CH 9–1. Purpose

The Defense Acquisition Guidebook (DAG), Chapter 9, provides guidance for the system security engineering (SSE) discipline and Department of Defense (DoD) program protection for defense acquisition programs. The program manager (PM) and the systems engineer (SE) should use DAG Chapters 3 and 9 to effectively plan and execute program protection activities across the acquisition life cycle.

CH 9–2. Background

Program protection provides the processes, methodologies, and techniques to enable program offices to identify information, components, and technologies, as well as determine the most appropriate mix of measures to protect the information, components, and technologies from known security threats and attacks. These protection measures impact the development of the system being acquired, the operations of the program office, and the means by which the items are acquired.

CH 9–2.1 Purpose of Program Protection

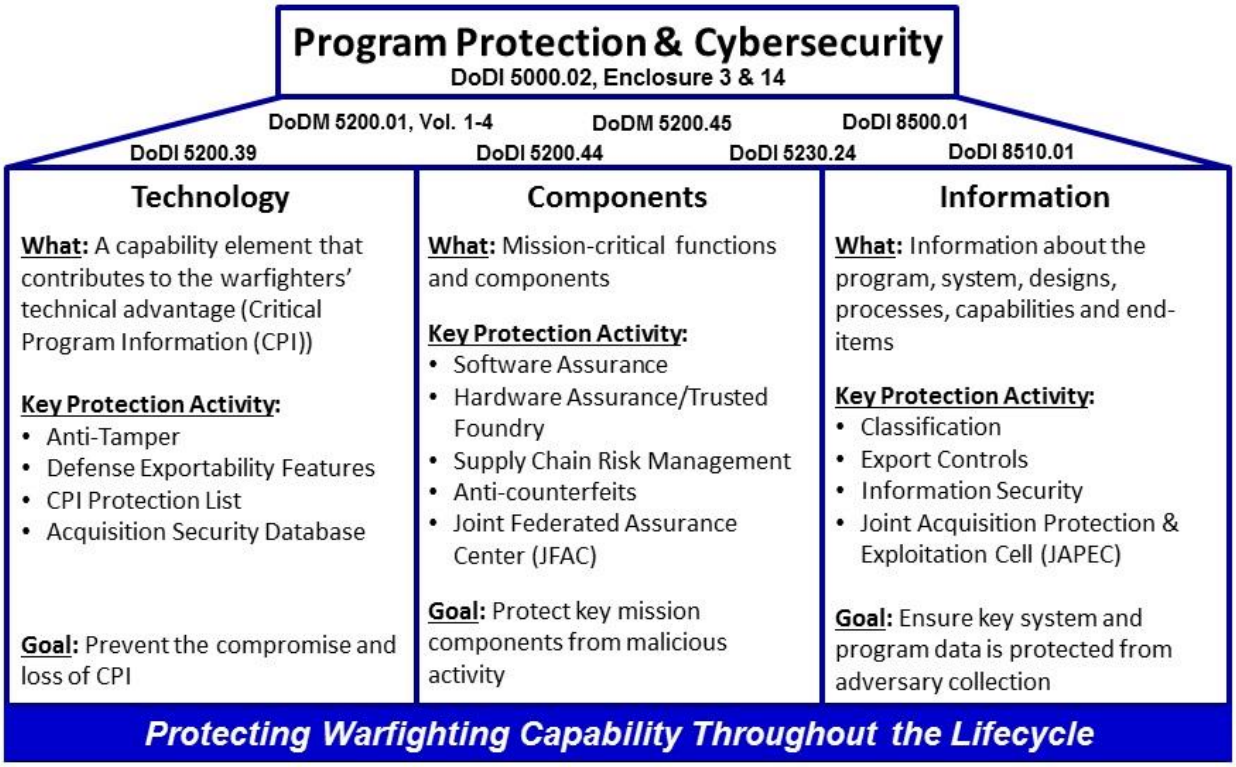
The purpose of program protection is to give PMs an effective way to understand, assess, and prioritize the broad spectrum of security threats and attacks to the acquisition program, and to identify the right, cost-effective mixture of measures to protect against such attacks. Since the scope of the acquisition program can include all program and system information, organization and personnel, enabling networks, and relevant systems (i.e., systems in acquisition, enabling systems, and support systems), PMs should consider security threats and attacks to the following program elements that can be exposed to targeting:

- Government program organization
- Contractor organizations and environments
- Software and hardware
- System interfaces
- Enabling and support equipment, systems, and facilities
- Fielded systems.

To address threats and vulnerabilities associated with these program elements, program protection focuses on (as shown in Figure 1):

- Information (including program and system information)
- Technology (critical program information (CPI))
- Components (mission-critical functionality).

Figure 1: Key Program Protection Activities



Policies, guidance and white papers are found at our initiatives site: https://www.acq.osd.mil/se/initiatives/init_pp-sse.html

CH 9–2.2 Program Protection Policy and Guidance

PMs and Systems Engineers (SEs) should know and understand the statutory and regulatory Systems Engineering (SE) mandates. Table 1 identifies top-level Program Protection-related policy.

Table 1: Key Program Protection Related Policies

Program Protection Policies
DoDI 5000.02, Operation of the Defense Acquisition System
DODI 5000.02, ENCL 13, Cybersecurity in the Defense Acquisition System
DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI) and associated manuals (DoDM 5200.01 Vol 1-4)
DoDI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)
DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
DoDM 5200.45, Instructions for Developing Security Classification Guides
DoDI 5230.24, Distribution Statements on Technical Documents
DoDD 5200.47E, Anti-Tamper (AT)
DoDI 8500.01, Cybersecurity
DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

DoDI 5000.02, Operation of the Defense Acquisition System establishes policy for the management of all acquisition programs, including requirements for program protection. For program protection, the policy describes the content, submission, and approval requirements for PPPs throughout the acquisition life cycle (Milestones A, B, C, plus Full Rate Production [FRP] or Full Deployment Decision [FDD]), including operations and maintenance. It also apprises management of the risks to program and system information and critical program information, as well as mission-critical functions and components associated with the program

DODD 5000.02, ENCL 13, Cybersecurity in the Defense Acquisition System prescribes procedures for acquisition responsibilities related to cybersecurity (CS) in the Defense Acquisition System.

DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI) provides policy and responsibilities for collateral, special access programs, SCI, and controlled unclassified information (CUI) within an overarching DoD Information Security Program. The associated manuals provide procedures for the designation, marking, protection, and dissemination of CUI and classified information, including information categorized as collateral, SCI, and Special Access Program (SAP). For program protection, this issuance provides guidance for classification and declassification of DoD information that requires protection in the interest of national security.

DoDI 5200.39, Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation establishes policy that requires the identification and protection of CPI and defines CPI and its protections. Key activities include:

- Horizontal identification and protection analysis
- Anti-tamper analysis and protection
- Counterintelligence, intelligence, and security assessments and support
- International Cooperative Program CPI protection considerations.

DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission-critical functions or components (e.g., software, microelectronics). Key activities include:

- Identification of mission-critical functions and components
- Use of all-source intelligence analysis of suppliers of critical components
- Use of enhanced software and hardware vulnerability detection and mitigation
- Use of tailored acquisition and procurement strategies.

DoDM 5200.45, Instructions for Developing Security Classification Guides provide guidance for the development of security classification guidance.

DoDI 5230.24, Distribution Statements on Technical Documents establish policy for the marking and distribution of DoD technical information/documents.

DoDD 5200.47E, Anti-Tamper (AT) establishes policy and assigns responsibilities for AT protection of critical program information (CPI). It also designates the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) as the Principal Staff Assistant (PSA) responsible for oversight of the DoD AT program and policy, and designates the Secretary of the Air Force (SECAF) as the DoD Executive Agent (EA) for AT.

DoDI 8500.01, Cybersecurity establishes responsibility to protect and defend DoD information and information technology, and explicitly provides the Under Secretary of Defense for Acquisition, Technology and Logistics (USD) (AT&L) the responsibility to integrate policies established in the 8500.01 and its supporting guidance into acquisition policy, regulations, and guidance consistent with DoDD 5134.01.

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) establishes the requirement for DoD to implement the RMF to manage life cycle cybersecurity risk to DoD IT. For program protection, it establishes the following:

- The system categorization is to be documented in the cybersecurity strategy within the PPP.
- The security engineering of tailoring security control requirements and cybersecurity-testing considerations is integrated into the program's overall systems engineering process and then documented and updated in the Systems Engineering Plan (SEP) and PPP throughout the system life cycle.

Program protection guidance, in addition to the DAG, is provided on the Deputy Assistant Secretary of Defense for Systems Engineering (DASD [SE]) website, http://www.acq.osd.mil/se/initiatives/init_pp-sse.html.

CH 9–2.3 Program Protection Plan

The Program Protection Plan (PPP) is a living plan to guide efforts to manage the risks to CPI and mission-critical functions and components, as well as program and system information. This milestone acquisition document captures both systems security engineering (SSE) and security activities and the results of the analyses as the program and system become more defined.

PMs should employ SSE and security practices to prepare a PPP, using the Program Protection Plan Outline and Guidance. The PM should tailor the PPP as necessary to meet the characteristics of the system being acquired. The PM should also ensure that security considerations are incorporated into the system requirements, design, integration, and supply chain activities. The level of detail contained in the PPP should be commensurate with the maturity of the system design. The PPP should be updated for each of the technical reviews, and the security risks and mitigations should be assessed at each technical review.

The PPP is submitted for Milestone Decision Authority (MDA) approval at each Milestone review and the Full Rate Production or Full Deployment Decision Review. For programs with the Defense Acquisition Executive such as the MDA, PPPs are submitted to the DASD(SE) not less than 45 calendar days before the relevant review. Also, a DoD Component-approved draft PPP must be provided to the DASD(SE) 45 days before the Development Request for Proposal Release Decision Point.

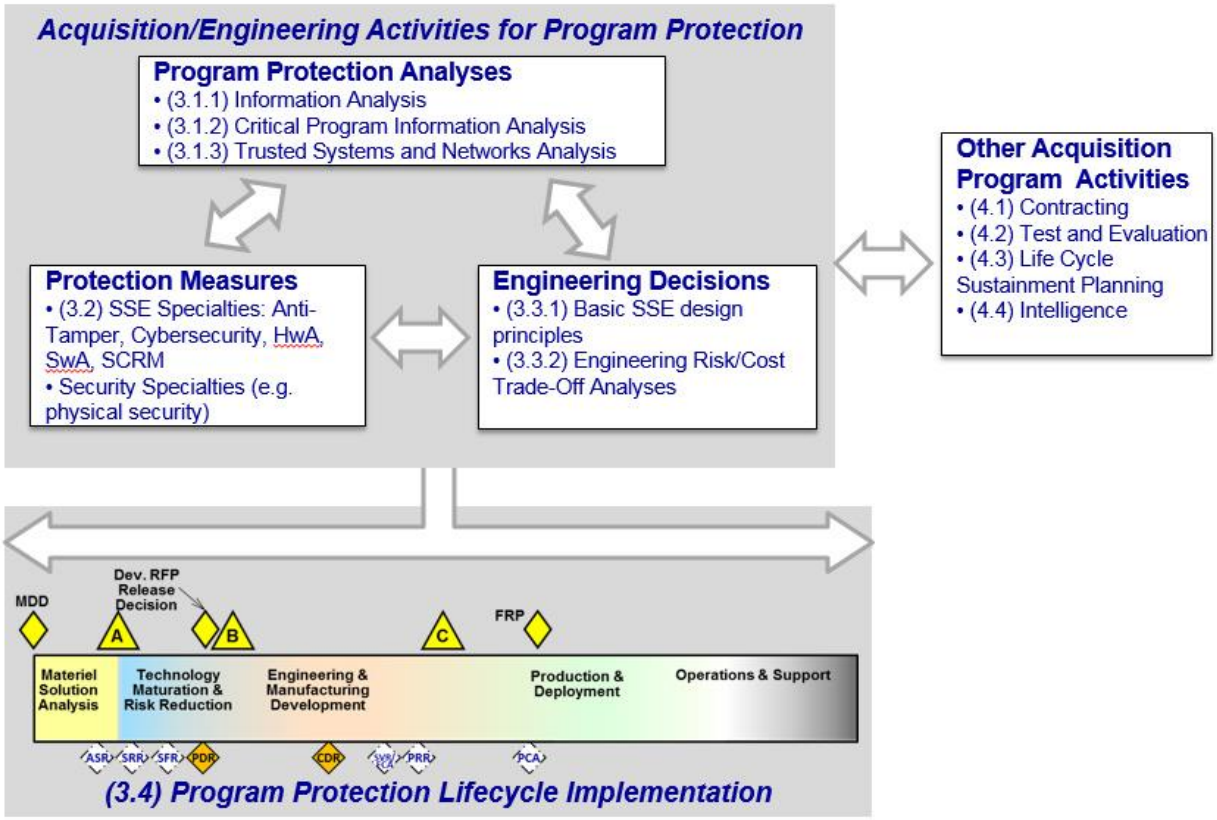
After the Full Rate Production or Full Deployment Decision, the PPP should transition to the PM responsible for system sustainment and disposal.

CH 9–2.4 Program Protection Activities and Relationships

The goal of program protection is to help programs identify and implement the most appropriate mix of measures to protect the program and system information, components, and technologies from the known security threats and attacks across the acquisition life cycle.

With that goal in mind, the program management office should execute the following program protection activities. Program protection activities and their relationships to each other and to other defense acquisition functions are captured in Figure 2, which also includes the Chapter 9 sections that describe each activity and relationship.

Figure 2: Overview of Program Protection Activities and Relationships



- *Program Protection Analyses:* Activities to help programs understand the risks to a program's technology, components, and information.
- *Protection Measures:* Activities to derive protection measures from the specialties within system security engineering (i.e., anti-tamper, RMF for DoD IT, exportability features, hardware assurance, software assurance, and supply chain risk management) and general security specialties to address security threats and attacks. Each specialty has a set of analyses, approaches, and protections that programs can utilize.
- *Engineering Decisions:* Activities, primarily trade-offs, to determine the most appropriate set of requirements given the program constraints. For program protection, this means conducting trades among protection measures. There is also a basic set of security principles that should be incorporated into the system design.

All of the above activities are executed iteratively across the acquisition life cycle in order to refine protection measures as the system design matures. Additionally, throughout the life cycle, program protection informs and is informed by other aspects of defense acquisition, including contracting, test and evaluation, life-cycle sustainment planning, and intelligence.

The Program Protection activities are further described in Sections 3 and 4.

