DEPARTMENT OF DEFENSE

TECHNOLOGY AND PROGRAM PROTECTION GUIDEBOOK

July 2022

Science and Technology Program Protection Office

Office of the Under Secretary of Defense
for Research and Engineering

Please direct comments, feedback, or questions on this document as follows:
Attention: Director, Systems Security
OUSD(R&E)/Science and Technology Program Protection Office
4800 Mark Center Drive, Suite 17C08
Alexandria, VA 22350-3400

Department of Defense Technology and Program Protection Guidebook

Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301-3030

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

July 26, 2022

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Technology and Program Protection Guidebook

The Technology and Program Protection (T&PP) Guidebook is forwarded for use by your Science and Technology Managers and Engineers. This Guidebook provides implementing guidance for Department of Defense Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage" and replaces Chapter 9, Program Protection, of the Defense Acquisition Guidebook (DAG). The T&PP Guidebook supports the Department's objective to appropriately tailor the capability being acquired through the acquisition pathways of the Adaptive Acquisition Framework.

The electronic version will be made available through the Defense Acquisition University along with other DAG-replacing guidebooks. Please disseminate the T&PP Guidebook across your organization. To ensure updates to this Guidebook, future updates may be approved and issued by the Director, Systems Security in the Science and Technology Program Protection Office.

Robert E. Irie
Director for Science & Technology Program Protection

Attachment:
As stated

Technology and Program Protection Guidebook Change Record

Date	Name (First, Last)	Change	Rationale

FOREWORD

The Technology and Program Protection (T&PP) Guidebook provides the implementing guidance for DoD Instruction (DoDI) 5000.83, *Technology and Program Protection to Maintain Technological Advantage,* for Science and Technology (S&T) managers and engineers.

The T&PP Guidebook incorporates and supersedes Defense Acquisition Guidebook (DAG) Chapter 9, *Program Protection*, which provided guidance for implementing DoDI 5000.02T, *Operation of the Defense Acquisition System*, Change 8 Enclosure 13, *Cybersecurity in the Defense Acquisition System*.

In addition to incorporating guidance from DAG Chapter 9, the T&PP Guidebook:

- Incorporates technology protection activities for DoD-sponsored research and technology that is in the interest of national security.
- Emphasizes the S&T manager and engineering responsibilities for technology protection, program protection, and cyber.
- Aligns S&T manger and engineering procedures for technology protection, program protection, and cyber activities with DoDI 5000.02, *Operation of the Adaptive Acquisition Framework.*

The office of primary responsibility for this guide is the Director, Science and Technology Program Protection (D, STPP) in the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). D, STPP will continue to develop and coordinate updates to the Guidebook, as required, based on policy changes and customer feedback. To provide feedback, send email to Director, Policy, Guidance & Standards (PG&S), Mr. Burhan Adam at burhan.y.adam.civ@mail.mil.

This and other Adaptive Acquisition Framework (AAF) Guidebooks are available through the DAU AAF webpage located at https://aaf.dau.edu/guidebooks/.

Table of Contents

List of Tables

List of Figures

1 Purpose

The T&PP Guidebook provides guidance for S&T managers and engineers to protect and maintain the Department's technological advantage. The T&PP Guidebook provides guidance to effectively plan and execute technology, program protection, and cyber activities for DoD-sponsored research and technology and defense acquisition programs across the technology and system life-cycles.

2 Background

DoD Components will manage risk of adversarial exploitation and compromise of defense technology and programs, beginning with early S&T investment and continuing throughout the entire Defense Acquisition System (DAS) life-cycle, until disposal.

Programs will employ systems security engineering methods and practices, including cybersecurity, cyber resilience, and cyber survivability in design, test, manufacture, and sustainment. Such methods and practices will ensure that systems function as intended, mitigating risks associated with known and exploitable vulnerabilities to provide a level of assurance commensurate with technology, program, system, and mission objectives.

The T&PP Guidebook provides processes, methodologies, and techniques to enable S&T managers and engineers to identify information, components, and technologies that require protection, and to determine the most appropriate mix of measures to protect them from known adversarial threats and attacks related to security and cybersecurity. DoD Components can drive approaches to integrate protection measures before and during the development of the acquired technology and system; system operations; and the means by which Components acquire the technology or system.

