or critical components is found with any piece-part or code missing, is suspected of having malicious code inserted, is altered in any way, or shows signs of tamper.

Counterfeit Materiel—Materiel whose identity or characteristics were deliberately misrepresented, falsified, or illegally altered.

Counterintelligence Support Plan (CISP)—The CISP is a formally coordinated action plan for CI support to protect research and technology at specific DoD research, development, test, and evaluation facilities and acquisition programs. The plan addresses key aspects of the installation, the activity or program, and the nature of the CI activities to be employed. A separate plan may be prepared for each DoD contractor or academic institution where CPI is involved.

Critical Asset Risk Management—The identification, assessment, protection, and real-time monitoring of cyber and physical mission critical infrastructures essential to the execution of the National Military Strategy.

Critical Component—A component which is or contains ICT including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of a system.

Critical Program Information (CPI)—(Per DoDI 5200.39). Elements or components of a program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage;

significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. CPI includes:

Information about applications, capabilities, processes, and end—items;

1. Components critical to a military system or network mission effectiveness; and
2. Technology that would reduce the US technological advantage if under foreign control.

Criticality Analysis—An end-to-end functional decomposition performed by Systems Engineers to identify mission critical functions and components. It includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions(s).

Horizontal Protection—Common security countermeasures for protecting similar technologies used by more than one program or technology project. It may extend across military components. Horizontal protection ensures cost-effective application of technology protection efforts.

Information and Communications Technology (ICT)— Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). ICT is not limited to, information technology (IT) as defined in section 11101 of title 40, U.S.C. (Reference (n)). Rather, this term reflects the convergence of IT and communications.

Information Technology—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources, including National Security Systems (NSS). It does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

Inherited CPI—CPI from other acquisition programs, subsystems, or projects that are being incorporated or implemented into another program.

Loss—A loss of CPI or critical components has occurred when it cannot be accounted for or physically located.

Mission Assurance—An integrated engineering-level assessment of analysis, production, verification, validation, operation, maintenance, and problem resolution processes performed over the life cycle of a program by which an operator/user determines that there is an acceptable level of risk to employment of a system or end item to deliver an intended capability in an intended environment. The objective of the assurance process is to identify and mitigate design, production, and test deficiencies that could impact mission success.

Mission Critical Function—Any function of which the compromise would degrade the system effectiveness in achieving the core mission for which it was designed.

Organic CPI— CPI initiated with the program, subsystem, or project.

Platform IT (PIT)—A special purpose system which employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or essential in real time to the mission performance. It only performs (i.e., is dedicated to) the information processing assigned to it by its hosting special purpose system (this is not for core services). Examples include, but are not limited to: SCADA type systems, weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems, such as water and electric.A critical component could be a subset of PIT components.

Program Protection Plan (PPP)—The principal document that identifies a system's critical program elements (CPI and critical components), threats, and vulnerabilities throughout the system's life cycle. Program Protection is a comprehensive effort that encompasses all security, technology transfer, intelligence, and counterintelligence processes through the integration of embedded system security processes, security manpower, equipment, and facilities.

Resident CPI—(Previously known Critical Technologies) CPI resident in the weapon system, including training and maintenance systems.

Resilience—The ability to avoid, survive, and recover from disruption. Disruption can be either a sudden or a sustained event and may be natural or manmade (e.g., internal failure or external attack). Resilience can be enabled by redundancy, diversity, and distributed functionality which allow systems to repel, absorb, and/or recover from attacks. Resilience can be enhanced through hardening, reduction of attack surfaces, critical mission segregation, and attack containment. System survivability can be enhanced by autonomous compromise detection and repair (self healing) and adaptation to and evolution from changing environments and threats.

Risk—A measure of future uncertainties in achieving program performance goals within defined cost and schedule constraints. It has three components: a future root cause, a likelihood assessed at the present time of that future root cause occurring, and the consequence of that future occurrence.

Software Assurance—The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.

Supply Chain Risk—The risk that 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.

Supply Chain Risk Management (SCRM)—A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing of mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

Suspect Counterfeit Materiel—Materiel, items, or products in which there is an indication by visual inspection, testing, or other information that it may meet the definition of counterfeit materiel provided herein.

Systems Security Engineering (SSE)—An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities.

Theft—The unauthorized access of CPI. Upon indication of theft of CPI, whether involving unclassified or classified, contractor proprietary, or Air Force/DoD data, PMs must notify the MDA with either proposed countermeasures and/or mitigation strategies that nullify the advantage(s) gained by the adversary, or indicate a proposed acceptance of the threat risk and the rationale.

Trusted Systems and Networks (TSN)—A DoD strategy and set of concepts to minimize the risk that DoD's warfighting capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's critical functions or critical components by foreign intelligence, terrorists, or other hostile elements.

Vulnerability—The characteristics of a system that causes it to suffer a definite degradation (loss or reduction of capability to perform its designated mission) as a result of having been subjected to a certain (defined) level of effects in an unnatural (man-made) hostile environment. Vulnerability is considered a subset of survivability. Vulnerability in an information system is a weakness in system security procedures, internal controls, or implementation that could be exploited.

Attachment 2

IDENTIFY STAKEHOLDERS AND CONDUCT INITIAL ANALYSIS

A2.1. Organization. The PM may assemble a team to support the program's protection planning. The PM's team of stakeholders and functional experts supports the security, intelligence, and counterintelligence needs of the technology or acquisition program for the life of the program.

A2.1.1. The size and nature of the project, program, or system will dictate the size and makeup of the protection team.

A2.1.2. The following functional areas may be included in protection planning:

A2.1.2.1. Program Management.

A2.1.2.2. Engineering (Chief or Senior Engineer).

A2.1.2.3. Scientific Support (Chief or Senior Scientist).

A2.1.2.4. Lead Command User Representative.

A2.1.2.5. Anti-Tamper.

A2.1.2.6. Information Protection/Security.

A2.1.2.7. Industrial Security IAW AFI 31-601 *Industrial Security Program Management.*

A2.1.2.8. Personnel Security.