For those seeking more detailed coverage of program protection concepts, policy and processes, the Defense Acquisition University (DAU) offers ACQ160, Program Protection Planning Awareness. An online course that takes approximately three days to complete, ACQ 160 is intended for the entire Acquisition Workforce, with focus on ENG, PM, IT, CON, LCL, and T&E career fields. More information can be found at http://icatalog.dau.mil/onlinecatalog/courses.aspx?crs_id=2082.

CH 9–2.5 Roles, Responsibilities, and Resources

Security, including cybersecurity, of DoD programs and systems is the collective responsibility of the entire acquisition workforce. However, the primary roles supporting program protection are the PM, systems engineer (SE), system security engineer, system security engineering specialists, security specialists, and chief developmental tester. The Program Management Office (PMO) is responsible for including the appropriate requirements in the solicitation in order to transition into the development effort.

Typical responsibilities for each of these roles are detailed below. Note that these roles are described functionally. Not every program will have an individual associated with each role; some programs will have individuals who fulfill multiple roles.

PMs have the overall responsibility for program protection planning throughout the acquisition life cycle as well as documenting the plans and results of the program protection analyses in a PPP, as required in DoDI 5000.02 encl. 1, Table 2 – Page 56. Specific responsibilities for the PM include:

- Managing the program protection risks
- Adequately resourcing program protection efforts (i.e., staff, budget)
- Initiating program protection efforts early and ensuring analyses are iteratively conducted throughout the acquisition life cycle
- Considering international acquisition and exportability early, along with their impact on program protection
- Incorporating program protection sufficiently into solicitations and contracts
- Completing and submitting the PPP for approval in accordance with DoDI 5000.02
- Support for activities to achieve protection consistency across programs.

SEs are responsible for ensuring the development and delivery of capability through the implementation of an approach with respect to cost, schedule, performance, and risk. This is accomplished using integrated and consistent systems engineering (SE) activities and processes, regardless of when a program enters the acquisition life cycle. The SE conducts trade-off analyses and integrates contributions from each engineering specialty and design consideration. Each plays a role in the design of the system, and it is the SE who works to synthesize and balance the requirements. One of these design considerations is system security engineering (SSE), which addresses program protection. As system security engineering relates to program protection, the SE is specifically responsible for:

- Integrating program protection/SSE into the program's systems engineering processes
- Conducting trade-off analyses with respect to system security and other design considerations
- Collaborating with the system security engineer on any system security requirements adjustments
- Incorporating system security requirements into the system performance specification, technical baselines, and solicitation documents
- Ensuring the PPP is informed by the systems engineering constraints and decisions
- Leading the development of the PPP.

System security engineers integrate contributions from system security engineering disciplines such as anti-tamper, RMF for DoD IT, exportability features, hardware assurance, software assurance, and supply chain risk management; and security specialties such as personnel security, industrial security, physical security, and information security. The outcome is a comprehensive program and system protection within the constraints of cost, schedule, and performance while maintaining an acceptable level of risk. To integrate all aspects of system security, the system security engineer leads the evaluation and balancing of security contributions to produce a coherent security capability across the system and the program. As it relates to program protection, the system security engineer is specifically responsible for:

- Conducting/leading program protection analyses for program and system information, CPI, and trusted systems and networks (TSN)
- Collaborating with system security engineering specialists and security specialists to assess vulnerabilities and identify protection measures

- Conducting trade-off analyses to integrate protection measures from across security engineering specialties and security specialties in order to reduce security risks to meet acceptable levels based on performance, cost, and schedule
- Translating protection measures into system security requirements, and adjusting them, based upon constraints and decisions relayed from the SE
- Collaborating with the SE to integrate the system security requirements into appropriate systems-engineering artifacts
- Ensure security approaches are documented in the PPP appropriately.

System security engineering specialists identify the system security threats and vulnerabilities and the appropriate system security protection measures within the scope of their system security engineering specialty. Specifically, these specialists are responsible for:

- Assisting the system security engineer with program protection analyses
- Identifying protection measures within their specialty
- Collaborating with the system security engineer to adjust protection measures based on constraints and decisions relayed from the SE
- Communicating resource needs to the SSE and SE.

As program protection integrates system security engineering specialties and security specialties, there is also a key role played by security specialists. Security specialists identify the security vulnerabilities and needed security protection measures within the scope of their security specialty. These specialists are specifically responsible for:

- Defining, implementing, and monitoring security protection measures
- Collaborating with the system security engineer in order to inform the program protection analyses and modifying the security protection measures to meet program needs.

The chief developmental tester ensures program protection is incorporated into the program's test and evaluation (T&E) efforts. The chief developmental tester is specifically responsible for:

- Planning of developmental test and evaluation (DT&E), which includes cooperative vulnerability testing
- Conducting verification and validation (V&V), with respect to system security requirements
- Ensuring required verifications against representative attack scenarios are performed, where applicable, to address system security requirements
- Planning for operational test and evaluation (OT&E), which should include adversarial testing—adversarial tests typically subject a system to a series of attacks, simulating the tactics of an actual threat exploiting the system's vulnerabilities; this may exclude testing from a hands-on reverse engineering perspective.

Contractors also play a key role in program protection. Contractors have the responsibility to conduct program protection planning and execution as contractually agreed upon (details on contracting for program protection can be found in Section 4.2). The Contractor's specific responsibilities for system security vary by contract, but typically include:

- Implementing security-related Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulation Supplements (DFARS)
- Integrating system security as part of its systems engineering activities
- Supporting program protection analysis and contributing to government updates of the PPP for each of the systems engineering technical reviews
- Assessing and mitigating system security risks as part of the technical assessment.

There are also other resources outside of the program office that can play a key role to ensure that comprehensive program protection is implemented. These resources include:

- Intelligence and Counterintelligence: Threat information is a key resource to help inform PM decisions related to program protection across the acquisition life cycle. Various intelligence and counterintelligence activities are available to PMs through their DoD Component. More information on how intelligence and counterintelligence support informs program protection can be found in Section 4.5.
- Joint Acquisition Protection and Exploitation Cell (JAPEC): The JAPEC facilitates collaboration of PMs with the intelligence and counterintelligence communities on system security protection, and analysis of unclassified controlled technical information (CTI) losses. This analysis enables PMs to determine if any necessary courses of action must be taken to mitigate the risks associated with losing technical information. More information about the JAPEC can be found in Section 4.4.1.
- Joint Federated Assurance Center (JFAC): The JFAC is a federation of DoD organizations that provides a variety of software (SwA) and hardware assurance (HwA) capabilities to support programs in mitigating their vulnerabilities. More information about how a program can utilize the services provided by the JFAC can be found in Section 4.5.
- DoD Executive Agent for Anti-Tamper (AT) and DoD Component Office of Primary Responsibility for AT: Confirms that AT requirements have been met before deployment and / or export of DoD systems with CPI.

PMs may use the above resources to support their program protection planning decisions.

CH 9–3. Best Practice

This Section describes the necessary program protection activities and how those activities are executed across the life cycle.

- Section 3.1 provides a description of analyses for each program protection consideration (i.e., information, technology, and components).
- Section 3.2 provides a description of each system security engineering (SSE) specialty and associated activities.
- Section 3.3 provides a description of key engineering design activities related to program protection, including key secure design principles and the execution of engineering trade-offs among protection measures.
- Section 3.4 provides guidance for executing the program protection activities described in Section 3.1 through 3.3 across the lifecycle, addressing each phase and relevant technical reviews and audits. These include the level of detail for the processes described in Section 3.2, as well as special considerations or areas of focus for specific points in the life cycle.

CH 9–3.1 Program Protection Analyses

There are three sets of interrelated analyses that are performed during program- protection planning, correlating to the three-program protection considerations listed in Section 2.1. Information Analysis (Section 3.1.1). Critical Program information (CPI) Analysis (Section 3.1.2), and Trusted Systems and Networks (TSN) Analysis (Section 3.1.3) encapsulate the methods and processes for protecting the program and system (information, technology, and components). These analyses are the primary activities for identifying and prioritizing what needs to be protected in the program and system.

The program protection processes, and their constituent activities and tasks, are not meant to be performed in a particular time-dependent or serial sequence. The Program Manager and Systems Engineer apply the processes iteratively, recursively, and in parallel (as applicable) throughout the life cycle to translate identified capability needs into balanced and integrated system-security solutions.

CH 9–3.1.1 Information Analysis

Information analysis is the set of activities that a program executes in order to identify, understand, and protect the information about the program and the information residing in the system being acquired. There are three information analysis activities:

- Identify information to be protected (Section 3.1.1.1): This includes the identification, classification, and marking of program and system information. It also provides the basis for a program to understand what information is associated with the program and system, as well as the importance of that information. Information identified provides the basis for decisions on protections (or other requirements) that must be implemented for the program and the system.
- Protect program information (Section 3.1.1.2): This includes activities related to selecting and implementing protections for information about the program. Information about the program includes organizations and personnel supporting the program, logistics and test documentation, key technologies, applications, processes, capabilities, suppliers, and end items.
- Protect system information (Section 3.1.1.3): These are the activities related to selecting and implementing protections for information on the system being acquired, which is defined as information residing on, processed by, or transiting through the system being acquired. These protections aim to ensure the confidentiality, integrity, and availability of information to preserve the assurance of the system being acquired.

Information analysis and related protections cover classified information and unclassified covered defense information (with a particular emphasis on technical information), as well as information that alone might not be damaging and might be unclassified, but which, in combination with other information could allow an adversary to compromise, counter, clone, or defeat warfighting capability.

When conducting information analysis, programs should pay particular attention to the identification and protection of technical information because technical information includes much of the research and engineering associated with DoD's programs; the majority of it resides on unclassified systems. If stolen, this information provides adversaries with insight into U.S. defense and industrial capabilities and allows them to save time and expense in developing similar capabilities. Therefore, protecting this information is critical to preserving the intellectual property and competitive capabilities of the defense industrial base and the technological superiority of our fielded military systems.

The output associated with information analysis can inform other program protection analyses:

- Critical Program Information (CPI) Analysis: Classification of information may be used as an input to CPI analysis. Classified information related to a system capability may indicate that the capability is advanced enough to be considered CPI and the severity of consequence of CPI compromise. Inversely, CPI identification can feed information analysis. If an item is identified as CPI, then the information associated with that item may be classified or warrant additional protections if the information is unclassified.
- Trusted Systems and Networks (TSN) Analysis: When assessing the risk to a mission-critical function/component (which accounts for risk to the design documents, supply chains, software, etc.), consider the security protection measures triggered by classification and marking of the information associated with that function/component. These protections should be accounted for in the determination of the likelihood of compromise or effort required by the adversary to compromise the function or component.

CH 9–3.1.1.1 Foundational Activities

Activities related to the identification, classification, and marking of information associated with a program are driven by DoD information security policies. These activities provide the foundation for a program to understand the information associated with the program and the system, as well as the importance of that information. The results of these foundational activities drive decisions about protections (or other requirements), which must be implemented for the program and the system.

In accordance with the information security policies listed in the Introduction, the program will conduct the following activities as they relate to the program circumstances. Note that these activities are not unique to acquisition programs and should not represent a separate effort from those currently being executed by information security activities programs.

- Classification and marking of all program information. The policies for classification and marking are found in DoDI 5200.01, and associated guidelines are available in DoDM 5200.01 Volumes 1 through 4.
- Development of a Security Classification Guide (if necessary). DoDM 5200.45 provides guidelines for developing security classification guides.
- Application of distribution statements for technical information. Distribution statements are applied to all technical information (both classified and unclassified). Policy and guidelines for applying these statements are available in DoDI 5230.24, DoDM 5200.01 Volume 2, and DoDM 5200.01 Volume 4. It is important for programs to consider the secondary distribution necessary for technical documents, given the importance and vulnerability of DoD technical information.

Some additional key points related to these foundational activities include:

- For programs containing classified information, the program office will coordinate with the Original Classification Authority (OCA) to set information security levels for each element of the program including unclassified, controlled classified, or classified (Confidential through Top Secret), and direct the classification and marking of any technical information in accordance with DoDM 5200.01, Volumes 1 through 4, and DoDI 5230.24.
- The program office is responsible for establishing and promulgating the security classification guidance consistent with the requirements in DoDM 5200.45. The PM is responsible for ensuring the promulgation of program-applicable security classification guides to the Government and contractor teams.
- Programs that contain classified information, generally, also contain unclassified CTI.
- For programs that contain only unclassified information, the PM may want to develop a document similar to the format of the Security Classification Guide (SCG) as a mechanism to identify and protect unclassified CTI. This will assist in implementation of DFARS requirements for safeguarding covered defense information.

Programs use the results of these activities to apply appropriate information security protections for the program and the system (which are addressed in more detail in Sections 3.1.1.2 and 3.1.1.3).

CH 9–3.1.1.2 Implementing Program Information Protections

Within the program office, personnel handle information in accordance with DoD policies and procedures. Government information systems that store, process, or transmit program information are also operated in accordance with DoD policies and procedures. Additional protections, such as increased limits on the distribution of controlled technical information, may choose to be implemented by a program.

Beyond how the program office handles its information internally, the program office must also relay requirements for handling and marking information to contractors through solicitations and contracts. Key aspects of this include the following:

- Processes, procedures, and protection for government and contractors to address a compromise of classified information are described in DoDM 5200.01 Volume 1 through 4, DoDI 5220.22, National Industrial Security Program (NISP), DoDM 5220.22, National Industrial Security Program Operating Manual (NISPOM). Defense Security Service administers the NISP and provides appropriate security education, training, and awareness to industry and government personnel. The NISPOM is implemented through Federal Acquisition Regulation (FAR) Clause 52.204-2 for contracts handling classified information.
- Identification and marking of unclassified Covered Defense Information (CDI) triggers protection requirements in DoDI 8582.01 and the mandatory DFARS Clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting.” Under DFARS Clause 252.204-7012, contractors are required to safeguard CDI NIST Special Publication 800-171, report cyber incidents of CDI and within 90 days of reporting the incident, provide media relevant to the incident to DoD when requested. Programmatic, strategic, and operational mitigations should be considered in determining an appropriate response to risks as the result of a cyber intrusion. Additionally, PMs are encouraged to engage eligible industry counterparts and recommend they

participate in the Defense Industrial Base Cyber Security/Information Assurance Program, established in Part 236 of Title 32 of the Code of Federal Regulations.
- Instructions for handling and marking are typically incorporated through Contracts Data Requirements List (DD Form 1423, Block 9), which are included as part of solicitations and contracts.

Programs can determine what program information is released through a contract. To mitigate some risk of losing technical information, programs need to limit the technical information released to a contractor to only what is necessary to perform the work of the specific contract.