Malicious activity by threat actors includes unauthorized activity to:

- Gain access to:
  - DoD-sponsored research to erode competitive technical or economic advantage.
  - DoD-advanced technology to erode U.S. technological superiority.
  - Intellectual property, designs, or technical information to weaken U.S. technological and military advantage.
- Compromise or disrupt critical missions by gaining access to operational and classified information.
- Insert malicious code or exploit existing vulnerabilities in hardware or software to disrupt or degrade system performance.
- Subvert or compromise DoD technology, systems, enabling systems, and support systems.

2.1 Purpose of Technology and Program Protection

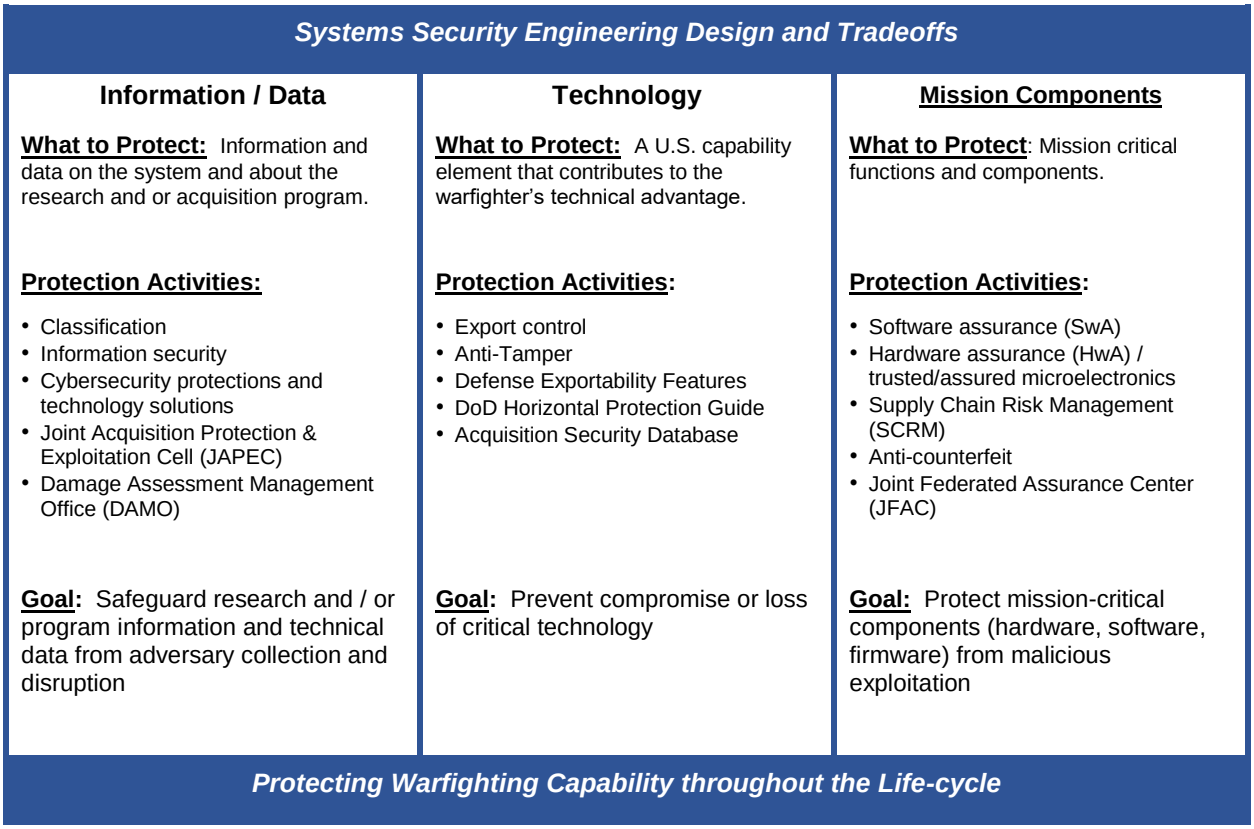
DoD technology, programs, systems, networks, supporting contractor facilities, and activities are at risk of attacks by state and non-state threat actors. The purpose of technology and program protection is to give S&T mangers and engineers an effective way to understand, assess, and prioritize the broad spectrum of adversary threats and attacks to technology and programs, and to identify the cost-effective mix of measures to protect against such attacks. S&T managers and engineers should consider protection measures that minimize adversary threats and attacks to the following elements exposed to targeting:

- Technical information and system data.
- Personnel.
- Government organizations, to include requiring activity, program office, and Government research and development laboratories.
- Contractors.
- Software and hardware.
- S&T capability, systems, enabling systems and supporting systems.
- System interfaces.
- Fielded systems.