A2.1.2.9. Physical Security.

A2.1.2.10. Operations Security.

A2.1.2.11. Communications Security.

A2.1.2.12. Foreign Disclosure.

A2.1.2.13. Program Protection/Acquisition Security.

A2.1.2.14. Logistics.

A2.1.2.15. Counterintelligence.

A2.1.2.16. Intelligence.

A2.1.2.17. Scientific and Technical Information Office.

A2.1.2.18. Special Security Office.

A2.1.2.19. Information Assurance.

A2.1.2.20. Contracting.

A2.1.2.21. Financial Management.

A2.1.2.22. Test Management.

A2.1.2.23. Other functional experts, as required.

A2.1.3. The PM identifies the need for a team charter appropriate to the program's security needs. A program protection team charter may include the program mission, the team's overall objective, and the roles and responsibilities of each represented area. It should be signed by the PM.

A2.2. Initial Activities. Initial protection planning tasks may involve the following activities:

A2.2.1. Review the modernization planning or Joint Capabilities Integration and Development System (JCIDS) requirements documents. Review each requirements document outlining the program protection requirements for the completion of each section of the program protection plan.A2.2.1.1 Conduct a program CPI study to determine if CPI are in the program. Functionally decompose system and technologies identified as CPI and critical components.

A2.2.1.1. Conduct a program critical components study.

A2.2.1.2. Assess the criticality levels of R-CPI, develop an AT Concept and develop a cost estimate to support the AT Concept.

A2.2.2. Assist in the preparation of the following documents and material:

A2.2.2.1. Program Protection Plan.

A2.2.2.2. Security Classification Guide(s).

A2.2.2.3. OPSEC Plan.

A2.2.3. Review each system security engineering, security, intelligence, and counterintelligence process (i.e., system security engineering, anti-tamper, computer security, communications security, operations security, information security, information protection, industrial security, personnel security, physical security, antiterrorism, force protection, international program, and other security requirements identified by the using command).

A2.2.4. Identify the functional experts needed by the PM to have viable program protection.

A2.2.5. Integrate protection and security requirements into program documentation.

A2.2.6. Determine if CPI and critical components are controlled unclassified information or classified.

A2.2.7. Request counterintelligence threat assessments for all CPI and critical components requiring supply chain assessments using the appropriate AFOSI (for CPI) and AFMC or AFSPC MAJCOM TSN Focal Point (for critical components) request for information (RFI) formats. All Critical Component RFIs must be routed through the MAJCOM TSN Focal Point for submission to DIA's SCRM TAC.

A2.2.8. Review threat data provided and determine the risk to the identified CPI and critical components.

A2.2.9. Employ the PM's approved CPI and critical components risk management approach.

A2.2.10. Determine if protective measures need to be designed into the system and if anti-tamper features need to be developed for each Resident CPI. Whichever protective countermeasure is used, it should be verified that it functions as designed to protect the system.

A2.2.11. Document protection countermeasures once CPI or critical components are identified and approved by the PM.

A2.2.12. Determine if other programs have like technologies or components and if protection measures are equivalent.

A2.2.13. Coordinate with other program offices or service organizations to resolve any protection discrepancies to achieve horizontal protection.

A2.2.14. Elevate horizontal protection issues through the proper acquisition chain of command if a protection conflict exists and no resolution is obtained at the working level.

A2.2.15. Develop critical information lists and inform project personnel of correct handling procedures.

A2.2.16. Establish an OPSEC program to prevent an adversary from compromising the program's CPI or critical components.

A2.2.17. Regularly update the PPP and notify personnel of changes.

A2.2.18. Identify security issues that require clarification from the using command or other organizations.

A2.2.19. Continually monitor threats to the system and determine if system security "design-ins" need to be added to the system's architecture.

A2.2.19.1. Propose additional security requirements to the using command.

A2.2.19.2. Tailor requirements to the individual contractor facility.

A2.2.19.3. Prevent duplicate or excessive security requirements and costs.

A2.2.19.4. Work with the program office and the contracting office to specify which requirements to include in solicitations and contracts.

A2.2.19.5. Evaluate plans received from bidders in response to solicitations.

A2.2.19.6. Conduct surveys of contractor's compliance.

A2.2.19.7. Review contractors' responses to problems identified in surveys.

A2.2.19.8. Recommend corrective actions to the contract administration office when a survey reveals a security problem.

A2.2.19.9. Provide general security assistance to program offices as necessary.

Attachment 3

THREAT ANALYSIS METHODOLOGY AND PROCEDURES

A3.1. Threat analysis and vulnerability analysis may be accomplished concurrently. These analyses establish the PM's risk assessments and resulting priorities.

A3.2. Developing a comprehensive threat picture involves evaluating all threats both natural and manmade. Adversary threats should be evaluated across the spectrum of potential adversary types (i.e. international terrorists, domestic terrorists, foreign intelligence, criminals, insider threat). As the system or project develops and moves toward operational status, evaluation should include proposed operating locations.

A3.3. Evaluating the full spectrum of hostile adversarial threats begins with collecting threat assessments from multiple disciplines. These assessments should include an analysis of the threat likelihood with the initial report when possible. Foreign collection and the adversary's technical capability should be addressed, preferably at the national level when applicable. For example, indicators of a high-likelihood threat by a foreign interest would include:

A3.3.1. A foreign interest with a confirmed or assessed requirement for acquiring program information.

A3.3.2. A foreign interest with the capability to acquire such information.

A3.3.3. Indications of probable sources and methods that might be employed to satisfy a collection requirement based on confirmed or assessed identification of foreign collection requirements.

A3.4. Examples of threat assessments include:

A3.4.1. Non-nuclear postulated threat.

A3.4.2. Nuclear Security Threat Capabilities Assessment (NSTCA).

A3.4.3. Intelligence threat assessment through the servicing intelligence organization.

A3.4.4. Counterintelligence Threat Assessment (CITA) through AFOSI.