CH 9–3.1.1.3 Implementing System Information Protections

Protection of information residing on or transiting through DoD systems is driven by the need for availability, integrity, and confidentiality. The foundational activities related to identifying, classifying, and marking information provide the basis for understanding what information will be residing on or transiting through the system being acquired, and what the availability, integrity, and confidentiality needs are for each type of information. For instance, classified information has different availability, integrity, and confidentiality needs than unclassified information.

The program will then select protection measures to meet the availability, integrity, and confidentiality needs for the types of information residing on the system. While the program has flexibility in selecting protection measures, there are specific situations in which DoD policy drives the implementation more specifically. Some of these situations include:

- Cross-domain solutions: When there is information in the system of more than one classification level, there may be a need to implement a cross-domain solution (if the information needs to be moved between classification levels). Programs should use validated security solutions when available and appropriate, such as those managed by the Unified Cross Domain Services Management Office described in DoDI 8540.01.
- Encryption: Based on the level of encryption required, a program may need to incorporate Federal Information Processing Standards (FIPS) or National Security Agency (NSA) certified cryptographic products and technologies into systems in order to protect information types at rest and in transit. Programs with certain cryptographic requirements, as determined by the information type or other protection considerations, should coordinate development efforts with the NSA Information Assurance Directorate.

These protection measures are captured in NIST 800-53r4, which is Step 2 of the Risk Management Framework (RMF) for DoD IT policy.

CH 9–3.1.2 Critical Program Information Analysis

CPI is the U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermine U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, training equipment, and/or maintenance support equipment, as defined in DoDI 5200.39 (Glossary Page 11).

Simply, CPI are often DoD-unique capabilities, those that are developed and owned by the U.S., that are necessary for U.S. technological superiority.

CPI compromise (when an exploiter acquires the CPI) may:

- Reduce U.S. technological superiority and shorten the combat-effective life of the system as the adversary develops and fields comparable capabilities and/or countermeasures
- Require research, development, and acquisition resources to counter the impact of compromise and regain or maintain the advantage
- Protection measures should be put in place to deter, delay, detect, and respond to attempts to compromise CPI.

CPI analysis is the means by which programs identify, protect, and monitor CPI. This analysis should be conducted early and throughout the life cycle of the program. Additionally, because CPI is critical to U.S. technological superiority, its value extends beyond any one program. As a result, CPI analysis should consider the broader impact of CPI identification and protection on national security.

CH 9–3.1.2.1 Critical Program Information Identification

CPI identification is conducted to determine if organic CPI (CPI owned by your program) and/or inherited CPI (CPI owned by another program but incorporated into your program/system) exists in the currently-known system or will exist in the operational, deployed system. CPI identification is also conducted to identify CPI that is no longer considered to provide a U.S. technical advantage to the warfighter and may no longer require its current level of protection.

CPI should be identified early and reassessed throughout the life cycle of the program, to include: prior to each acquisition milestone; prior to each system's engineering technical review; throughout operations and sustainment, and specifically during software/hardware technology updates.

To identify CPI, programs should:

- Use DoD, DoD Component, and program resources (e.g., intelligence products, security classification guides, the Acquisition Security Database [ASDB], DoD policy, provisos within license agreements) to identify technology areas and performance/capability thresholds associated with an advanced, new, or unique warfighting capability.
- Decompose the system to the lowest level possible to identify system attributes that exceed a threshold, and thus may indicate the presence of CPI.A threshold is a boundary associated with a capability or level of performance that exceeds what is available commercially or exists in adversary inventories.
- Produce an initial or updated list of CPI, or documentation stating that the operational, deployed system does not or will not contain CPI. Obtain PM approval of the CPI, incorporate the CPI into the PPP, and obtain Milestone Decision Authority approval of the CPI as part of the PPP.

Identification of CPI within a program typically involves collaboration among and input from the PM, SE, systems security engineer, science and technology representative, security representative, anti-tamper, and intelligence/counter-intelligence representative, as well as other program offices (if CPI is being inherited).

Please refer to the Acquisition Security Database (ASDB) for examples of CPI. CPI is not:

- Personally Identifiable Information
- Individually Identifiable Health Information
- Financial Information
- Logistics Information
- Operational Information (waypoints and target location data)
- System Performance
- Designs
- Manufacturing Details
- Vulnerabilities and Weaknesses
- Unmodified Commercial-Off-The-Shelf
- Multi-Level Security Solutions (defined in Committee on National Security Systems Instruction (CNSSI) Number 4009)
- Cross Domain Solutions (defined in CNSSI Number 4009)
- Cryptographic Solutions (defined in CNSSI Number 4009)

While the above may be classified and thus protected accordingly, they are not CPI because one or more of the following apply:

- It is not a capability,

- Its compromise does not result in technology transferred that can be used by the adversary to bolster their warfighting capability by leveraging the transferred technology,
- Its compromise does not result in technology transferred that can be used by the adversary to counter U.S. capabilities based on weaknesses or patterns identified within the transferred technology, or
- It does not live on the weapons system, training equipment, maintenance support equipment, or other supporting end-item.

CH 9–3.1.2.2 Critical Program Information Protection Measure Selection

CPI protection should commence soon after the CPI has been identified, and, like CPI identification, CPI protection should also continue throughout the life cycle of the program.

CPI protection measures seek to deter, delay, detect, and react to attempts to compromise CPI on the end item as a result of hands-on, reverse engineering attacks. Protections triggered by the identification of CPI include anti-tamper and defense exportability features. Other protection measures, listed under other system security engineering specialties, may also contribute to the protection of CPI; however, these protections are not triggered by the identification of CPI. For example, information about CPI, including design and manufacturing know how, is typically classified and would be protected in accordance with a Security Classification Guide and through NIST 800-53r4 protections on a government program office and NIST 800-171 protections on contractor-owned information systems. An adversary may target the supply chain to obtain that design and manufacturing know how, and, if compromised, would have the same consequence as if the CPI were acquired by reverse engineering the end-item.

In order to select the appropriate protection measures, programs should consider the:

- Consequence of CPI compromise--the impact on U.S. technological superiority if the CPI is compromised
- Exposure of the system--the likelihood that an adversary will be able to obtain the end item through battlefield loss or export,
- Assessed threat--foreign adversary interest and skill in obtaining CPI
- Known vulnerabilities of the system.

For more information on consequence of CPI compromise, system exposure and vulnerabilities, please refer to the Anti-Tamper Technical Implementation Guide. For threat information, programs should request a Counterintelligence Threat Assessment from the supporting Defense Counterintelligence Component in accordance with DoDI O-5240.24. For more information on the assessed threat, please refer to DAG Chapter 7, Section 4.3.

To initiate and coordinate counterintelligence activities supporting your program, follow the instructions in DoDI O-5240.24, Enclosure 4. The results of this coordination should be documented in a formal and living plan describing the activities to be conducted by a Defense Counterintelligence Component in support of your program; this plan is known as the Counterintelligence Support Plan (CISP) and is an annex to the PPP. The CISP should be reviewed and updated annually.

For organic CPI, identify all appropriate protections. For inherited CPI, confirm that the inherited protections protect the CPI at a level appropriate to the inheriting system's circumstances; adjust or add protections as needed, given any change to consequence of CPI compromise, exposure of the system, the assessed threat, and known vulnerabilities.

CH 9–3.1.2.3 Critical Program Information Monitoring

CPI monitoring should commence soon after the CPI has been identified, and should continue throughout the life cycle of the program.

CPI monitoring is the process for determining if an event has occurred that requires the program to reassess CPI or its associated protections. Events may include, but are not limited to, the following:

- Operational Environment: A change in the physical location of the system with CPI other than that for which it was originally designed
- Protection Effectiveness: A change in the ability of the CPI protections to deter, delay, detect, and respond to attempts to compromise CPI
- Security Classification: A change to a relevant SCG, and thus the classification thresholds
- System Modification: A change to the system architecture and/or designs
- Capability Maturation: A change in the state-of-the-art for a particular capability and thus the thresholds used for CPI identification
- Threat: A change in foreign adversary interest and skill in obtaining CPI.

If these events occur, the program should reassess CPI and associated protection measures.

CH 9–3.1.2.4 Horizontal Protection of Critical Program Information

Because CPI is not always unique to one program (i.e., two programs may contain similar CPI, or one program may inherit CPI from another), there is a risk of not protecting CPI similarly across all programs. In doing so, programs may:

- Expose similar or the same CPI to greater risk
- Undermine or diminish the protection investment made by another program
- Apply an inconsistent level of resources to protect CPI.

To prevent this from happening, programs are required to ensure horizontal protection; they should apply a consistent level of protection to similar CPI.

To meet this requirement, programs should first understand that horizontal protection starts with horizontal identification. Horizontal identification, a consistent determination of CPI across two or more programs, is challenging, given that historically, this decision has been program-centric. However, given the importance of CPI to U.S. technological superiority, the Office of the Secretary of Defense (OSD) and the DoD Components provide tools and resources to assist programs in making consistent and aligned decisions.

In support of horizontal identification, programs should make use of CPI identification subject matter experts and technologists within their DoD Component, security classification guidance, and DoD policy (e.g., DoDI S-5230.28). Additionally, programs should consult the ASDB, including the list of example CPI, to help identify the same or similar CPI associated with other programs. For more information about the ASDB, please contact your DoD Component ASDB representative or email OSD.ASDBHelpdesk@mail.mil.

In support of horizontal protection, programs are encouraged to work with the DoD Office of the Executive Agent for Anti-Tamper (ATEA) and its DoD Component Office of Primary Responsibility for Anti-Tamper early and often for guidance.

Where horizontal protection disagreements arise, affected programs should discuss, negotiate, and agree upon the level of protection required to ensure that an equivalent level of risk is achieved across the affected systems, considering potential differences in system exposure. If programs cannot reach agreement, the ATEA may inform the Low Observable/Counter-Low Observable (LO/CLO) Tri-Service Committee and the Milestone Decision Authority of any AT-related horizontal protection issues per DoDD 5200.47E (Encl. 2, para 7.b. – Page 5).

CH 9–3.1.3 Trusted Systems and Networks Analysis

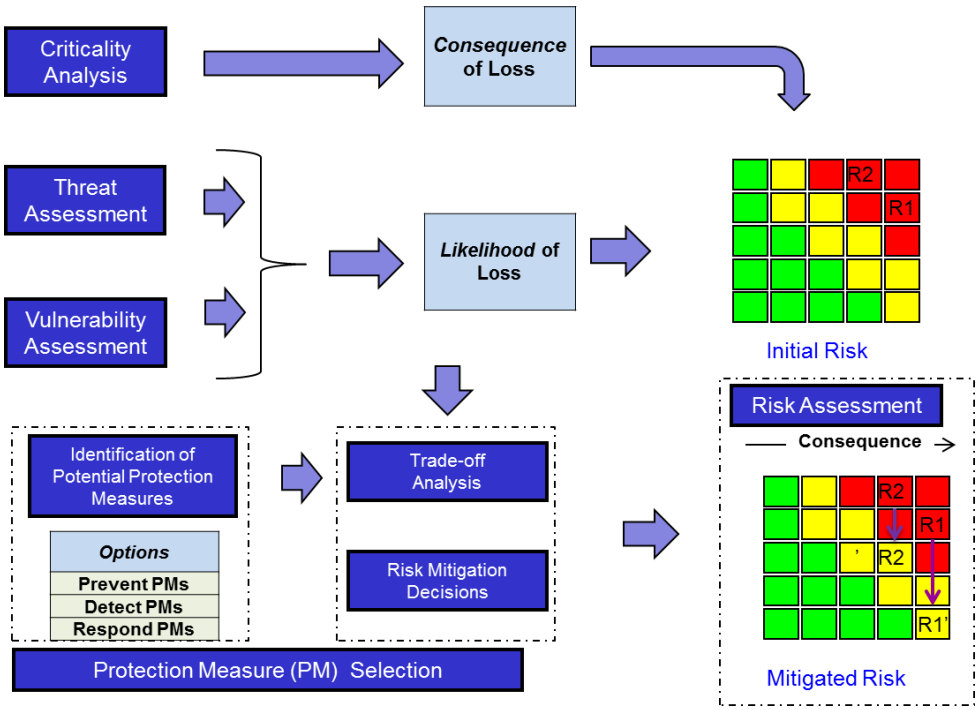
The goal of TSN Analysis is to protect those functions and components that are critical to conducting the system's intended mission(s) from intentional malicious insertion-related threats and attacks. TSN planning and execution activities include the following:

- Identification of the mission-critical functions and critical components of the system, commensurate with the system requirements decomposition

- Assessment and analysis of threats, vulnerabilities, and risk for identified mission-critical functions and critical components
- Risk mitigation and protection measures for planning and implementation
- Proactive planning and implementation of TSN key practices
- Trade-space considerations for protection measure selection
- Risk identification after protection measures are implemented, including follow-up mitigation plans and actions as well as assessments of residual risk.

TSN Analysis is completed by a program through conduct of a Criticality Analysis (CA), Threat Assessment (TA), Vulnerability Assessment (VA), Risk Assessment (RA), and Protection Measure Selection, all of which will be covered in greater detail in subsequent sections. The relationships between these activities are described in Figure 3. The TSN Analysis process is applied throughout the acquisition life cycle and should take into consideration the system security risks for the program. As the system evolves, the program should reconsider the criticality of the functions and components as well as the vulnerabilities and threats. By periodically repeating the risk management process, the program may identify additional threats and vulnerabilities that were not identified in previous iterations because the level of detail of the design was not sufficient to identify them. This continuous risk management process informs the system design trade-offs. Discovery of a potentially malicious source from the threat assessment may warrant additional checks for vulnerabilities in other (less critical) products procured from that source. For each program protection risk that is assessed as "high" or "very high," a risk cube and mitigation plans are needed.

Figure 3: TSN Analysis Methodology



Efforts to identify mission-critical functions and critical components and their protection begin early in the life cycle and should be revised as system designs evolve and mature. Iterative application of TSN Analysis, reinforced by tools such as threat design sensitivity analysis, misuse scenario evaluation, fault isolation trees, and system response analysis, will yield incremental refinements in the determination of what to protect and how to protect it. The analysis should be updated at each of the systems engineering

technical reviews to take into account the latest design and implementation decisions, as well as additional threat and vulnerability information.