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

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

Figure 1: Technology and Program Protection Activities



2.2 Technology and Program Protection Policy and Guidance

Table 1 provides a summary of top-level technology and program protection-related policies and guidance. The DoD issuances can be found at the following website: https://www.esd.whs.mil/DD/.

Table 1: Technology and Program Protection Policy and Guidance

Policy/Guidance	Title and Overview
DoD Directive 5111.21	***Arms Transfer and Technology Release Senior Steering Group and Technology Security and Foreign Disclosure Office.*** Describes the authorities of the Arms Transfer and Technology Release Senior Steering Group (ATTR SSG) and the Technology Security and Foreign Disclosure Office (TSFDO).
DoD Directive 5200.47E	***Anti-Tamper.*** Establishes policy and assigns responsibilities for Anti-Tamper (AT) protection of CPI. Designates the Secretary of the Air Force as the DoD Executive Agent for AT (DoD EA for AT).

Policy/Guidance	Title and Overview
	Designates the Under Secretary of Defense for Research and Engineering/Chief Technology Officer (USD(R&E)/CTO) as the Principal Staff Assistant responsible for oversight of the DoD AT program and policy.
DoD Instruction 5000.02	***Operation of the Adaptive Acquisition Framework.*** Establishes policy and prescribes procedures for managing acquisition programs, pursuant to the relevant sections of Title 10, United States Code. Restructures defense acquisition guidance to improve process effectiveness and implement the AAF. Describes the responsibilities of principal acquisition officials and the purpose and key characteristics of the acquisition pathways.
DoD Instruction 5000.02T	***Operation of the Defense Acquisition System.*** Establishes policy for the management of all acquisition programs. Authorizes Milestone Decision Authorities to tailor the regulatory requirements and acquisition procedures to more efficiently achieve program objectives, consistent with statutory requirements. .
DoD Instruction 5000.82	***Acquisition of Information Technology.*** Establishes functional acquisition policy and procedures for all programs containing Information Technology (IT).
DoD Instruction 5000.83	***Technology and Program Protection to Maintain Technological Advantage.*** Establishes policy, assigns responsibilities, and provides procedures for S&T managers and engineers to manage systems security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering. Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for Technology Area Protection Plans (TAPPs), S&T Protection Plans, Program Protection Plans (PPPs), and engineering cybersecurity activities.

Policy/Guidance	Title and Overview
DoD Instruction 5000.88	***Engineering of Defense Systems.*** Establishes policy, assigns responsibilities, and provides procedures to implement engineering of defense systems.
DoD Instruction 5000.89	***Test and Evaluation.*** Establishes policy, assigns responsibilities, and provides procedures for test and evaluation (T&E) programs across five of the six pathways of the AAF: urgent capability acquisition, Middle Tier of Acquisition (MTA), Major Capability Acquisition (MCA), software acquisition, and Defense Business Systems (DBS).
DoD Instruction 5000.90	***Cybersecurity for Acquisition Decision Authorities and Program Managers.*** Establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk by program decision authorities and program managers (PMs) in the DoD acquisition processes, compliant with the requirements of DoDD 5000.01, DoDI 5000.02T, DoDI 8510.01, and Chairman of the Joint Chiefs of Staff Instruction 5123.01H.
DoD Instruction 5200.01	***DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI).*** Provides policy and responsibilities for collateral, special access programs, Sensitive Compartmented Information (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). Provides guidance for classification and declassification of DoD information that requires protection in the interest of national security.
DoD Instruction 5200.39	***Critical Program Information Identification and Protection within Research, Development, Test, and Evaluation.*** Establishes policy and assigns responsibilities for the identification and protection of CPI, and defines CPI. Responsibilities include: • Horizontal identification and protection analysis. • AT analysis and protection. • Counterintelligence, intelligence, and security assessments and support. • International Cooperative Program CPI protection considerations.
DoD Instruction 5200.44	***Protection of Mission Critical Functions to Achieve Trusted Systems and Networks.*** Establishes policy and assigns responsibilities to manage supply chain risk and to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design, or sabotage or subversion of a system's mission critical functions or critical components, by foreign intelligence, terrorists, or other hostile elements.