A3.4.5. DIA SCRM Threat Analysis Center (TAC) Reports.

A3.4.6. System Threat Assessment Report (STAR).

A3.4.7. System Threat Assessment (STA).

A3.4.8. Applicable Capestone Threat Assessment.

A3.5. Threats may also include natural occurrences like weather, earthquakes, and fire.

A3.6. The potential threats identified are mapped to the CPI and critical components to include the likelihood of the threat occurring. The mapping process involves linking the CPI and critical components to potential threats and tactics that may be employed. Vulnerability to the threats is assessed separately. As an example of likelihood, evaluate if the group posing a threat has or is projected to have the capability to affect the CPI and critical components.

A3.7. After mapping the CPI and critical components, some gaps in threat information may become evident, requiring additional or more detailed threat assessments.

A3.8. Threats are not static and require routine revalidation and/or updates to threat assessments. Potential changes in the operational threat should be reviewed as they occur using the PPP process.

A3.9. Resources for Threat Analysis. AFOSI and DIA's SCRM TAC can provide the program with threat analyses. See DoDI O-5240.24 for CI support to the protection of CPI and critical components.

A3.10. AFOSI provides CI support to defense technology and acquisition programs and personnel. Through these efforts, the CI specialist works closely with the PM to monitor and track supported CPI and critical components and technologies identified by the PM during the life cycle process.

A3.11. PMs should request counterintelligence threat assessments from their servicing TSN Focal Point or CI specialist.

A3.12. Intelligence assessments are requested via the Community On-Line Intelligence System for End Users and Managers (COLISEUM).

A3.13. Use the list of questions provided in Table A3.1 as a guide to prepare the threat assessment request.

Table A3.1. Requesting a Threat Assessment.

QUESTION	RESPONSE
1. Name of Program/Project/Product.	
2. Program/Project/Product Manager, Organization, Location, and Telephone Numbers.	
3. Security Manager Address and Telephone Numbers.	
4. Contract Numbers/Prime Contractor/Location/Mailing Address/Security Manager/Telephone Number.	
5. Major Subcontractors/Address/Subcontract Numbers/Security Managers/Telephone Numbers.	
6. Against what will the system be targeted? Focus on exploitation and reverse engineering in discussing the threat.	
7. What are the program's critical technologies, components, and information (CPI)?	
8. What specific technologies do you need to protect? Which contractor(s) is involved?	
9. What specific information or core technologies are classified? Is special access program technology involved?	
10. Where are the technologies located (e.g., aboard aircraft, within buildings, mounted in vehicles, man-packed)?	
11. If the material is a weapons system, what specific component or components require protection (e.g., sights, range finder, target acquisition system, is the system or technology touch or sight sensitive)?	

12. If you are protecting a computer system, what specific component(s) of the system requires protection (e.g., software, hardware)? a. Is the system stand-alone or networked? b. Can you access the system from other systems at other facilities or bases? c. Are links between systems encrypted? d. How are the systems linked (e.g., dedicated land lines, microwave)?	
13. If an aircraft is involved, what specific component of the aircraft requires protection (e.g., which specific computer chip from which specific card from which specific black box)? a. Can you remove the components from the aircraft? b. Can you see the components from outside the aircraft?	
14. If vehicles are involved, are the vehicles dedicated to this system or activity? a. Are these vehicles unique to this system or activity? b. Can you see the system components from outside the vehicle? c. Can you remove the components of the system from the vehicle?	
15. What are the identifiable, exploitable characteristics of the technology? a. Are there unique physical characteristics involved? b. Can you see the characteristics of the system from outside it? c. Does the system have an electronic signal emission? d. What is the system's operating frequency range? e. Is the system active or passive? f. What is the system’s power output? g. What is the system's range?	
16. Are there specific communications associated with this system? a. Where are these systems employed? (Indicate the location of bases or facilities.) b. How will you use the system?	
17. With what facilities is the system associated? a. Are the facilities unique to the system? b. Can you see the facilities from the outside? c. Where are the facilities located (e.g., military base, civilian community, industrial complex, public building)? d. What access controls exist for the building?	
18. What aspects of the training must you protect? (Indicate particular activities, participants, location, association with system)	
19. Where will you do the system testing? (Indicate any previous test dates, locations, as well as future test dates and locations.)	

20. Is the system site sensitive (that is, are you worried about the site being seen)? If yes, why?	
21. What types of emissions do systems tests or test sensors generate?	
22. Has or will any testing be done against actual or simulated foreign equipment? If yes, identify the foreign equipment, test locations, and dates.	
23. Do any plans exist, or have there been inquiries about, foreign involvement (e.g., foreign sales, foreign cooperative development, co-production, joint ventures)? If yes, with whom are negotiations taking place and what is the current status?	
24. What are the major milestone dates for this program?	
(**NOTE:** If classified, this form must contain all appropriate classification markings.)	

Attachment 4

VULNERABILITY ANALYSIS

A4.1. Threat analysis and vulnerability analysis may be accomplished concurrently. These analyses are utilized to establish the PM's risk assessments and resulting priorities. Vulnerabilities are potentially exploitable areas or situations that can be used by an adversary to degrade, destroy, or collect information about CPI and critical components. Vulnerabilities may occur in many forms including physical, technological, or procedural.

A4.2. Identifying the vulnerabilities of designated CPI and critical components includes evaluating the weakness, potential consequences if exploited, and existing countermeasures.

A4.3. For each CPI or critical component, the PM should put the vulnerabilities in a priority sequence order from highest (most severe consequences if exploited) to lowest. For critical components, the criticality analysis process described in Chapter 4 establishes this priority order.

A4.4. Resources for risk analysis. AFI 31-101, *Integrated Defense*, provides a useful discussion of risk assessment methodology. The Defense Acquisition Guide (DAG) chapter on program protection (Chapter 13) provides guidance and approaches to identifying vulnerabilities. DoD 5205.02-M, *DoD OPSEC Manual*, provides detailed guidance on risk assessment methodology for critical information. A4.5. Some additional factors to be considered are:

A4.4.1. How the CPI and critical components are stored, maintained, or transmitted (e.g., electronic media, blueprints, training materials, facsimile, or modem).