Table 2 describes the level of detail required for TSN Analysis as it progresses through the life cycle, commensurate with its system specification level. In the Production and Deployment and the Operations and Support phases, it is expected that the analysis will be updated periodically to the level of detail of the Product Baseline (the same level of detail described in the column of the table labeled 'System Verification Review [SVR]/Functional Configuration Audit [FCA], Production and Deployment [P&D], and Operation & Sustainment (O & S) Phases. A periodic analysis should be conducted to support the development of an updated PPP for the FRP/FDD Decision Review. For a system upgrade, a program may have to conduct the analyses at all levels of detail described in the Alternative Systems Review (ASR) through SVR/FCA, as the system upgrade goes through development and is delivered in the system. Sections 3.1.3.1 through 3.1.3.5 summarize the analyses and techniques that comprise the TSN Analysis. Additional guidance for the TSN Analysis can be found in the *Trusted Systems and Networks (TSN) Analysis* white paper found at the http://www.acq.osd.mil/se/initiatives/init_pp-sse.html website.

Table 2: TSN Analysis Level of Detail Throughout the Life Cycle

Life Cycle Event	Criticality Analysis (CA)	Vulnerability Assessment (VA)	Risk Assessment (RA)	Protection-Measure (PM)
ASR	• Mission-based functions	• Response to Milestone A Vulnerability Questionnaire	• Objective risk criteria established • Applied at function level	• Risk-based supply chain, design and software PM selected via trade-off study
SRR	• System requirements level functions	• Vulnerability Questionnaire and Vulnerability Database DB assessment	• Risk criteria updated applied at system level	• Risk-based system function level PM selection
SFR	• Subsystem level subfunctions	• Vulnerability Questionnaire and DB assessment to critical subsystem level	• Risk criteria updated and applied at subsystem level	• Risk based subsystem function level PM refinement and selection
PDR	• Assembly/ component	• Vulnerability Questionnaire and DB assessment to critical Assembly/Component	• Risk criteria updated and applied at assembly level	• Risk based assembly level PM selection
CDR	• Component/ part	• Vulnerability DB, static analysis and diversity assessment to critical component level	• Risk criteria updated and applied at component level	• Risk-based component level PM selection
SVR/FCA, P&D and O&S Phases	• Part (preliminary)	• Vulnerability DB, static analysis and diversity assessment to critical part level	• Risk criteria updated and applied at prelim part level of critical components	• Risk-based part level PM selection

All selected protection measures should be incorporated into relevant solicitations, system specifications, and statements of work. The Request for Proposal (RFP) should incorporate the results and decisions from the systems engineering technical review immediately preceding the RFP release. In the generic life cycle, the Technology Maturation and Risk Reduction (TMRR) phase RFP would be based on the ASR analysis results; the Engineering and Manufacturing Development (EMD) phase RFP would be based on the System Functional Review (SFR) analysis results; and the Production RFP would be based upon the Critical Design Review (CDR) analysis results.

CH 9–3.1.3.1 Criticality Analysis

The criticality analysis allows a program to focus attention and resources on the system capabilities, mission-critical functions, and critical components that matter most. Mission-critical functions are those functions of the system that, if corrupted or disabled, would likely lead to mission failure or degradation. Mission-critical components are primarily the elements of the system (hardware, software, and firmware) that implement mission-critical functions. It can include components that perform defensive functions that protect critical components, and components that have unobstructed access to critical components.

Criticality analysis includes the following iterative steps:

- Identify and group the mission capabilities the system will perform
- Identify the system's mission-critical functions based on mission capabilities, and assign criticality levels to those functions
- Map the mission-critical functions to the system architecture and identify the defined system components (hardware, software, and firmware) that implement those functions (i.e., components that are critical to the mission effectiveness of the system or an interfaced network)
- Allocate criticality levels to those components that have been defined
- Identify suppliers of critical components.

The identified functions and components are assigned levels of criticality commensurate with the consequence of their failure of the system's ability to perform its mission, as shown in Table 3.

Table 3: Protection Failure Criticality Levels

Criticality Level	Description
Level I Total Mission Failure	Failure that results in total compromise of mission capability
Level II Significant/Unacceptable Degradation	Failure that results in unacceptable compromise of mission capability or significant mission degradation
Level III Partial/Acceptable	Failure that results in partial compromise of mission capability or partial mission degradation
Level IV Negligible	Failure that results in little or no compromise of mission capability

The criticality analysis is an iterative process. The first iteration identifies the primary critical functions. The second iteration should be completed in conjunction with the vulnerability assessment to identify functions that have unobstructed access to the critical functions. These functions have the same level of criticality as the functions they access. The third iteration identifies components which enable the critical functions (e.g., if a critical function depends on a particular software library, that library is also critical).

When identifying critical functions, associated components, and their criticality levels, programs should consider the following:

- Microelectronics and software components are especially susceptible to malicious alteration throughout the program life cycle.
- Dependency analysis should be used to identify those functions on which critical functions depend, which themselves become critical functions (e.g., defensive functions and initialization functions).
- The program should identify all access points to protect unobstructed access to critical components (e.g., implement least-privilege restrictions).

When critical functions and components have been identified through the criticality analysis, the program may use the results along with the vulnerability assessment and threat assessment to determine the security risk.

The program office should perform a criticality analysis throughout the acquisition life cycle - at a minimum, before each systems engineering technical review.

CH 9–3.1.3.2 TSN Threat Analysis

All-source intelligence is available to the PM to understand the threats to the system and the threats posed by specific suppliers. Multiple sources of intelligence can be used to feed into this analysis.

One specific source for supplier threat information is DIA's DoD Supply Chain Risk Management (SCRM) Threat Analysis Center (TAC). DoD has designated the DIA to be the DoD enterprise focal point for threat assessments needed by the PM to inform and assess supplier risks.

DIA supplier threat assessments provide threat characterization of the identified suppliers to inform risk-mitigation activities. The PM and the engineering team should use these threats assessments to assist in developing appropriate mitigations for supply chain risks. TAC requests should be submitted for all Level I and Level II critical functions and components, as identified by a criticality analysis. At a minimum, a list of suppliers of critical components should be created. TAC requests may be submitted as soon as sources of critical functions and components are identified.

The PM should request threat analysis of supply chain risk through their respective DoD Component TSN Focal Points. For the policy and procedures regarding the request, receipts, and handling of TAC reports, refer to DoDI O-5240.24. It is expected that the number of supplier threat assessment requests will grow as the criticality analysis becomes more specific and the system architecture and boundaries are more fully specified. As a result, programs should expect to submit a greater number of TAC requests between Milestones B and C (i.e., Preliminary Design Review [PDR] and Critical Design Review [CDR]).

In addition, the Technology Targeting Risk Assessment (TTRA) is a MS A requirement for all ACAT programs. For further information, refer to DAG chapter 7, section 4.3.2.

In the absence of threat information, a program should assume a medium threat for Level I and Level II critical components, in order to avoid missing an opportunity for implementing cost-effective protection measures. If a threat is not assumed for critical components, and the threat report is returned indicating a high threat, the cost to mitigate the risk posed by the threat may be prohibitive.

CH 9–3.1.3.3 TSN Vulnerability Assessment

Vulnerability is any weakness in system design, development, production, or operation that can be exploited by a threat to defeat the system's mission objectives or significantly degrade its performance. Decisions about which vulnerabilities need to be addressed and which protection measures or mitigation approaches should be applied are based on an overall understanding of risks and program priorities. The search for vulnerabilities begins with these mission-critical functions and associated critical components. The vulnerability assessment is one step in the overall TSN Analysis process and interacts with other analyses in the following ways:

- Investigation of vulnerabilities may indicate the need to raise or at least reconsider the criticality levels of functions and components identified in earlier criticality analyses.
- Investigation of vulnerabilities may also identify additional threats, or opportunities for threats, that were not considered risks in earlier vulnerability assessments.
- Vulnerabilities inform the risk assessment and the protection measure risk cost-benefit trade-off.
- Discovery of a potentially malicious source from the threat assessment may warrant additional checks for vulnerabilities in other (less-critical) products procured from that source. Therefore, threat assessments can inform vulnerability assessments.

Potential malicious activities that could interfere with a system's operation should be considered throughout a system's design, development testing, production, and maintenance. Vulnerabilities identified early in a system's design can often be eliminated with simple design changes at lower cost than if implemented later. Vulnerabilities found later may require add-on protection measures or operating constraints that may be less effective and more expensive.

Common types of vulnerabilities that can be identified by a review of system design and engineering processes are:

- Access paths within the supply chain that allow threats to introduce components that could cause the system to fail at some later time (components here include hardware, software, and firmware)
- Access paths that allow threats to trigger a component malfunction or failure at a time of their choosing
- Existence of malicious code, counterfeit hardware, or other evidence of non-genuine information and communications technology (ICT)
- Vulnerabilities within the development environment and development processes.

The supply chain here includes any point in a system's design, engineering and manufacturing development, production, configuration in the field, updates, and maintenance. Access opportunities may be for extended or brief periods. The need to protect the supply chain extends the vulnerability assessment beyond the system to the program processes and tools used to obtain and maintain the hardware, software, and firmware components used in the system.

Six techniques and tools available for identifying vulnerabilities are:

- Milestone A vulnerability assessment questionnaire: A set of 'yes' or 'no' questions that a program answers to identify vulnerabilities in the Statement of Work (SOW) and system performance specification prior to RFP release.
- Vulnerability Database Assessment: Includes the Common Attack Pattern Enumeration and Classification database (CAPEC), used for the analysis of common destructive attack patterns; the Common Weakness Enumeration database (CWE), used to examine software architecture/design and source code for weaknesses; and the Common Vulnerability Enumeration database (CVE), used to identify software vulnerabilities that enable various types of attacks.
- Static analyzers: Identify software vulnerabilities and relate the vulnerabilities to the CWE and CVE entries. Some static and dynamic analyzer tools are available that will identify specific CVE- and CWE-listed vulnerabilities. These static and dynamic analyzers from different vendors apply different criteria and often find different vulnerabilities, meaning a program should determine which analyzer(s) is best suited for its specific program needs.
- Component diversity analysis: Examines the critical function designs for common components to assess the impact of malicious insertion to a component that is used to implement multiple critical functions or sub-functions.
- Fault Tree Analysis (FTA): FTA assumes a top-down analysis that uses Boolean logic to identify system failures. An important twist in applying FTA to SSE is that the potential sources of failures are malicious actors, not random device failures. Malicious actors invalidate many assumptions made about randomness and event independence in reliability analysis. FTA assumes hypothetical system or mission failures have occurred, and traces back through the system to determine the contributing component malfunctions or failures. For a vulnerability assessment, the possible access paths and opportunities that a threat would have to exercise to introduce the vulnerability or trigger the failure should also be considered.
- Red team penetration testing: Red teams typically subject a system and the development environment under test to a series of attacks, simulating the tactics of an actual threat, to test access controls and software vulnerabilities.

Vulnerability assessment techniques are further described in the document titled *Trusted Systems and Networks (TSN) Analysis*, dated June 2014, found at the http://www.acq.osd.mil/se/initiatives/init_pp-sse.html website.

CH 9–3.1.3.4 TSN Risk Assessment

A program must perform a risk assessment (RA), at a minimum, for each Level I and Level II critical function or component identified in its criticality analysis. The criticality level generated through the criticality analysis is used to determine the risk consequence. The risk likelihood is based upon the results of the vulnerability assessment and threat assessment, or the knowledge or suspicion of threats within the supply chain and of potential vulnerabilities within supplied hardware, software, and firmware products. A simple way to translate multiple vulnerabilities into likelihood is to use an equal weighting of a

number of common vulnerabilities to create vulnerability likelihood. A similar approach is used to combine multiple threats into threat likelihood. Consider the difficulty in carrying out various cyber activities that are harmful, commensurate with threat information and potential vulnerabilities. Additional information on RAs is described in the document titled *Trusted Systems and Networks (TSN) Analysis*, dated June 2014, found at the http://www.acq.osd.mil/se/initiatives/init_pp-sse.html website.

CH 9–3.1.3.5 TSN Protection Measure Selection

TSN protection measures are cost-effective activities and attributes that manage risks to critical functions and components. They vary from process activities (e.g., using a blind buying strategy to obscure end use of a critical component) to design attributes and should be selected to mitigate a particular risk. For each protection measure being implemented, the program should identify someone responsible for its execution and a time- or event-phased plan for implementation.

A program typically selects protection measures after conducting a TSN risk assessment, although protection measures may be applied against other parts of the system, not just those identified as criticality Level I and Level II. There are “good hygiene” activities within each of the specialties described in Section 3.2 that may reduce TSN risk more broadly but may not occur as a direct result of a full TSN Analysis. The program should prepare a list of mitigations and protection measures to inform and provide options for analysis of trade-offs between cost and risk. No one set of mitigations is appropriate for all systems. The best set of mitigations and protection measures depends on a particular system--its environment, mission, and threats. Each mitigation or protection measure may have a phased implementation plan.

CH 9–3.2 SSE Specialties

This section provides an overview of the SSE specialties and how each contributes to program protection. The SSE specialties include anti-tamper, Risk Management Framework (RMF) for DoD IT, defense exportability features, hardware assurance/trusted microelectronics, software assurance, and supply chain risk management. Each specialty brings a unique perspective, methods, skills, and protections that contribute to an overall protection scheme.

In order to achieve the intended objectives of program protection, a program must select the most appropriate set of protection measures within program’s cost, schedule, performance, and other constraints.

Beyond the SSE specialties described in this section, program protection also considers protections that are implemented through security specialties. The security specialties include all the traditional aspects of security, which are usually under the responsibility of the program’s security manager. These include physical security, information security, industrial security, personnel security, and any unique security associated with certain DoD activities. These activities are typically driven by policies that aren’t directly associated with program protection. However, when selecting protection measures from the SSE specialties, a program also considers the protections resulting from implementation of these traditional security specialties.

CH 9–3.2.1 Anti-Tamper

Anti-tamper (AT) is intended to deter, prevent, delay, or react to attempts to compromise CPI in order to impede adversary countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering. Consequently, AT is driven by the CPI that is identified via the process described in Section 3.1.2. Properly implemented AT should reduce the likelihood of CPI compromise resulting from reverse engineering attacks for systems in the hands of an adversary (i.e., those lost or left on the battlefield, or exported).

Upon the identification of CPI, program management offices should contact their DoD Component Office of Primary Responsibility (OPR) for AT for guidance. Programs should expect to conduct the activities in Table 4 below to support the identification and implementation of AT requirements and delivery of AT protections. Programs should repeat this analysis when events occur that trigger a reassessment of CPI protection measures (See section 3.1.2.3).