Policy/Guidance	Title and Overview
	Responsibilities for Trusted Systems and Networks (TSN) include: • Identification of mission-critical functions and components through the criticality analysis process. • Use of all-source intelligence analysis of suppliers of critical components. • Use of enhanced software and hardware vulnerability detection and mitigation. • Use of SwA and HwA tools, best practices, and mitigations. • Use of tailored acquisition and procurement strategies. • Use of risk management.
DoD Instruction 5200.48	***Controlled Unclassified Information.*** Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order 13556 and Part 2002 of Title 32, Code of Federal Regulations (CFR).
DoD Instruction 5230.24	***Distribution Statements on Technical Documents.*** Establishes DoD policy, assigns responsibility and prescribes procedures for marking and managing technical documents, including research, development, engineering, test, sustainment, and logistics information, to denote the extent to which they are available for secondary distribution, release, and dissemination without additional approvals or authorizations. Establishes a standard framework and markings for managing, sharing, safeguarding, and disseminating technical documents in accordance with policy and law.
DoD Instruction 8500.01	***Cybersecurity.*** Establishes a DoD cybersecurity program to protect and defend DoD information and IT. Establishes the positions of DoD principal authorizing official (PAO) and the DoD Senior Information Security Officer (SISO) and continues the DoD Information Security Risk Management Committee (DoD ISRMC).
DoD Instruction 8510.01	***Risk Management Framework for DoD Information Technology.*** Establishes the Risk Management Framework (RMF) for DoD IT.
DoD Instruction 8582.01	***Security of Non-DOD Information Systems Processing Unclassified Nonpublic DOD Information.*** Establishes policy, assigns responsibilities, and provides direction for managing the security of non-DoD information systems that process, store, or transmit unclassified nonpublic DoD information, including CUI.
DoD Manual 5200.01 Volumes 1-3	***Volume 1: DoD Information Security Program: Overview, Classification, and Declassification.*** Provides guidance for classification and declassification of DoD information that requires protection in the interest of the national security.

Policy/Guidance	Title and Overview
	Volume 2: DoD Information Security Program: Marking of Information. Provides guidance for the correct classification marking of information. ***Volume 3: DoD Information Security Program: Protection of Classified Information.*** Provides guidance for safeguarding, storage, destruction, transmission, and transportation of classified information.
DoD Manual 5200.45	***Instructions for Developing Security Classification Guides.*** Provides guidance for the development of security classification guidance.
DoD Manual 5220.22	***The National Industrial Security Program Operating Manual (NISPOM).*** Codified in Part 117 of Title 32, CFR.
DoD Manual 5220.32 Volumes 1-2	***Volume 1: National Industrial Security Program: Industrial Security Procedures for Government Activities.*** Provides procedures for the protection of classified information that is disclosed to, or developed by, contractors, licensees, and grantees of the U.S. Government (USG). Prescribes industrial security procedures and practices applicable to USG activities using the DoD as their cognizant security agency to ensure maximum uniformity and effectiveness in DoD implementation of the National Industrial Security Program (NISP). ***Volume 2: National Industrial Security Program: Industrial Security Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence.*** Provides industrial security procedures and practices related to Foreign Ownership, Control, or Influence (FOCI) for DoD and non-DoD agencies, who have entered into agreements with DoD to act on their behalf to provide industrial security services to ensure maximum uniformity and effectiveness in DoD implementation of the NISP.
Program Protection Plan Outline and Guidance	***Program Protection Plan Outline and Guidance (PPP O&G).*** Provides an outline, content, and formatting guidance for the PPP required by DoDI 5000.83 and DoDI 5000.02. The outline structure and tables describe the minimum content that may be tailored to meet individual program needs. https://acqnotes.com/wp-content/uploads/2018/04/PPP-Outline-and-Guidance-v1-July2011.pdf
Science and Technology Protection Guide	***Science and Technology Protection Guide.*** Provides a sample process to assist in developing an overall methodology to protect DoD-sponsored S&T projects from unauthorized disclosure.

Policy/Guidance	Title and Overview
	https://www.dodtechipedia.mil/dodc/download/attachments/696558266/S%26T%20Protection%20Guide_Updated_20210331_cleared.docx?version=1&modificationDate=1625852523000&api=v2 (CAC or DTIC account required)
Science and Technology Protection Plan Template	***Science and Technology Protection Plan Template.*** Provides a recommended template for an S&T Protection Plan. https://login.dtic.mil/sso/oauth2/authorize?registration=https%3A%2F%2Freg.dtic.mil%3A443%2FDTICRegistration%2F&state=e21c5fbc-ff84-abde-8212-f0116c1e332b&response_mode=form_post&redirect_uri=https%3A%2F%2Fwww.dodtechipedia.mil%3A443%2Fagent%2Fcdsso-oauth2&response_type=id_token&scope=openid&client_id=dodtechipedia&agent_provider=true&agent_realm=%2Fcertificate&nonce=17A264357A3592F4062EDEB889968511 (CAC or DTIC account required)

Program protection-related education and training courses and credential programs are available at Defense Acquisition University (DAU) to train the workforce on practices and methods to proactively implement technology, program protection, and cyber mitigations related to adversarial threats.