A4.4.2. How the CPI and critical components are used (e.g., bench testing or field testing).

A4.4.3. What emanations, exploitable signals, or signatures are generated by or reveal the CPI/ critical components (e.g., telemetry, acoustic, or radiant energy).

A4.4.4. Where the CPI and critical components are physically located during development (e.g., program office, test site, contractor, or vendor) and fielding (e.g. engine bay, or cockpit).

A4.4.5. What types of OPSEC indicators or observables are generated by program or system functions, actions, and operations involving CPI or critical components.

Attachment 5

RISK MANAGEMENT AND COUNTERMEASURE SELECTION METHODOLOGY

A5.1. Risk management of CPI and critical components should be performed in a manner consistent with accepted risk management practices as detailed in the Risk Management Guide for DoD Acquisition, 6th Edition, Aug 2006. The PM should use the 5x5 risk matrix to weigh the likelihood and consequence of each risk in determining the appropriate risk mitigation approach. The PM should consider the entire national investment, including the future investment needed to address compromised CPI or critical components. At Milestone B or PDR (whichever comes first), the MDA approves the PM's baseline CPI list and associated protections.

A5.2. Once the risk management plan has been developed, the PM documents risk management intent in the PPP, identifying the risk acceptance levels and the mitigation plan.

A5.3. Countermeasures are applied to mitigate or eliminate the projected vulnerabilities negating an adversary's ability to exploit vulnerability. Comprehensive Courses of Action (CCAs) with countermeasures are developed for each CPI or critical component showing a baseline of where protection is today (current countermeasures) and projected effectiveness with additional countermeasures. Countermeasures can vary from technical (e.g. design or implementation) to procedural (e.g. T&E of CPI and critical components elements, additional physical security) to procurement (e.g. "blind buys"). Cost should be presented in relation to effectiveness and should be time or event phased.

A5.4. COAs selected may include an incremental implementation beginning with no cost or low cost (i.e. procedural) and moving toward the final COA implementation to meet the acceptable risk as funding is established or the project matures to a point where implementation is possible. The COA selected (with countermeasures) is documented in the PPP.

A5.5. The PPP Outline and Guidance establishes specific questions and criteria that should be addressed for general countermeasures and for specific areas of interest including Anti-Tamper, Information Assurance, Software Assurance, Supply Chain Risk Management, and System Security Engineering. Some additional questions to consider include:

A5.5.1. Why were these specific countermeasures selected?

A5.5.2. Which specific vulnerabilities do they remedy?

A5.5.3. When and how will they be implemented or increased?

A5.5.4. When and how will they be terminated or reduced?

A5.5.5. How much are they expected to cost?

Attachment 6

MONITORING CPI AND CRITICAL COMPONENTS PROTECTION

A6.1. General. The implementation and monitoring of countermeasures must be addressed in the PPP for each individual CPI or critical components. If countermeasures are determined to be inadequate in satisfying the Program Manager risk tolerance level, then the PPP process should be revised to address those situations or inadequacies. To ensure countermeasure effectiveness PMs should implement a training program detailing the efforts, procedures, and methods used to protect CPI and critical components.

A6.2. Program Protection Survey (PPS). IAW DoD 5200.1-M, the PPS provides the PM with information about the effectiveness of the security applied to the program. At least one PPS should be conducted on ACAT I and ACAT II acquisition programs containing CPI or critical components during each phase of the acquisition cycle. Use the list of facilities handling CPI and critical components and the PPP to plan and conduct a PPS. The PPS should be the PM's primary tool to evaluate and validate the PPP with the objective to:

A6.2.1. Assess the overall effectiveness of the PPP during a given phase.

A6.2.2. Provide specific indicators of possible losses of CPI and critical components.

A6.2.3. Provide specific information on how the loss of CPI and critical components could occur.

A6.2.4. Provide information to update the PPP for the remaining phases.

A6.2.4.1. Identify potential critical infrastructure vulnerabilities to determine how to mitigate them.

A6.3. PPS Purpose. The PPS is used to assess the effectiveness of the established program protection following PPP approval and implementation. Based on the results of the survey, the PM may continue the PPP as written, or refocus resources to eliminate any security shortfalls.

A6.3.1. The PM determines if the previously identified CPI and critical components received adequate protection during a given phase. Focus on specific threats and countermeasures.

A6.3.2. The PM should limit the survey to determine the effectiveness of the protection and countermeasures planned and implemented at a specific facility to protect the CPI or critical components of a selected program. The survey methodology is to reproduce an adversary's approach to the program being assessed, not to assess compliance with security procedures.

A6.3.3. A written report should be provided to the PM addressing, as a minimum:

A6.3.3.1. Effectiveness of the mitigations used for the program's CPI and critical components.

A6.3.3.2. Recommendations to improve protection measures to eliminate or reduce vulnerabilities.

A6.3.4. The PPS should not be used as an inspection and should not be graded. To obtain accurate information and be a successful tool, the team conducting the survey depends on positive cooperation and assistance from the program management organization and the facility being surveyed.

A6.3.5. The PPS report should be provided only to the PM. Any further distribution should be done only with PM approval. PMs should retain official file copies of each survey conducted. Along with the PPS report, the PPS team chief should provide lessons learned to the PM discussing specific areas of PPP strengths and weaknesses (including details such as actual locations, personnel names, and other program identifying information which are not included in the report). The PPS report should:

A6.3.5.1. Be correlated to common trends and/or problems in the technology or acquisition community.

A6.3.5.2. Concentrate on generic problems with resources, facilities, and/or training.

A6.3.5.3. NOT be conducted at contractor-owned or operated locations unless the provisions of the contract authorize compliance reviews.

A6.3.5.4. Should be coordinated with the servicing government security oversight office.

A6.4. Additional Surveys.

A6.4.1. Security Surveys.