Table 4: AT Activities Throughout the Life Cycle

Life Cycle Event	Anti-Tamper Activities
ASR	• AT requirements for the preliminary system performance specification • AT implementation costs, vulnerabilities, and its impact on system performance or maintenance • Preliminary AT requirements incorporated into TMRR System Requirement Document SRD • AT requirements and design activities in TMRR SOW
SRR	• Updated AT requirements for the system performance specification
SFR	• Updated AT requirements addressed via the System Functional Baseline • Draft AT requirements incorporated into EMD SRD • Address AT design and AT implementation activities in EMD SOW
PDR	• Updated AT requirements addressed via the Allocated Baseline
CDR	• Final AT requirements addressed via the Initial Product Baseline • AT implementation costs and residual vulnerabilities • AT Evaluation plan and execution • Final AT requirements incorporated into Production SRD • Final AT implementation activities in Production SOW
SVR/FCA, P&D and O&S Phases	• AT evaluation and associated evaluation results

To help meet these Systems Engineering and Technical Review objectives, programs must develop the AT products in Table 5 for review and concurrence by the DoD Executive Agent for AT (typically submitted as Appendix D of the PPP) or to the DoD Component OPR for Anti-Tamper (as delegated by the DoD Executive Agent for Anti-Tamper).

Table 5: Products and Timeline

AT Product:	AT Concept	Initial AT Plan	Final AT Plan	AT Evaluation Plan	AT Evaluation Report
Domestic Cases	Milestone A (105 days prior to)	PDR (60 days prior to)	CDR (60 days prior to)	CDR (60 days after)	Milestone C (60 days prior to)
Foreign Military Sales (FMS)	Letter of Offer and Acceptance Signature (105 days prior to)	PDR (60 days prior to) or 60 days post contract award	CDR (60 days prior to)	CDR (60 days after)	System Export (60 days prior to)
Direct Commercial Sales (DCS) and International Cooperative Program (IC)	Delivery of Sale Proposal or International Agreement Signature (105 days prior to)	PDR (60 days prior to)	CDR (60 days prior to)	CDR (60 days after)	System Export (60 days prior to)

Exemptions or exceptions for AT requirements must be documented, reviewed by the DoD Executive Agent for Anti-Tamper, and approved in the PPP by the MDA for the program.

The following AT reference documents are available via the DoD AT website or can be obtained through your DoD Component OPR for AT:

- AT Desk Reference: Provides programmatic guidance on AT Plan deliverables, evaluation points, schedules, and stakeholders

- AT Guidelines: Provides technical guidance on processes and methodologies for determining AT protection level requirements
- AT Security Classification Guide: Provides classification requirements for AT deliverables
- AT Plan Template: Provides the outline and guidance to assist with AT work product development

CH 9–3.2.2 Risk Management Framework for DoD IT

The Risk Management Framework for DoD IT replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life cycle cybersecurity risk to DoD IT in accordance with the National Institute of Standards and Technology (NIST) Federal Information System and Organization information system policies, DoDI 8500.01 and DoDI 8510.01.

Table 6 lists activities for PMs and SEs to incorporate the RMF for DoD IT activities into the system life cycle. For any system upgrades, a program may have to repeat analyses at all levels of detail described (ASR through SVR/FCA), at least informally, as the upgrade process progresses from requirements through production.

Table 6: RMF for DoD IT Activities Throughout the Life Cycle

Life Cycle Event	RMF for DoD IT Activities
ASR	• Categorize the information types • Select security control (SC) baseline • SC trace to the preliminary system performance specification • Incorporate SC requirements into the TMRR system performance specification and SOW
SRR	• Refine derived SC system-level requirements • Incorporate into specifications for the technical solution
SFR	• Tailor the security controls • Allocate tailored SC into system requirements • Ensure the updated tailored SC requirements are included in the system functional baseline • Incorporate CS functional requirements and verification methods into the initial Development RFP
PDR	• Tailor and Allocate SC requirements to the hardware and software design • Incorporate tailored SC requirements into system performance specification, SOW, and other contract documents for Development RFP • Align the security assessment plan with the T&E master plan to ensure inclusion of CS testing
CDR	• Tailor and Allocate SC requirements to the hardware and software design • Incorporate tailored SC requirements into system performance specification, SOW, and other contract documents for Development RFP • Align the security assessment plan with the T&E master plan to ensure inclusion of CS testing
SVR/FCA, P&D and O&S Phases	• Tailor and Allocate SC requirements to the hardware and software design • Incorporate tailored SC requirements into system performance specification, SOW, and other contract documents for Development RFP • Align the security assessment plan with the T&E master plan to ensure inclusion of CS testing

For more guidance on RMF, refer to:

- Department of the Air Force: Air Force Instruction 17-130
- Department of the Army: Guidance under development

- Department of the Navy: Secretary of the Navy Instruction 5239.3C

CH 9–3.2.3 Exportability Features

Defense exportability features include AT protection measures suitable for export and differential capability modifications, to include removal of technologies and/or capabilities that are prohibited for export. In support of program protection, defense exportability features are a means of protecting CPI in export configurations.

As early as possible, DoD program managers are encouraged to assess both: (1) the feasibility of designing and developing defense exportability features in initial designs, and, (2) the potential international demand for the system and expected benefits of foreign sales to the United States.

Early planning for defense exportability makes systems available to allies more rapidly, and at a lower cost per unit. This supports DoD's larger goal of enabling foreign sales in order to enhance coalition interoperability, decrease costs to DoD and international partners through economies of scale, and improve international competitiveness of U.S. defense systems.

For more information on defense exportability features and the associated DEF Pilot Program, refer to:

- DAG CH 1, Sections CH 1–3.4.3.7.and CH 1–4.2.8.
- USD(AT&L) Memorandum for DoD Component Acquisition Executives (CAEs), "Defense Exportability Features Policy Implementation Memorandum and Guidelines," dated April 9, 2015
- Director, International Cooperation, OUSD (AT&L) Memorandum for DoD CAEs, "Supplemental Guidance for Review and Submission of Industry Requests for an Adjusted DEF Pilot Program Cost-Sharing Portion," dated February 23, 2016.

CH 9–3.2.4 Hardware Assurance

Hardware Assurance (HwA) refers to the level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.

HwA protection measures reduce the likelihood an adversary will successfully: (1) exploit vulnerabilities built into microelectronics, their embedded software and/or intellectual property; (2) insert malicious logic in microelectronics during development, fabrication, and programming; or (3) introduce counterfeit microelectronics or unauthorized or tainted embedded software, intellectual property, or tools, into the supply chain –ultimately impacting the functionality of a microelectronics critical component.

The Program Management Office's TSN Analysis should identify if any of the following microelectronic types will be used in its program:

- Application-specific integrated circuits (ASICs) designed for a particular DoD end use
- Government-off-the-shelf (GOTS) components, designed for general military applications such as radiation hardened components or general purpose applications,
- Commercial-off-the-shelf (COTS) components, to include programmable logic devices (PLDs), field-programmable gate arrays (FPGAs), memory, and microprocessors, as well as analog to digital (A/D) and digital to analog (D/A) converters—this includes subassemblies such as cards, as well as fully assembled components. For example, FPGAs are COTS components, and the intellectual property used to program them are often COTS components as well. The intellectual property that is used can also be GOTS or custom developed.

Each type of microelectronics has a corresponding set of HwA protection measures that can be applied.

ASICs with a DoD-military end use must be acquired from a Defense Microelectronics Activity (DMEA)-accredited supplier. To ensure a trusted process flow, the PM should include a requirement in the

solicitation, which directs the use of a DMEA-accredited Trusted Supplier as well as a fully trusted flow that flows down to the Trusted Supplier's subcontracted services.

Additionally, for ASICs and GOTS, the PM, during source selection, should require that the Original Component Manufacturer (OCM) has a process for independent verification, validation, and protection of intellectual property at each phase of the design process. Opportunities to insert malicious functionality start in the design process. To guard against unintentional defects as well as malicious acts during design and fabrication, the prudent OCM will conduct inspections, tests, and independent peer reviews. Beyond that, independent verification and validation options can be pursued based on perceived residual risk. The Joint Federation Assurance Center (JFAC) can advise programs on available options to ensure hardware.

COTS microelectronics, when DoD end use is apparent, should be handled by security cleared personnel and in cleared facilities as they move through the supply chain, especially where the printed circuit board population occurs and where FPGA or other COTS microelectronics programming and software assurance are performed. The use of security keys and verification of FPGA hardware and programming are also risk mitigations for avoiding malicious reprogramming. The program office should consult with the JFAC to determine if the JFAC has assessed the COTS microelectronics that are critical components of the system, as well as any embedded software or intellectual property used for their programming. If no previous assessment has been performed, the program office should determine if the JFAC recommends that the COTS microelectronics be assessed based on use within the system. If available, program offices should consider procuring their critical components that are COTS microelectronics from the Defense Logistics Agency's Qualified Manufacturers List (QML) or Qualified Supplier List of Distributors (QSLD). For all other COTS microelectronics, programs should use OCMs or their authorized distributors to the greatest extent possible.

When practical, the SOW should include the selective use of testing techniques to test for malicious functionality. It should also require the contractor to use its configuration management, parts management, and purchasing systems to manage their sourcing decisions and custody controls for microelectronics to reduce the likelihood of them being targeted for malicious attack.

The system's design and its critical functions and components are mapped during Criticality Analysis to the contractor Bills of Material (BOM) for the system.

The contractor and component suppliers use configuration and parts management processes and purchasing systems to establish and control product attributes and the technical baseline. These processes, in combination with the critical components identified on the BOM, provide the PM with a disciplined way of coordinating Supply Chain Risk Management (SCRM) considerations, to include HwA, during microcircuit selection, acquisition, and, later on, sustainment. They also facilitate the monitoring of the supply chain for possible product or source changes requiring the reassessment of HwA risk and convey special sourcing and handling considerations, e.g., chain of custody recording and bonded storage, for critical components to the logistics and purchasing communities.

Table 7 provides an overview of HwA life-cycle activities. Used in concert with Table 9, it provides a phased list of activities/products for PMs and SEs to manage microelectronic vulnerabilities, implement procurement process activities and constraints, and systematically establish requirements to increase hardware assurance. In the Production and Deployment phase and in the Operations and Support phases, it is expected that the analysis will be updated periodically to the level of detail of the Product Baseline (the same level of detail described in the column of the table labeled 'SVR/FCA, P&D and O&S Phases'). For any system upgrades, a program may have to repeat analyses at all levels of detail described (ASR through SVR/FCA), at least informally, as the upgrade process progresses from requirements through production.

Table 7: Hardware Assurance Activities Throughout the Life Cycle

Life Cycle Event	Hardware Assurance Activities
ASR	• Identify notional critical functions to be implemented with microelectronics

Life Cycle Event	Hardware Assurance Activities
	• Establish notional HwA protection measures • Incorporate HwA protections / acceptance criteria in the SOW • Establish microelectronics component manufacturer and distributor qualification criteria and/or sources e.g., Trusted Supplier, QML, QSLD, OCM, etc.
SRR	• Ensure sources qualifications meet microelectronics criteria • For microelectronics purchases, establish HwA-related procurement practices e.g., life time buys, secured storage, selective testing of parts, etc., and criteria for manufacturers as well as the intellectual property, tools, etc., that are required to program critical components
SFR	• Identify all microelectronic critical components as well as the embedded software, intellectual property, tools, etc. used to program them • Select protection measures to include selective testing, vetting of intellectual property and tools • Update SOW for EMD phase with critical microelectronics supplier and verification and validation acceptance criteria
PDR	• Confirm use of DMEA-accredited Trusted Suppliers and trusted service flow for ASICs designed for DoD custom-end use • Confirm use of Defense Logistics Agency DLA, QML, Original Equipment Manufacturer OEM, or authorized distributor as appropriate for COTS and GOTS components • Confirm plan for use of life-time buys, secure storage and handling, and selective testing for parts where practicable; particularly for critical components • Ensure anti-counterfeit procedures, inspections, and traceability in place • Identify all microelectronic critical components as well as the embedded software, IP, tools, etc., used to program them • Confirm and revise protection measures, to include selective testing, vetting of IP and tools, etc., to be used as needed
CDR	• Update list of microelectronic critical components, to include the embedded software, Intellectual Property (IP), tools, etc., used to program them • Revise protection measures as needed • Initiate selective testing for malicious insertions where practicable, to included vetting and V&V of embedded software, IP, and tools
SVR/FCA, P&D and O&S Phases	• Update list of microelectronics critical components • Revise protection measures as needed • Continue selective testing for malicious insertions

CH 9–3.2.5 Software Assurance

Software assurance (SwA) is the level of confidence that software functions as intended and is free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the life cycle Public Law 112-239-Jan 2013 see Section 933.

Malicious code and coding defects make systems vulnerable to attacks that may cause software to fail and thus pose a significant risk to DoD warfighting missions and national security interests. These vulnerabilities in software may be difficult and even impossible to detect; adversaries actively seek to identify and use these vulnerabilities as a means of attack. Adversaries may: (1) exploit vulnerabilities inadvertently built into software; (2) exploit flaws in the architecture and design that render the system more vulnerable; (3) insert malicious logic during development, test, and operation: or (4) introduce

malicious inserts into the software supply chain. Any software, most importantly those that perform mission critical functions, can be targeted.

DoD systems incorporate an extensive amount of software; therefore, defense programs must conduct early planning to integrate software assurance protection measures to counter adversarial threats that may target that software. Of particular interest are software assurance protection measures:

- Undertaken during development, integration, and test
- Designed to mitigate attacks against the operational system (the fielded system)
- Address threats to the development environment.

A plan and statement of requirements for software assurance should be developed for the program early in the acquisition life cycle, and incorporate these requirements into the request for proposal (RFP) at each milestone. That plan should then be used by the program to track and measure SwA activities throughout the acquisition life cycle. The progress toward achieving the plan should be measured by actual accomplishments/results that are reported at each of the Systems Engineering Technical Reviews and recorded as part of the PPP.

Table 8 illustrates a sequence of acquisition activities across the life cycle for SwA. In the Production and Deployment phase, and the Operations and Support phase, it is expected that the analysis will be updated periodically to the level of detail of the Product Baseline (the same level of detail described in the column of the table labeled 'SVR/FCA, P&D and O&S Phases'). For any system upgrades, a program may have to repeat analyses at all levels of detail described (ASR through SVR/FCA), at least informally, as the upgrade process progresses from requirements through production. The SwA activities outlined in this table should be tailored to the program's specific characteristics and needs. For example, some programs may use agile and rapid development models, while other programs are structured around waterfall milestone technical/gate reviews. Automated software vulnerability analysis tools and remediation techniques should be incorporated throughout the life cycle, as required in DoDI 5000.02.