A6.4.1.1. The purpose of initial and follow-on surveys is to evaluate the adequacy of additional security requirements outlined in the contract and PPP. The PPS is the tool used to conduct the surveys. Other inspection results, such as those conducted by DSS or Inspector General, may be utilized during the PPS, but will not replace the PPS.

A6.4.1.2. Security surveys must be cost-effective. Do not conduct surveys where there are other means of evaluating security. Where security requirements are minimal, the PM may authorize the contractor to perform a survey. In these cases, the contractor should provide written certification to the PM of security at the facility.

A6.4.1.3. Pre-award Surveys. Pre-award surveys should be used to:

A6.4.1.3.1. Ensure the contractor can meet the requirements identified in the solicitation.

A6.4.1.3.2. Determine whether the contractor has satisfied the requirements by participating in the Industrial Security Program or some other security program.

A6.4.1.3.3. Evaluate the contractor's security plan(s) and physical security measures.

A6.4.1.3.4. If the survey identifies problems in the contractor's program, recommend contract amendments to the contract administration office.

A6.4.1.4. An initial survey should be conducted not later than 90 days after the contract is awarded or CPI is identified, and at 2-year intervals thereafter. PMs may vary the 2-year survey cycle if additional surveys are not cost-effective, or if there is a need for more frequent surveys.

A6.4.1.5. The contractor and contract administration office should be notified in advance of a proposed survey. However, if security is in question no-notice surveys may be used.

A6.4.1.6. Security surveys should be addressed to the requesting PM with informational copies to the operational command(s). A copy of the most recent survey should be kept in the security office supporting the program.

A6.4.1.7. Security specialists should evaluate corrections that the contractor proposes. If corrective action seems inappropriate, the program office and contracting officer should recommend further action.

A6.4.1.8. The PM should notify the cognizant DSS office of Industrial Security of proposed surveys at cleared contractor facilities which fall under the Industrial Security Program. Where the protection of classified CPI will be a subject of the survey, the cognizant DSS office should be requested to participate as a member of the survey team.

Attachment 7

PROGRAM PROTECTION PLAN (PPP) DOCUMENTATION

A7.1. Overview. PPPs are Integrated Life Cycle Management (ILCM) documents that are reviewed and coordinated by appropriate stakeholders. The PPP id**e**ntifies elements of the program, classified and unclassified, which require protection to prevent unauthorized disclosure or inadvertent transfer of Resident CPI or information. The PPP is a risk-based, living plan that captures the program's CPI, critical components, threats, vulnerabilities, countermeasures, cost, and risk. Development of the PPP begins upon initial identification of CPI or critical components and is updated throughout the life cycle of the program. It is the program's primary document to protect CPI and critical components from unauthorized access, inadvertent disclosure, or compromise. Reference DoDI 5200.39, DoDI 5200.44, and the Defense Acquisition Guide (DAG) Chapter 13 on program protection, which also has a link to the OSD PPP Outline and Guidance.

A7.1.1. PPPs for ACAT Programs. A PPP is required for all ACAT programs regardless of CPI determination. The PPP should be developed in accordance with the OSD format found on the DAG website. The PPP is approved by the MDA. The MDA may tailor the contents of the PPP to meet individual program needs.

A7.1.2. PPPs for Other Applicable Programs. All new and legacy systems must address mission critical functions and components requiring risk management to protect capabilities. This includes AFPD 10-9 legacy systems undergoing any modification IAW AFI 63-131. PMs perform protection planning IAW DoDI 5000.02, AFI 63-101/20-101, and using this pamphlet for guidance. The approval authority may tailor the PPP contents or approval process for all ACAT III programs.

A7.1.2.1. Technology Projects. The PM for a technology project requiring a formal Technology Transition Plan (TTP) must document the results of the CPI identification process and develop a PPP when CPI exists. If the CPI is protected using Anti-Tamper as a protective countermeasure and/or has Anti-Tamper protections, the approved AT plan should also be provided to the Transition Agent as a classified annex to the PPP.

A7.2. PPP Documentation Requirements and Related Functional Considerations. PMs should review other documentation and functions that are integral to the acquisition process. They may need to include or reference them in the PPP. The following should be included as appendices as applicable:

A7.2.1. Anti-Tamper (AT) Plan. Annex to PPP.

A7.2.2. Counter Intelligence Support Plan (CISP). Annex to PPP.

A7.2.3. Acquisition Information Assurance Strategy (IAS). Annex to PPP.

A7.2.4. Security Classification Guide (SCG). Annex to PPP.

A7.2.5. Criticality Analysis (CA). Annex to PPP.

A7.2.6. System Engineering Plan (SEP). The SEP is a top-level management document that describes system engineering program tasks including secure system design. Designing in protection countermeasures is the objective of secure system design during protection

planning efforts. Secure system design protections include anti-tamper and information assurance countermeasures.

A7.2.7. Operations Security (OPSEC) Plan. OPSEC needs to be integrated into all technology, acquisition, and sustainment efforts (including testing). When a program has critical information, the PM must ensure OPSEC countermeasures are applied throughout the life cycle. An OPSEC plan is part of the countermeasures in the PPP. See AFI 10-701.

A7.2.8. System Security Concept (SSC)/System Security Standard (SSS). The operating command may provide enabling and operating concepts for how the system will be secured. This can provide the PM with additional security insights for the protection approach and countermeasure selection. See DoD 5200.1-M, chapter 7 and appendix 1, and AFI 31-101.

A7.2.8.1. The security concept is developed by evaluating projected system threats and vulnerabilities to assess the associated risk. System critical characteristics and sensitivity levels to mission capability should be correlated with the national security information categories, intelligence indicators, trusted computer system evaluation criteria, system operating modes, essential communication nodes, physical security criteria, OPSEC, and emissions security. The security concept evolves as the system matures to include projected security requirements such as protection levels or critical asset risk management and the associated manpower, facilities, and critical infrastructure nodes needed for operation.

A7.2.8.2. The SSC or SSS enables seamless security when transitioning the system to the operational command. In particular, identification of required resources and identification of classified material with Information Security protection requirements should be addressed to ensure resources are available when needed.

A7.2.9. Special Security Agreement (SSA)/National Interest Determination (NID). SSAs and NIDs are related to work performed for the US by companies under Foreign Ownership, Control, or Influence (FOCI). If a PM requires an SSA-cleared company to have access to proscribed information, the PM and contracting officer must complete a NID to confirm that disclosure of such information will not harm national security interests. Proscribed information includes Top Secret, COMSEC materiel, restricted data, SAP and SCI. Access to the proscribed information will not be granted without an approved NID and the approval of the agency with control jurisdiction of the proscribed information. The requirement for NIDs applies equally to new and existing contracts with SSA-cleared companies when acquired by foreign interests. Upon notification from DSS of the pending merger or acquisition of a cleared company by a foreign interest, the program office should review the company's FOCI action plan. If the company is proposing to use an SSA to mitigate FOCI, DSS will advise the program office of the need for a NID, and SAF/AAZ will determine whether a favorable NID will be issued. See DoDI 5220.22, *National Industrial Security Program*, DoD 5220.22-M, *National Industrial Security Program Operating Manual* and AFI 31-601, *Industrial Security Program Management*.

A7.2.10. Technology Assessment Report and Control Plan (TA/CP)/Delegation of Disclosure Authority Letter (DDL). Foreign disclosure is the act of permitting access to classified or controlled unclassified military information by an authorized representative of a foreign government or international organization. It includes Foreign Military Sales (FMS), FMS-Direct Commercial Sales hybrid programs, Co-Production, International Cooperative

Research, Development, Testing and Evaluation agreements, when in operating or test environments with foreign government personnel. One-time disclosure authorizations may be documented in a specific memorandum or visit authorization. Requirements for continuing information disclosures are normally documented in a DDL. See DoD 5200.1-M and AFI 16-201 for TA/CP and DDL requirements.

A7.2.10.1. The TA/CP is accomplished anytime the program may have foreign involvement and serves three purposes:

A7.2.10.1.1. Assesses the feasibility of U.S. participation in joint programs from a foreign disclosure and technology security perspective.

A7.2.10.1.2. Supports drafting the Delegation of DDL. A DDL is a prerequisite to the disclosure of U.S. Government information to foreign entities.

A7.2.10.1.3. Serves as a supporting document for decision reviews.

A7.2.10.2. The TA/CP consists of two sections:

A7.2.10.2.1. Technology Assessment Section. This section focuses on the risk of disclosing U.S. technology or information to other countries. It identifies the technology of concern, its classification or control method, and why it is under development. It evaluates the availability of comparable foreign technology, previously released U.S. technologies, and any material released under other programs. Finally, it compares technologies and military capabilities, and possible damage resulting from compromise of these technologies or capabilities.

A7.2.10.2.2. Control Plan Section. This section describes the measures necessary to minimize potential risk associated with the material's release. It should discuss reducing the risk of compromise by phasing the release of information, using disclosure restrictions and using special security procedures to limit access to critical information. It should also include a discussion of any modification to the system, design, or production produced under the agreement, or any legal or proprietary concerns associated with such an agreement.

A7.2.10.3. DDLs are issued when there are requirements to disclose information in support of continuing programs. The program office, in coordination with the command or foreign disclosure officer (FDO), prepares a DDL derived from the TA/CP as part of the request for authority to negotiate and conclude an international agreement. Reference AFI 16-201 for further guidance.

A7.2.11. Life Cycle Protection Cost Estimates. The following guidance is intended to clarify how to allocate protection costs in the PPP. Direct costs associated with the Work Breakdown Structure (WBS) should be documented in the PPP and detailed for each acquisition phase. Protection costs include manpower, equipment, services, and other costs that directly contribute to the protection of CPI, critical components and other sensitive system design information. Protection costs should be reflected in accordance with the WBS. See MIL-STD-881, *Work Breakdown Structures for Defense Materiel Items*.

A7.2.11.1. Identify only the costs of Program Protection that exceed normal NISPOM costs. (Accounting for security costs associated with NISPOM compliance has limited

utility as the majority of defense contractors include costs as part of management costs and do not normally segregate security costs for NISPOM compliance.)

A7.2.11.2. Manpower costs for protection during operational use as well as the development program should include all personnel who provide direct support to the program protection effort.

A7.2.11.3. List equipment used in the protection effort and associated cost. For example, include the cost of safes, secure computers, software, entry controls, alarms, vault area construction, administrative equipment, and security equipment engineered into the weapon system.

A7.2.11.4. Other miscellaneous costs should be identified including the transport of classified components.

A7.2.11.5. Additional requirements to meet demilitarization and disposal costs should be identified if applicable.

A7.2.11.6. PPP cost information cannot be released to international customers.

A7.2.12. Freedom of Information Act (FOIA) Requests. PMs should evaluate and include prudent and necessary life cycle planning to address FOIA requests in accordance with DOD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program*. The primary objective is to develop methods to effectively balance public release needs and protection of program information.

A7.2.13. Scientific and Technical Information (STINFO). PMs should use prudent life cycle planning to address the need to:

A7.2.13.1. Mark data controlled IAW DoDI 5230.24, *Distribution Statements on Technical Documents*.

A7.2.13.2. Withhold unclassified technical data from public disclosure in accordance with DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure* and AFI 61-204, *Disseminating Scientific and Technical Information*.

A7.3. Security Actions during PPP Coordination. Use encryption when emailing PPPs. CPI should be protected as FOUO at a minimum. See DoD 5200.01-v4 for exemptions. If there is Sensitive Compartmented Information (SCI) used in association with a system, the program office should coordinate the PPP with the cognizant Special Security Office (SSO).

Attachment 8

CPI IDENTIFICATION SURVEY AND DECISION AID

A8.1. The USD (I)-developed CPI identification survey provides a common set of criteria to assist PMs in determining if their program, project, or research effort has CPI. A Research, Development, Test, and Evaluation (RDT&E) organization (e.g. the Air Force Research Laboratory) whose programs do not have a DoDI 5000.02 acquisition program element may tailor the CPI identification survey.