Table 8: Software Assurance Activities Throughout the Life Cycle

Life Cycle Event	Software Assurance Activities
ASR	• Identify SwA roles and responsibilities needs for the program • Contribute to selection of secure design and coding standards for the program • Identify critical functions that use software • Identify SwA activities across the system life cycle • Establish requirements to mitigate software vulnerabilities, defects, or failures based on mission risks • Incorporate SwA requirements into solicitations • Plan for SwA training and education • Develop and document an understanding of how your system may be attacked via software (i.e., attack patterns) • Plan for static analysis and other automated verification procedures and/or identify SwA service providers to assist with SwA services and when they will be performed (i.e. JFAC portal for more information)
SRR	• Select automated tools for design, vulnerability scan/analysis, etc. • Determine security requirements for programming languages, architectures, development environment, and operational environment • Develop plan for addressing SwA in legacy code • Establish assurance requirements for software to deter, detect, react, and recover from faults and attacks • Perform initial SwA reviews and inspections, and establish tracking processes for completion of assurance requirements

Life Cycle Event	Software Assurance Activities
SFR	• Assess system requirements for inclusion of SwA • Establish baseline architecture and review for weaknesses (CWEs) and susceptibility to attack (CAPEC); refine potential attack surfaces and mission impacts
PDR	• Review architecture and design against secure design principles, which include system element isolation, least-common mechanism, least privilege, fault isolation, input checking, and validation • Determine if initial SwA Reviews and Inspections received from assurance testing activities are documented • Confirm that SwA requirements are mapped to module test cases and to the final acceptance test cases • Establish automated regression testing procedures and tools as a core process
CDR	• Enforce secure coding practices through Code Inspection augmented by automated Static Analysis Tools • Detect vulnerabilities, weaknesses, and defects in the software; prioritize; and remediate • Assure chain-of-custody from development through sustainment for any known vulnerabilities and weaknesses remaining and mitigations planned • Assure hash checking for delivered products • Establish processes for timely remediation of known vulnerabilities (e.g., CVEs) in fielded COTS components • Ensure planned SwA testing provides variation in testing parameters, e.g., through application of Test Coverage Analyzers • Ensure program critical function software and Critical Components receive rigorous test coverage
SVR/FCA, P&D and O&S Phases	• Verify test resources and test cases, test scenarios and test data • Continue to enforce secure design and coding practices through inspections and automated scans for vulnerabilities and weaknesses • Maintain automated code vulnerability scans, reporting, prioritization, and execute defect remediation plans • Maintain and enhance automated regression tests and employ Test Coverage Analyzers to increase test coverage • Conduct periodic penetration tests using the enhanced automated test coverage • Monitor evolving threats and attacks, respond to incidents and defects, identify and fix vulnerabilities, and incorporate SwA enhancing upgrades. PMO should provide plan for updates, replacements, maintenance, or disposal of CPI, critical components, and critical functions software • Ensure chain-of-custody across development, from development to sustainment, and during sustainment for the record of weaknesses and vulnerabilities remaining and mitigations planned

Additional references and resources for developing a SwA strategy for DoD systems and technologies include:

- Joint Federated Assurance Center (JFAC), April 2016: The JFAC website, https://jfac.army.mil contains a growing body of knowledge, service-providing activities, tools, contracts, and help supporting the Department's use of SwA (DoD CAC required).
- State of the Art Resource (SOAR) for Software Vulnerability Detection, Test, and Evaluation: Discusses families of tools available for use in the implementation of SwA across the life cycle.

- Software State of the Art Matrix: Outlines the intended uses of various families of tools and the vulnerabilities they detect.
- DoD SwA Countermeasures White Paper, March 2014: The purpose of the software assurance protection measures section of the Program Protection Plan (PPP) is to help programs develop a plan and statement of requirements for SwA early in the acquisition life cycle and to incorporate the requirements into the request for proposals.
- Defense Information Agency (DISA) Security Technical Implementation Guides (STIGs), May 2015: The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to malicious attack.
- Open Web Application Security Project (OWASP): The OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain trustworthy applications.
- Build Security In Security Model (BSIMM), 2015: The BSIMM is designed to help you understand, measure, and plan a software security initiative.
- Common Weaknesses and Enumeration (CWE) Portal, A community-developed dictionary of software weaknesses and types. (CVE, CAPEC)
- DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, June 2015

CH 9–3.2.6 Supply Chain Risk Management

DoD systems and networks rely extensively on commercial, globally interconnected, and sourced components, which, while providing numerous benefits, also create opportunities for adversaries to intentionally affect mission-critical components while they are in the supply chain. Supply Chain Risk Management (SCRM) is a means for understanding and managing these supplier risks, and for identifying practices that reduce the risk of malicious or subversive exploitation of mission-critical components intended to affect component performance, as well as the risks posed by inherent vulnerabilities in the supply chain.

To effectively manage supply chain risks, programs should develop a set of SCRM practices and protection measures to minimize intentional malicious activities as well as to detect and respond to supply chain attacks. These practices and protections are procurement activities as well as HwA and SwA activities for critical components in the system.

PMs should implement practices and protection measures to the contractor in the solicitation through requirements in the Statement of Work (SOW) – during every phase of the lifecycle. Example protection measures include use of secure shipping practices, limiting component access to cleared personnel, and hiding the intended end use of the component.

Table 9 provides activities for PMs and SEs to assess supply chain vulnerabilities and implement processes to increase the security of the supply chain. In the Production and Deployment and in the Operations and Support phases, it is expected that the analysis will be updated periodically to the level of detail of the Product Baseline (the same level of detail described in the column of the table labeled 'SVR/FCA, P&D and O&S Phases'). For any system upgrades, a program may have to repeat analyses at all levels of detail described (ASR through SVR/FCA), at least informally, as the upgrade process progresses from requirements through production.

Table 9: SCRM Activities Throughout the Life Cycle

Life Cycle Event	SCRM Activities
ASR	• Identify supply chain threat mitigation practices for system critical functions • Incorporate SCRM practices into the SOW
SRR	• Refine supply chain practices • Update supply chain vulnerabilities • Update SCRM practices within the SOW

Life Cycle Event	SCRM Activities
	• Update and elaborate System SCRM requirements
SFR	• Identify SCRM requirements for identified critical functions. • Include SCRM-related design requirements into system functional baseline
PDR	• Identify SCRM requirements for specific components implementing critical functions • Incorporate SCRM process and system requirements into system performance specification, SOW, and other contract documents for Development RFP
CDR	• Reassess supply chain vulnerabilities • Update SCRM requirements for components based on the maturation of the system design • Update system performance specification and relevant documents for future contract releases to reflect updated SCRM requirements
SVR/FCA, P&D and O&S Phases	• Analyze component changes and assess supply chain risks associated with any tech refreshes • Update SCRM-related procurement, process, and system requirements in necessary contract documents

For more guidance on SCRM practices, see NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

CH 9–3.3 Engineering Design Activities

The program protection analyses and effort within each SSE specialty provide the requisite knowledge for identifying risks and selecting protections. These analyses have to be translated into an effective set of engineering requirements and reflected in the design. One way of ensuring that security is properly incorporated into the system is through secure design principles, as discussed in Section 3.3.1. Additionally, decisions related to protection-measure selection should be driven by trade-off analyses (Section 3.3.2), just as it is for any other design considerations.

CH 9–3.3.1 Secure Design Principles

Sufficiently mitigating program protection related risks is more successful and cost-effective if security is thoughtfully considered throughout the design process. One means of ensuring this is adhering to a set of secure design principles. As a design consideration, system security engineering's best practices include ensuring the system architecture and design address how the system:

- Manages access to, and use of the system and system resources
- Is configured to minimize exposure of vulnerabilities that could impact the mission, including techniques such as design choice, component choice, security technical implementation guides, and patch management in the development environment (including integration and T&E), in production, and throughout sustainment;
- Is structured to protect and preserve system functions or resources, e.g., through segmentation, separation, isolation, or partitioning;
- Monitors, detects, and responds to security anomalies;
- Maintains priority system functions under adverse conditions;
- Interfaces with DoD Information Network or other external security services.

CH 9–3.3.2 SSE Trade-off Analyses

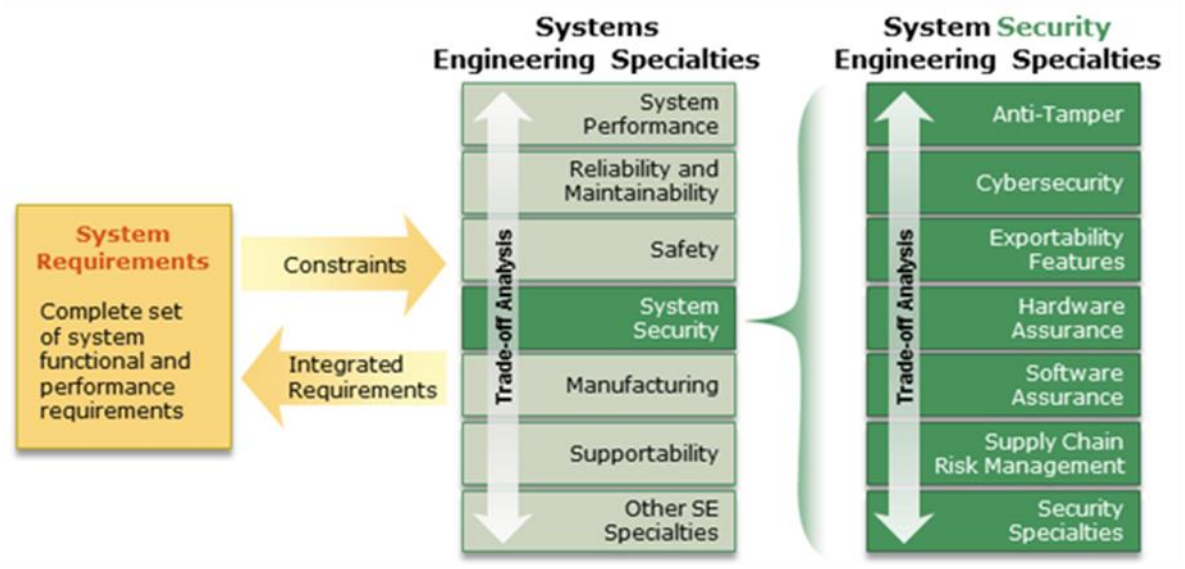
Program protection provides the means for analyzing and integrating the protections offered by each system security engineering (SSE) specialty (see Section 3.2 for more on SSE specialties) to determine the most appropriate set of protection measures within the given constraints.

The typical method used for performing this analysis and integration is trade-off analyses. Trade-off analysis can help engineers make tough choices among competing system requirements in order to design an end solution within the constraints of cost, schedule, and performance while still maintaining an acceptable level of risk.

There are two levels of trade-off analyses that include system security (as shown in Figure 4):

- At the SSE-level, the system security engineer performs trade-off analyses to integrate the proposed protection measures from each SSE specialty into a single set of protection measures that most cost-effectively addresses the risks identified through program protection. This set becomes the SSE input to the SE's analysis.
- At the system-level, the SE performs trade-off analyses to balance overall system performance, system attributes/design considerations (which includes SSE as one consideration), cost, and schedule.

Figure 4: SSE Trade-off Analysis



There may be multiple iterations of these analyses, as the initial SSE input (or portions of it) to the SE's analysis may be deemed unacceptable. This places a new constraint on the system security engineer, and means that the SSE-level analysis must be adjusted for this new constraint. This integration occurs regularly across the life cycle, as protection measures decisions will be affected as the design matures.

CH 9–3.4 SSE Activities in the Life Cycle

SSE activities analyze the threats, vulnerabilities, risks, and risk mitigations to CPI, mission-critical functions and critical components, and program and system information, with the results of these activities documented in the Program Protection Plan. The level of detail expected is commensurate with the level of the system specification, design, and implementation.

- Section 3.4.1 provides an overview of life-cycle expectations for program protection and system security engineering (SSE).
- Section 3.4.2 provides overviews of Program Protection and SSE expectations for each of the phases leading up to a major program Milestone. This security-specific material builds on the systems engineering activities, processes, input/output, and expectations described in DAG CH 3, Sections 3.2.1 to 3.2.6.
- Section 3.4.3 focuses on specific SSE objectives that should be met at technical reviews and audits, in which the protections are applicable.

CH 9–3.4.1 Life Cycle Expectations

The Program Protection Plan (PPP) is a living document, required at Milestones A, B, C, the Development RFP Decision Point, and the Full-Rate Production Decision Review or Full Deployment Decision Review as described in DoDI 5000.02 It is a best practice to update the PPP after any contract award to reflect the contractor's approved technical approach, before export decisions, through operations and sustainment; and to report progress at each technical review event.

Key SSE criteria can be specified for each of the phases leading up to a major program milestone, and it is important to establish these criteria across the full life cycle in order to build security into the system. Life cycle considerations, in general, include the following:

- Iteratively perform program protection analyses described in Sections 3.1 through 3.3 to assess and manage system and program security risks.
  - Determine mitigation approaches to address process vulnerabilities and design weaknesses.
  - Identify and implement protection measures.
  - Perform cost/benefit trade-offs where necessary.
- Integrate security into requirements and SE processes.
  - Integrate security requirements into the evolving system designs and baselines.
  - Use secure design considerations to inform life cycle trade-space decisions.
- Incorporate security requirements, processes, and protection measures into each contract throughout the acquisition life cycle. This includes relevant content in statements of work and the system performance specification, as described in Section 4.2.
- Identify life cycle resources needed to ensure sustainability of protection measures in operations.

CH 9–3.4.2 Activities in Life Cycle Phases

Within each phase of the acquisition life cycle, program protection activities and outcomes are driven by the maturity of the system. As the system matures, program protection analyses are iteratively updated and support the development of Program Protection Plans for each milestone and the appropriate milestone decisions.

CH 9–3.4.2.1 Pre-Materiel Development Decision

Based on the technical maturity of the system, the focus of program protections to begin to identify system security risks is based on the range of candidate materiel solution approaches. This program protection information supports the Milestone Decision Authority's (MDA) decision to authorize entry into the acquisition life cycle and pursue a materiel solution. A program protection plan is not required for the Materiel Development Decision.

CH 9–3.4.2.2 Materiel Solution Analysis Phase

Based on the technical maturity of the system, the focus of the program protection plan is to describe and document the plan, repeatable processes and methodologies, and resources to identify and mitigate system security risks. This key program protection information supports the Milestone A decision by providing evidence that the program has adequately addressed system security risks, given the technical maturity point.