A8.2. The PM should complete and certify inputs to this survey.

A8.3. Once the survey is completed, the PM signs the certification page and delivers the survey, certification pages, and supporting documentation to the appropriate AFMC or AFSPC organization protection POC.

A8.4. The PEO and/or the responsible organization protection office will use the results of the survey to determine the potential for CPI and what follow-on actions, if any, may be required IAW DoD 5200.01-v1. The decision should be documented in an official memorandum to the office submitting the survey. CPI and critical components should be protected based on classification level as described in DoDM 5200.1-M.

A8.5. Administrative items that do not apply should be marked "N/A".

A8.6. All survey questions should be answered. Clarifying remarks may be attached on a separate piece of paper.

A8.7. If questions arise while completing this survey, contact the responsible protection office for the program.

A8.8. When filled in, the CPI survey is classified and controlled according to content. At a minimum, CPI surveys will be marked "For Official Use Only" IAW DoD 5200.01-v4.

Table A8.1. CPI Identification Survey Administrative Data and Survey Questions.

I. CPI Survey Administrative Data and Information.	
POC for this survey (name, phone, e-mail):	
Service/Agency:	
Organization:	
Program/Project/Research Effort Name:	
ACAT (if applicable):	
Budget Activity:	
Current MS (if applicable):	
Next MS/MS Date (if applicable):	
PMD#/Code:	

LOA (Letter of Offer & Acceptance):			
Program/Project/Research Effort Description: (A brief overview will suffice)			
II. <u>CPI Survey Questions.</u>			
1.0 Will this program use only unmodified commercial items, non developmental items (NDI), or commercial off the shelf (COTS) items?		YES	NO
2.0 Will the combination of commercial items, NDI, or COTS, items remain functionally unmodified for this intended military application?			
3.0 Will this program use the commercial items, NDI, or COTS items in their original commercial intended purpose?			
4.0 Does the program result in a new mission or military capability?			
5.0 Is the program considered "State of the Art"?			
6.0 Is the program using technology or information available solely from U.S. sources, U.S. academic institutions, or U.S. industry?			
7.0 Will this program exploit a specific technical vulnerability?			
8.0 Will this program involve a permanent modification or upgrade of a fielded system resulting in an increase in mission or military capability?			
9.0 Has a decision been made to withhold information from the public about this program?			
10.0 Is this a research program?			
11.0 Will any of this program be a part of any foreign inventory?			
12.0 Will this program develop unique items used to evaluate capabilities or requirements?			
13.0 Will this program require development of unique training items related to operations or maintenance?			
III. <u>CPI Survey Result Certification</u>. I hereby certify the answers on this survey are correct and accurate to the best of my knowledge. Signature/Title _____Date:_____			

Figure A8.1. CPI Identification Decision Aid.

Discussion Area 1 (Concept)

1.1. Is the concept in the public domain? **NO - go to 1.1.1 // YES - go to 1.1.2**
1.1.1. Does the concept provide us an enhanced capability? **NO – End Branch // YES – Candidate CPI Discussion**

1.1.2. Are other countries/organizations pursuing the same or a similar concept? **NO – Go to 1.1.2.1 // YES – Go to 1.1.3**
1.1.2.1. Would divulging US intent to pursue it cause public outcry or diplomatic harm? **NO – End Branch // YES – Candidate CPI Discussion**

1.1.3. Has a demonstrator been developed by another country/organization? **NO – Go to 1.1.3.1 // YES – Go to 1.1.3.2**
1.1.3.1. Have we developed a demonstrator? **NO – End Branch // YES – Candidate CPI Discussion**
1.1.3.2. Is our conceptual approach markedly different? **NO – End Branch; Go to 1.2 // YES – Candidate CPI Discussion**

1.2. Would the disclosure of the operational concept (just the concept) enable an adversary to counter or defeat the system capability directly? **NO – Go to 1.3 // YES – Candidate CPI Discussion**

1.3. Does the relationship between the system and its intended user reveal a unique operational capability, specific target, or mission set? **NO – End Thread // YES – Candidate CPI Discussion**

Discussion Area 2 (Materials)

2.1. Are materials, computer languages or devices innovative themselves, or as they are used / employed? **NO – End Branch // YES – Go to 2.1.1**
2.1.1. Do these materials, computer languages, or devices provide an enhanced capability? **NO – End Branch // YES – Candidate CPI Discussion**

Discussion Area 3 (Design)

3.1. Are any COTS/GOTS used, integrated or modified in a unique way that provides an enhanced capability, or were new capabilities developed as a result of modifications to COTS/GOTS? Do the COTS/GOTS support critical functions therefore warranting enhanced supply chain risk management? **NO – Go to 3.2 // YES – Candidate CPI Discussion**

3.2. Would obtaining this design (to include Intellectual Property) provide an adversary a technological advantage? **NO – Go to 3.3 // YES – Go to 3.2.1**
3.2.1. Does this item's function and/or capability depend on this design? **NO – Go to 3.3 // YES – Candidate CPI Discussion**

3.3. Was the system designed to specifically exploit a known foreign vulnerability (software, hardware, or procedural)? **NO – Go to 3.4 // YES – Candidate CPI Discussion**

3.4. Would the information resulting from modeling/simulation, test/evaluation or training systems) reveal enhanced system performance or capability? **NO – End Branch // YES – Candidate CPI Discussion**

Discussion Area 4 (Manufacturing)

4.1. Are manufacturing/fabrication/coding processes standard and / or well known? **NO – Go to 4.2 // YES – Go to 4.1.1**
4.1.1. Do any of these manufacturing/fabrication/coding processes provide an enhanced capability? **NO – Go to 4.2 // YES – Candidate CPI Discussion**

4.2. Do the processes for manufacturing/fabrication/computer coding/tooling require or reveal unique tooling or materials? **NO – End Branch // YES – Go to 4.2.1**
4.2.1. Do the tooling or materials provide an enhanced capability? **NO – End Thread // YES – Candidate CPI Discussion**