During this phase, the program is required to develop an MDA-approved PPP for the Milestone A decision, which meets the SSE objectives described in the Alternative Systems Review section, Section 3.4.3.1. Additionally, the program office should incorporate generic program protection language into system performance specification and Statement of Work (SOW) during the development of draft Request for Proposal (RFP) in support of Technology Maturity and Risk Reduction phase (see Section 4.2)

CH 9–3.4.2.3 Technology Maturation and Risk Reduction Phase

Based on the technical maturity of the system, the focus of the program protection plan is to describe and document the plan, repeatable processes and methodologies, analyses performed, and resources to identify and mitigate system security risks. This is key program protection information to support the

Milestone B decision by providing evidence that the program has adequately addressed system security risks, given the technical maturity point.

During this phase, the program is required to develop an updated DoD Component-approved draft PPP for the Development RFP Release Decision Point that meets the SSE objectives described in the System Requirements Review section, Section 3.4.3.2, as well as the System Functional Review section, Section 3.4.3.3. The program is also required to develop an updated MDA-approved PPP for the Milestone B decision, which meets the SSE objectives described in the Preliminary Design Review (PDR) section, Section 3.4.3.4, even if the program did not conduct a formal system-level PDR prior to the milestone.

Additionally, the program office should incorporate program protection language into the system performance specification and SOW during development of the RFP in support of the Engineering and Manufacturing Development phase and Low Rate Initial Production (if applicable) (see Section 4.2)

CH 9–3.4.2.4 Engineering and Manufacturing Development Phase

Based on the technical maturity of the system, the focus of the program protection plan is to describe and document the plan, repeatable processes and methodologies, analyses performed, and resources to identify and mitigate system security risks. This key program protection information supports the Milestone C decision by providing evidence that the program has adequately addressed system security risks, given the technical maturity point.

During this phase, the program is required to develop an updated MDA-approved PPP for the Milestone C decision that meets the SSE objectives described in the Critical Design Review (CDR) section, Section 3.4.3.5, even if the program did not conduct a formal CDR. It is also required to develop a System Verification Review/Functional Configuration Audit section, Section 3.4.3.6. In addition to the PPP, other deliverables that require updated system security material include the SEP, TEMP, System Threat Assessment, and Risk Assessment. Intermediate products, such as the product requirements and architecture, should be delivered and maintained as part of the products of system development, so they can be used in later system maintenance. This helps provide the traceability to maintain the system's security.

Additionally, the program office should incorporate program protection language into the system performance specification and SOW during development of the RFP in support of the Production and Deployment phase (see Section 4.2)

CH 9–3.4.2.5 Production and Deployment Phase

Based on the technical maturity of the system, the focus of the program protection plan is to describe and document the plan, repeatable processes and methodologies, analyses performed, and resources to identify and mitigate system security risks. This is key program protection information to support the FRP or FDD decision by providing evidence that the program has adequately addressed system security risks given the technical maturity point.

During the Production and Deployment phase, the program is required to develop an updated PPP for the Full Rate Production Decision Review (FRP DR) or Full Deployment Decision Review (FD DR) that reflects the Physical Configuration Audit (PCA)-verified Product Baseline. This update to the PPP should include content to the level of detail provided in the Bill of Material (BOM) as well as the SSE objectives described in the Physical Configuration Audit section, Section 3.4.3.8. The PPP should describe plans to phase in any needed system security risk mitigation. Further updates to the PPP should be incorporated, based upon updated threat, vulnerability, and BOM changes prior to Initial Operational Capability (IOC) and Full Operational Capability (FOC).

Additionally, the program office should incorporate program protection language into the system performance specification and SOW during the development of the RFP in support of the FRP DR or FD DR (see Section 4.2)

CH 9–3.4.2.6 Operations and Support Phase

While the primary emphasis of program protection is on the design and acquisition phases of a system life cycle, sustainment considerations should be addressed for the protection profile to secure the system

throughout operations. Repair depots, for example, should be aware of CPI, mission-critical functions and components, as well as program and system information on systems they are maintaining so that the depots can appropriately protect these items from compromise and unauthorized disclosure.

Sustainment planning and execution seamlessly span a system's entire life cycle, from Materiel Solution Analysis to disposal. Sustainment planning should be flexible, using a criticality analysis focus, and reflect an evolutionary approach; it should accommodate modifications, upgrades, and re-procurement. The sustainment plan should be a part of the program's Acquisition Strategy and integrated with other key program planning documents as appropriate (e.g. PPP and Life Cycle Sustainment Plan).

CH 9–3.4.3 Technical Review and Audits

To design for security, the program incorporates program protection planning and execution activities in systems engineering technical reviews and audits.

Systems Engineering technical reviews and audits provide a key Systems Engineering health and risk assessment tool that is discussed in detail in CH 3 Section 3.3.

The following subparagraphs provide system security engineering (SSE) criteria, recommended as systems engineering technical review and audit entrance/exit criteria, in order to assess and ensure that an appropriate level and discipline of SSE activities are conducted across the full system context.

CH 9–3.4.3.1 Alternative Systems Review

The objectives for the Alternative Systems Review (ASR) are defined in Table 10 (from Chapter [CH] 3, Table 12). For a full description of ASR responsibilities, inputs and outputs, see CH 3 Section 3.3.1.

Table 10: ASR Objective (From CH 3-3.1. Table 12)

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
Alternative Systems Review (ASR)	Recommendation that the preferred materiel solution can affordably meet user needs with acceptable risk	System parameters defined; balanced with cost, schedule, and risk	Initial system performance established and plan for further analyses supports Milestone A criteria

At the technical maturity point associated with the ASR a program should have accomplished the following SSE objectives:

- Completed initial identification of program information classification and marking requirements (more information available in DAG Section 3.2.1).
- Completed an initial assessment of potential classified information and an initial CPI Analysis.
- Completed an initial Trusted Systems and Networks (TSN) Analysis, including the following:
  - An initial criticality analysis, threat assessment, and vulnerability assessment, performed with a focus on malicious insertion to the level of detail commensurate with mission-level functional requirements
  - An initial risk assessment and set of risk mitigations (protection measures) based upon the criticality analysis, threat assessment, and vulnerability assessment; these assessments include a focus on supply chain risk management (SCRM) and software assurance.
- Identified an initial set of risk mitigations (protection measures) for CPI and critical functions and incorporated the mitigations into the system requirements and into the system processes (e.g., procurement, configuration management, design, maintenance, and sustainment)
- Established plans to protect processes, tools, information elements, data, potential CPI and critical functions.

CH 9–3.4.3.2 System Requirements Review

The objectives for the System Requirements Review (SRR) are defined in the Table 12. For a full description of SRR responsibilities, inputs and outputs, see CH 3 Section CH 3–3.3.2.

Table 11: SRR Objective (From CH3-3.1. Table 12)

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
System Requirements Review (SRR)	Recommendation to proceed into development with acceptable risk	Level of understanding of top-level system/ performance requirements is adequate to support further requirements analysis and design activities.	Government and contractor mutually understand system /performance requirements including: (1) the preferred materiel solution (including its support concept) from the Materiel Solution Analysis (MSA) phase; (2) plan for technology maturation; and (3) maturity of interdependent systems.

At the technical maturity point associated with the SRR, a program should have accomplished the following SSE objectives:

- Addressed plans to protect CPI, critical functions/components, processes, tools, information elements, and data as part of the system requirements, Statement of Work (SOW), and solicitation.
- Completed a CPI Analysis, including as a minimum:
  - Identification of CPI
  - An assessment of the risk of CPI compromise, loss, or alteration
  - Determination of risk mitigations (protection measures)
- Completed a Trusted Systems and Networks (TSN) Analysis, including all the steps of the SSE risk management process:
  - Updated the criticality analysis, threat assessment, and vulnerability assessment with a focus on malicious insertion to the level of detail commensurate with the system performance specification.
  - Updated the risk assessment, a set of risk mitigations (protection measures), and a trade-off analysis to determine which risk mitigations are to be implemented in the system requirements.
  - Implemented relevant SCRM key practices on critical microelectronic components identified during criticality analysis.
- Completed an integrated security risk assessment including the risk of information exposure, technology and CPI compromise, and supply chain risk management (includes HwA and SwA).
- Considered security requirements in the development of the system performance requirements and non-tailorable design requirements.

CH 9–3.4.3.3 System Functional Review

The objectives for the System Functional Review (SFR) are defined in Table 12. For a full description of SFR responsibilities, inputs and outputs, see CH 3 Section 3.3.3.

Table 12: SFR Objective (From CH3-3.1. Table 12)

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
System Functional Review (SFR)	Recommendation that functional baseline satisfies performance requirements and to begin preliminary design with acceptable risk.	Functional baseline established and under formal configuration control. System functions in the system performance specification decomposed and defined in specifications for lower level elements, that is, system segments and major subsystems.	Functional requirements and verification methods support achievement of performance requirements. Acceptable technical risk of achieving allocated baseline. See Ch 3 Section 4.1.6 Configuration Management Process for a description of baselines.

At the technical maturity point associated with the SFR, a program should have accomplished the following SSE objectives:

- Addressed plans to protect CPI, critical functions/components, processes, tools, information elements, and data as part of the system requirements.
- Completed an updated CPI Analysis, including as a minimum:
  - Identification of CPI
  - An assessment of the risk of CPI compromise, loss, or alteration
  - Determination of risk mitigations (protection measures)
- Completed an updated TSN Analysis, including all the steps of the TSN risk management process:
  - Updated the criticality analysis, threat assessment, and vulnerability assessment with a focus on malicious insertion to the level of detail commensurate with the SFR system specification and design.
  - Updated the risk assessment, a set of risk mitigations (protection measures) and a trade-off analysis to determine which risk mitigations are to be implemented in the system requirements and processes.
- Implemented relevant SCRM key practices on critical microelectronic components identified during criticality analysis.
- Identified an updated set of risk mitigations (protection measures) for CPI and critical functions and has incorporated them into the subsystem and component requirements and into the system processes (e.g., procurement, configuration management, design, maintenance, and sustainment).
- Traced system security requirements to lower-level elements for all risk mitigations, to include requirements for classified information elements and applicable security controls.
- Established secure design and coding standards.
- Established an inter-organizational agreement for suppliers to notify entities affected by supply chain compromises.

CH 9–3.4.3.4 Preliminary Design Review

The objectives for the Preliminary Design Review (PDR) are defined in Table 13. For a full description of PDR responsibilities, inputs and outputs, see CH 3 Section 3.3.4.

Table 13: PDR Objective (From CH3-3.1. Table 12)

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
Preliminary Design Review (PDR)	Recommendation that allocated baseline satisfies user requirements and developer ready to begin detailed design with acceptable risk.	Allocated baseline established such that design provides sufficient confidence to proceed with detailed design. Baseline also supports 10 USC 2366b certification, if applicable.	Preliminary design and basic system architecture support capability need and affordability goals and/or caps achievement. See Ch 3 Section 4.1.6 Configuration Management Process for a description of baselines.

At the technical maturity point associated with the PDR, a program should have accomplished the following SSE objectives:

- Addressed plans to protect CPI, critical functions/components, processes, tools, information elements, and data as part of the system requirements, SOW, and solicitation
- Completed an updated CPI Analysis, including as a minimum:
  - Identification of CPI
  - Assessment of the risk of CPI compromise, loss, or alteration
  - Determination of risk mitigations (protection measures)
- Completed an updated TSN Analysis, including all the steps of the SSE risk management process:
  - Updated the criticality analysis, threat assessment, and vulnerability assessment with a focus on malicious insertion to the level of detail commensurate with the PDR system specification and design.
  - Updated the risk assessment, a set of risk mitigations (protection measures), and a trade-off analysis to determine which risk mitigations are to be implemented in the system requirements and processes.
- Implemented relevant SCRM key practices on critical microelectronic components identified during criticality analysis.
- System security requirements (including all protection measures/mitigations) have been traced to lower-level elements in the preliminary design (hardware – verifiable component characteristics; software – computer software components (CSC); computer software units (CSU); and the required security controls).
- Incorporated secure design and coding standards.
- Identified an updated set of risk mitigations (protection measures) for CPI and critical functions and incorporated these into preliminary design.
- Verified that there is an inter-organizational agreement for suppliers to notify entities affected by supply chain compromises

CH 9–3.4.3.5 Critical Design Review

The objectives for the Critical Design Review (CDR) are defined in Table 14. For a full description of CDR responsibilities, inputs, and outputs, see CH 3 Section 3.3.5.

Table 14: CDR Objective (From CH3-3.1. Table 12)

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
Critical Design Review (CDR)	Recommendation to start fabricating, integrating,	Product design is stable. Initial product baseline established.	Initial product baseline established by the system detailed design

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
	and testing test articles with acceptable risk.		documentation; affordability/should-cost goals confirmed. Government assumes control of initial product baseline as appropriate. See Ch 3 Section 4.1.6 Configuration Management Process for a description of baselines.

At the technical maturity point associated with the CDR, a program should have accomplished the following SSE objectives:

- All system security requirements traced among the Functional, Allocated, and the Initial Product Baseline are complete, consistent, and incorporate measures to protect CPI, mission-critical functions and critical components, processes, tools, information elements, and data.
- Completed an updated CPI Analysis.
- Completed an updated Trusted Systems and Networks (TSN) Analysis.
- Implemented relevant SCRM key practices on critical microelectronic components identified during criticality analysis.
- Completed an updated risk assessment that reflects system security risks and status and updated these in the program's Risk Register/Database, reviewed to include the risks identified in the RMF Security Assessment Report (SAR), where applicable.
- Updated the Cost Analysis Requirements Description (CARD) based on the system product baseline, which reflects system security-related components.
- Updated the program schedule and critical path drivers to reflect all system security events
- Reviewed security-related test criteria for completion status.
- Reviewed DT&E assessments of cybersecurity T&E status, where applicable.
- Reviewed a draft Security Assessment Plan for needed remediation actions as input to the Security Assessment report to achieve Authorization to Operate (ATO).

CH 9–3.4.3.6 System Verification Review/ Functional Configuration Audit

The objectives for the System Verification Review (SVR) are defined in Table 15. For a full description of SVR responsibilities, inputs, and outputs, see CH 3–3.3.6.

Table 15: SVR Objective (From CH 3-3.1. Table 12)

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
System Verification Review (SVR)/Functional Configuration Audit (FCA)	Recommendation that the system as tested has been verified (i.e., product baseline is compliant with the functional baseline) and is ready for validation (operational assessment) with acceptable risk.	System design verified to conform to functional baseline.	Actual system (which represents the production configuration) has been verified through required analysis, demonstration, examination, and/or testing. Synonymous with system-level Functional Configuration Audit (FCA). See Ch 3 Section 4.1.6 Configuration

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
			Management Process for a description of baselines.