Discussion Area 5 (Integration)

5.1. If COTS/GOTS are used, are they integrated in a unique way providing an enhanced capability or were new capabilities developed? **NO – Go to 5.2 // YES – Candidate CPI Discussion**

5.2. If non COTS/GOTS are used, are they integrated in a unique way providing an enhanced capability or were new capabilities developed as a result of the integration? **NO – End Branch // YES – Candidate CPI Discussion**

5.3. Are any legacy items, non COTS/GOTS, and/or COTS/GOTS integrated in any combination with each other that provides an enhanced capability, or were new capabilities developed as a result of the integration? **NO – End Branch // YES – Candidate CPI Discussion**

Discussion Area 6 (Operational Environment)

6.1. Would obtaining this item alone enable another organization/country to degrade the item or system's operational capability? **NO – End Branch // YES – Candidate CPI Discussion**

Attachment 9

PIT DETERMINATION CHECKLIST

Table A9.1. Platform IT Determination Checklist (Consult AFI 33-210 for latest version).

Platform IT Determination Checklist.

Question	Responses	If one or more checked	If none checked
(1) Does the IT system or IT component do any of the following with respect to **DoD owned or controlled information systems**? Reference: DoDD 8500.01	☐ Receive ☐ Transmit ☐ Process ☐ Store ☐ Display	CONTINUE WITH QUESTION 2	**STOP.** **There is no Information Assurance Requirement.**
(2) Which of the following describe the IT system or IT component? **(check all that apply)**	☐ It is **physically part of or embedded** in the platform Briefly describe below how the system is physically part of or embedded in the system: ☐ Its special-purpose mission is **dedicated to** the platform's mission Briefly describe below how the special-purpose mission is dedicated to the	CONTINUE WITH QUESTION 3	**STOP** **The IT is not Platform IT** and is subject to the DIACAP C&A process.

Question	Responses	If one or more checked	If none checked
	platform's mission: ☐ Its special-purpose mission is **essential in real time** to the platform's mission Briefly describe below how the special-purpose mission is essential in real time to the platform's mission:		
(3) Does the mission of the IT **provide <u>general IT services</u>**, such as e-mail, common office applications, networking for one or more non-Platform IT systems, business functions, etc.?	☐ Yes (Note: Do not check "yes" if the only possible connection from the IT in question is to another Platform IT system. Also, e-mail, chat and VoIP used exclusively for tactical operator-to-operator communications with procedures in place limiting the use of e-mail and chat may be part of Platform IT systems.)	**STOP** **The IT is not Platform IT** and is subject to the DIACAP C&A process.	CONTINUE WITH QUESTION 4
(4) Does the IT system or IT component perform any of these **special-purpose missions?**	☐ Weapon System ☐ Training Simulation	**The IT is considered to be Platform IT** and is exempt from the	**STOP** **The IT does not appear to be Platform IT** and is

Question	Responses	If one or more checked	If none checked
(check all that apply)	☐ Diagnostic Testing and/or Maintenance ☐ Research and Development (R&D) of Weapon Systems ☐ Calibration ☐ Medical Technology ☐ Transportation ☐ Industrial Control Systems/SCADA Systems ☐ Utility Distribution, such as for Water or Electric ☐ Fire control and targeting; missile; gun; active EW; decoy; launcher; vehicle; artillery; man-deployable system; flight, bridge, classroom training simulator; ☐ Sensor (acoustic, passive EW, ISR, national, control, navigational); radar; P2P or LOS data link; voice comm.; IFF; C2 of forces; navigation system; GPS; displays/consoles;	DIACAP C&A process, but still must incorporate IA requirements. **CONTINUE WITH QUESTION 5** .	subject to the DIACAP C&A process. If the PM/IAM is still unclear as to whether the IT is Platform IT, the PM may submit program and technical information to the AF-CA for an official determination.

Question	Responses	If one or more checked	If none checked
	tactical support database or decision aid; some mobile PCs ☐ Unmanned systems (UAV/ UAS, RPA, and RCS) ☐ Modeling and Simulation		
(5) Does the IT in question have any interconnection to a non-Platform IT system? (Note 1: If the configuration of the Platform IT system changes, the new changes must be addressed with this guide). Note 2: If the configuration of the Platform IT system changes requiring an interconnection to a non-Platform IT system then these changes must be addressed with this guide ref paragraph 3.0, page 16.	☐ Yes Briefly describe below the interconnection to a non-Platform IT system.	The interconnection is subject to the DIACAP C&A process. Submit the package to the AF-CA.	The IT is required to incorporate IA controls but is not subject to the DIACAP C&A process. Follow IA PIT C&A guidance. Submit this checklist and PIT Determination Concurrence request package to the PIT DAA Representative for coordination.

Attachment 10

KEY PROGRAM PROTECTION TASKS BY ACQUISITION PHASE

Table A10.1. Key Program Protection Tasks By Acquisition Phase.

Key Program Protection Tasks by Acquisition Phase	Technical Development	Engineering & Manufacturing	Production & Deployment	Operations & Support
System security concept study to ID key protection concepts & support development of protection requirements	X			
Integrate system security protection and countermeasure needs	X	X	X	X
Request System Threat Assessment (STA) or Report (STAR)	X	X	X	X
Request Counterintelligence Threat Assessment (CITA)	X	X	X	X
Develop Security Classification Guide (SCG) (time-phased)	X	X	X	X
Initiate system security Certification and Accreditation (C&A)	X	X	X	X
Refine critical function list and identify critical system components	X	X	X	X
Identify candidate CPI and critical components and manufacturing facilities	X	X	X	X
Request DIA SCRM TAC assessments on critical components	X	X	X	X
Complete PIT determination for inclusion in IAS document		X		
Conduct Threat Analysis (TA)	X	X	X	X
Conduct Vulnerability Analysis (VA)	X	X	X	X
Conduct risk analysis	X	X	X	X
Select countermeasures	X	X	X	X