At the technical maturity point associated with the SVR, a program should have accomplished the following SSE objectives:

- Completed an updated CPI Analysis.
- Completed an updated Trusted Systems and Networks (TSN) Analysis, including all the steps of the SSE risk management process based on the system as tested and associated documentation. Include other specialized analysis such as fault tree analysis (FTA) and AT to identify derived system architecture and behavior changes.
- Established review criteria to specifically examine functionality of program protection requirements implemented in the system as tested.
- Assigned that audit personnel fully reflect the security disciplines necessary to assess all program protection measures implemented in the system as tested.
- Ensured that the program's non-recurring SSE requirements are executable with the existing budget.
- Program protection risks are known and being appropriately managed to an acceptable level of risk and residual risks identified.
- Verified the system through required analysis, demonstration, and testing (including blue/red team and penetration testing where applicable) after fully implementing all protection measures with results that indicate readiness for operational test and evaluation success (operationally effective and suitable).
- Fully documented, funded, and staffed life cycle sustainment protection measures for CPI and its critical function/component, including but not limited to software and cybersecurity vulnerability management, incident response, SCRM, and AT protections.

CH 9–3.4.3.7 Production Readiness Review

The objectives for the Production Readiness Review (PRR) are defined in Table 16. For a full description of PRR responsibilities, inputs, and outputs, see CH 3–3.3.7.

Table 16: PRR Objective (From DAG CH3-3.1. Table 12)

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
Production Readiness Review (PRR)	Recommendation that production processes are mature enough to begin limited production with acceptable risk.	Design and manufacturing are ready to begin production.	Production engineering problems resolved and ready to enter production phase.

At the technical maturity point associated with the PRR, a program should ensure that the same set of objectives as described in the SVR/FCA is appropriately updated.

CH 9–3.4.3.8 Physical Configuration Audit

The objective for the Physical Configuration Audit (PCA) is defined in Table 17. For a full description of PCA responsibilities, inputs, and outputs, see CH 3–3.3.8.

Table 17: PCA Objective (From CH3-3.1. Table 12)

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
Physical Configuration Audit (PCA)	Recommendation to start full-rate production and/or full deployment with acceptable risk.	Product baseline established. Verifies the design and manufacturing documentation, following update of the product baseline to account for resolved OT&E issues, matches the physical configuration.	Confirmation that the system to be deployed matches the product baseline. Product configuration finalized and system meets user's needs. Conducted after OT&E issues are resolved. See Ch 3 Section 4.1.6 Configuration Management Process for a description of baselines.

At the technical maturity point associated with the PCA, a program should have accomplished the following SSE objectives:

- Ensured that counterfeit/substandard hardware/software components for CPI and critical components are not incorporated into the final system
- Ensured that any assurance-specific audits have been completed and documented
- Ensured that any source code delivered is actually the source code used by the system (where it is claimed to be)
- Ensured that packaging includes relevant seals to verify authenticity and impede tampering.

CH 9–4. Additional Planning Considerations

As a systems engineering design consideration, the activities to execute system security engineering and program protection are closely coupled with the systems engineering efforts. As with systems engineering, there are links between program protection and other key aspects of defense acquisition. This Section provides information on how program protection informs or is informed by other aspects of defense acquisition. It also provides additional program protection considerations that are unique to specific acquisition models or system domains.

- Section 4.1 addresses how program protection is incorporated into solicitations and contracts.
- Section 4.2 discusses the complementary relationship between program protection and test and evaluation (T&E).
- Section 4.3 addresses the influence of program protection on lifecycle sustainment planning.
- Section 4.4 addresses how intelligence and counterintelligence activities support program protection decisions.
- Section 4.5 addresses the Joint Federated Assurance Center (JFAC) and the ways programs can utilize the JFAC as part of their program protection activities.

CH 9–4.1 Contracting for Program Protection

The Systems Engineering (SE) role in contracting is described in CH 3–2.7. As part of this comprehensive SE role, the system security engineer has a key role in ensuring that program protection-related requirements (i.e., features in the system design, methods and processes used to develop the system) are included in contracts and solicitations. The content of the most current Program Protection Plan (PPP) and related analysis is used to drive the content of the Request for Proposal (RFP).

The results of each analysis are used to create the system performance specification protection measure requirements and the SOW protection measure requirements for the RFP. It is a best practice to include these requirements in the program/project's initial RFP issued for the system and then provide updates for subsequent RFPs. In cases where the design is not yet defined, the program protection requirements will

mostly be in the form of Statement of Work (SOW) tasks that require the contractor to perform program protection methods to determine the needed system protection features.

Contents to be incorporated into the RFP include:

- Requirements derived from protection measures need to be incorporated into the System Requirements Document (SRD) and the SOW.
- PPP analysis activities, performed in parallel with the contractor's design and development, need to be incorporated as contractor activities into the SOW.
- When program protection needs to be a factor in source selection, add the necessary program protection topics to Section L and the associated evaluation criteria to Section M of the RFP.

RFPs may be issued for each phase of the Acquisition Life Cycle. The SE and system security engineering (SSE) technical content of the RFP is aligned to the SE baselines established at the most recent SE technical review. The RFP for each phase is often developed during the preceding phase.

Section C: Description/Specification/Work Statement. The following is a list of the ways in which protection measures are incorporated into Section C of the RFP:

- Protection measures that specify what the system will do are added to the SRD in the form of system requirements.
- Protection measures that describe how the contractor will develop the system (i.e., supply chain protections or software development standards) are added to the SOW in the form of SOW statements.
- Protection measures that describe program protection analysis (CPI and TSN) to be performed during the contract to identify additional protection measures are also added to the SOW as SOW statements.
- Protection measures that require supporting documentation to be provided to the government become a Contract Data Requirements List (CDRL), with a Data Item Description (DID) to explain the expected content. (The CDRL and DID are included in Section J, Exhibit A.)

Section I: Contract Clauses. Include the relevant DFARS clauses in Section I of the RFP. One particular clause is DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, which requires that:

- DoD and its contractors and subcontractors protect unclassified covered defense information, which includes unclassified controlled technical information, residing on their unclassified information systems
- Contractors report cyber incidents (e.g., unauthorized access and disclosure, lost media, denial of service) that affect unclassified covered defense information resident on or transiting the contactor's information system.

Per DFARS Subpart 204.73, all DoD solicitations and contracts are to include DFARS 252.204-7012, which sets forth the reporting criteria and requirements for safeguarding certain types of unclassified information, collectively referred to in the clause as Covered Defense Information (CDI).

Section I may also include DFARS clause 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System, which addresses contractor responsibilities for detecting and avoiding the use or inclusion of counterfeit electronic parts, the use of trusted suppliers, and the requirements for contractors to report counterfeit electronic parts and suspect counterfeit electronic parts.

This section may also include FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems, which requires contractors to limit information system access to authorized users and to control information posted or processed on publicly accessible information systems.

This section may also include FAR Clause 52.204-2 for contracts handling classified information.

Section J: List of Documents, Exhibits, and Other Attachments. Section J will list the attachments for the RFP and Exhibit A (CDRLs) for the entire contract. In each CDRL, the government indicates the distribution statement with which the contractor's deliverable is to be marked. Specifically for system security, the National Industrial Security Program Operating Manual (NISPOM) requires the government to include DD Form 254 (included as an exhibit and listed in Section J: List of Attachments), which defines to the contractor (or subcontractor) the security requirements and classification guidance that are necessary to perform on a classified contract. DD Form 254 requires that the contractor:

- Protect all classified information to which they have access or custody. A contractor performing work within the confines of a federal installation should safeguard classified information according to the procedures of the host installation or agency.
- Appoint a U.S. citizen employee, who is cleared as part of the facility clearance to be the facility security officer (FSO). The FSO will supervise and direct security measures necessary for implementing the applicable requirements from this manual, and related federal requirements for classified information.

Section L: Instructions, Conditions, and Notices to Offerors. Section L may request descriptions of the offeror's approach to program protection or to a specific aspect of program protection. For example, the following statement will allow the government to assess each competitor's approach to program protection and factor it into the source selection:

- For level I and level II critical functions and components the offeror should describe the approach to implementing protection measures and secure designs.

Alternatively, a narrower focus may be used in order for the government to assess each offeror's approach more comprehensively for areas of particular concern (e.g., SwA). The offeror should describe their approach to software assurance. At a minimum, the contract should describe its approach to:

- Secure design and coding standards
- Secure design and code inspections
- Static analysis tools
- Attack definition, weaknesses, and vulnerabilities
- Penetration testing
- Security monitoring and response

A set of generic RFP language is contained in a document titled "Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals."

CH 9–4.2 T&E for Program Protection

The results of program protection analyses, which are documented in the PPP, may generate requirements that should be addressed by T&E. T&E personnel, led by the chief developmental tester (or equivalent), use the PPP and other system artifacts (such as the system design, system performance specifications, or statement of work activities) as references for developing test plans and test resource and capability requirements, and other information relating to testing and evaluation of the system. This information should be detailed in the Test and Evaluation Master Plan (TEMP).

One key aspect of T&E documentation in this area is the Developmental Evaluation Framework. The Developmental Evaluation Framework has four major areas. One of these areas is titled Cybersecurity. The categories underneath the Cybersecurity area are flexible and can be defined in any way necessary to meet program needs.

The system security engineer and DT&E test lead cooperate throughout the Acquisition Life Cycle to refine requirements and test plans, beginning before Milestone A. The system security engineer provides input to the DT&E test lead as system requirements are defined. The DT&E test lead uses those requirements to define needed testing and resources. The PPP informs the DT&E test lead's understanding of system requirements, including critical functions, and components and software

vulnerabilities. When developmental testing begins, the DT&E test lead provides the system security engineer with test results, which should be analyzed to determine if the products work as specified. Analysis may suggest the need to refine requirements or make engineering changes to improve program protection.

CH 9–4.3 Life-Cycle Sustainment Planning for Program Protection

Addressing the security of a program and system does not stop once development ends. The threat environment, vulnerabilities, supply chains, and other components are constantly changing, impacting the security risk to the warfighter. Although there is no requirement to develop a Program Protection Plan (PPP) after the FRP or FD Decision Review point, all PPPs up to that point should have included plans for maintaining and updating protection measures throughout the life cycle. It is also best practice for a program to maintain and update the PPP as necessary to account for changes in the program and system (e.g., changes to a supplier of a critical component) or changes to the operational/threat environment (e.g., new attack vectors or vulnerabilities that impact the program protection risks).

CH 9–4.4 Intelligence Support for Program Protection

Program protection processes and analyses rely on intelligence inputs to better understand adversary warfighting capabilities, technological maturity, and counterintelligence inputs for more-complete comprehension of:

- Threats to program information, mission-critical functions and components, and CPI, including foreign collection methods,
- Successful attacks (compromise or loss events) as well as unsuccessful attacks.

Programs should request and analyze intelligence and counterintelligence products/reports (see CH 7–4.1. and CH 7–4.3. for specifics on the products/reports) to inform:

- CPI, TSN, and Information Analysis – What measures are most effective against a perceived threat or actual threat (attacks)?
- CPI Analysis – What capabilities are above and beyond those of our adversaries? What capabilities have been compromised? Are there threats to facilities with CPI, and are these facilities adequately protecting CPI?
- Information Analysis – What information has been compromised and lost?

These products/reports should be requested throughout the acquisition life cycle in order to inform program protection analysis during each stage of system development and to capture the evolving threat (i.e., more-advanced attacks and new threats based on the changing system environment).

CH 9–4.4.1 Joint Acquisition Protection and Exploitation Cell

The Joint Acquisition Protection and Exploitation Cell (JAPEC) integrates and coordinates analyses regarding unclassified Controlled Technical Information (CTI) losses. The JAPEC enables increased efforts across the DoD to proactively mitigate future losses and exploit opportunities to deter, deny, and disrupt adversaries that may threaten US military advantage. Key responsibilities of the JAPEC from a program's perspective include:

- Integrating all-source information in order to improve protection of CTI, which is common across programs and capabilities, and provide scalable options for analyzing the increasing threat to technologies that reside in or transit the Defense contractor-owned and contractor-operated networks
- Facilitating the identification of CTI, which is common across programs and technologies
- Providing referrals to the Military Departments' Counterintelligence Organizations (MDCO) or other defense agencies providing CI support for incidents involving compromised CTI
- Best practices for CTI protection.

Programs will utilize the expertise of the JAPEC as part of analyses of any compromised controlled technical information. The JAPEC will assist in the analysis and provide recommendations to the PM to address risks associated with compromised CTI. These recommendations may include, but are not limited to, such suggestions as:

- Program adjustments, including accelerating alternative technologies
- Warfighting changes, such as updating tactics, techniques, and procedures
- Capability requirements adjustments to address a change in threat
- Education and training in threat or counterintelligence
- Increasing protective features (e.g., use of isolated networks or increased use of classification guidance).

CH 9–4.5 Joint Federated Assurance Center

The Joint Federated Assurance Center (JFAC) is a federation of DoD organizations that have a variety of software (SwA) and hardware assurance (HwA) capabilities to support programs.

The JFAC develops, maintains, and offers vulnerability detection, analysis, and remediation capabilities through a federation of organizations and facilities from the Military Departments, Defense Agencies, other DoD activities, and other federal departments, agencies, and activities. The JFAC also facilitates collaboration with Science and Technology (S&T) acquisition, Test and Evaluation (T&E), and sustainment efforts to ensure that assurance capabilities and investments are effectively planned, executed, and coordinated to support program office needs.

Program offices are encouraged to visit the JFAC Portal for more information and guidance on how the JFAC can assist your program(s). A DoD CAC is required to open.

Additional details on the JFAC organization's capabilities and responsibilities can be found in Deputy Secretary of Defense Policy Memorandum 15-001 "Joint Federated Assurance Center (JFAC) Charter," dated February 9, 2015.

CH 9–Version and Revision History

The table below tracks chapter changes. It indicates the current version number and date published, and provides a brief description of the content.

Version #	Revision Date	Reason
0	02/02/2017	Chapter 9 Initial Upload
1	05/31/2017	Edited Section 9-3.1.3.2
2	07/03/2017	Corrected numerous hyperlinks
3	08/17/2017	Corrected numerous hyperlinks
4	10/04/2017	Corrected two hyperlinks; improved reference to TSN Analysis document in paragraphs 9–3.1.3.3 and .4; improved reference to TSN-related document at end of section 9-4.1 and added hyperlink
5		Update reference to Cybersecurity enclosure of DoDI 5000.02 from 14 to 13, per Change 4; update Figure 1; address DAU course ACQ 160 in 9-2.4.