2.3 Technology and Program Protection Roles and Responsibilities

Technology and program protection of DoD technology, programs and systems is the collective responsibility of the entire workforce, to include contractors.

S&T managers are typically scientists and engineers who manage basic research, applied research, and/or advanced technology development activities. They may also be involved with direct support to acquisition PMs. Their primary duties include developing plans and budgets for assigned S&T projects and acquiring the services of expert scientists, engineers, and technical support personnel to perform S&T work for DoD. S&T managers have responsibility for mitigating vulnerabilities and maintaining awareness of new and emerging threats to DoD-sponsored research and technology that is in the interest of national security.

PMs have overall responsibility for technology and program protection planning and execution for the system/capability. The AAF requires PMs to "tailor-in" the regulatory information that they will use to describe their program at the Materiel Development Decision (MDD) or program inception found in the Milestone and Phase Information Requirements (MPIR) tables, located in the Milestone Document Identification Tool (MDID). In this context, "tailor-in" means that the PM will identify and recommend for Milestone Decision Authority (MDA) approval, the regulatory information that the Component will employ to document program plans and how the Component will format that information and provide it for review by the decision authority. PMs' overall responsibility for technology and program protection planning and execution for the system/capability include:

- Managing technology and program protection cost, schedule and technical risks.
- Adequately resourcing technology and program protection efforts (i.e., staff and budget).

- Considering international acquisition and exportability early, including technology security and foreign disclosure (TSFD) requirements and defense exportability features (DEF).
- Planning and implementing Operational Security (OPSEC) for the program.
- Informing operators of technical risks when the system is fielded.

Systems Engineers (SEs) are responsible for ensuring the design, development and delivery of capability through implementation of a technical approach that balances cost, schedule, and performance risk. This is accomplished using integrated and consistent systems engineering activities and processes, regardless of when a project enters an acquisition pathway life-cycle. SEs conduct cost/benefit trade-off analyses and integrate contributions from each engineering specialty and design consideration. Each engineering specialty plays a role in the design of the system. The SE works to synthesize and balance the requirements. Systems security engineering design considerations for technology and program protections are some of many requirements that must be balanced in the design, development and delivery of the system/capability. SE responsibilities for systems security engineering include:

- Integrating systems security engineering activities into the system engineering processes.
- Conducting cost/benefit trade-off analyses with respect to systems security and other design considerations.
- Collaborating with systems security engineers (SSEs) on systems security requirements.
- Incorporating systems security requirements into the System Requirements Document (SRD)/system performance specification and solicitation (e.g. Contract Data Requirements Lists (CDRLs) have identified the appropriate marking and distribution statements for the technical information that will be delivered by the contractor) and ensuring CTI provided in the solicitation has the appropriate marking and distribution statements applied.
- Informing SSEs of operational and system constraints, and engineering cost/benefit trade-off decisions that affect technology and program protection planning and execution.
- Managing technology protection, program protection and cybersecurity technical risks.
- Supporting the development of the PPP.

SSEs integrate contributions from multiple systems security engineering disciplines such as AT, DEF, HwA, SwA, SCRM, cybersecurity, and other security disciplines, which include personnel security, industrial security, physical security, and information security. The outcome is comprehensive technology, program and system protection within the constraints of cost, schedule, and performance requirements while maintaining an acceptable level of risk. To integrate all aspects of systems security, the SSE evaluates and balances security contributions to produce a reasoned security capability across the technology, program and system/capability. The SSE responsibilities include:

- Collaborating with various engineering and security specialists to assess threats and vulnerabilities to inform the identification of appropriate protection measures.
- Conducting/leading program protection analyses for information, CPI, and TSN.
- Collaborating with SEs and security specialists to assess vulnerabilities and identify program measures.

- Conducting cost/benefit trade-off analyses to integrate protection measures from across systems security engineering specialists and security specialties to reduce security risks to meet acceptable levels based on performance, cost, and schedule.
- Translating protection measures into systems security requirements and adjusting them, based on constraints and engineering design decisions.
- Collaborating with SE to integrate the systems security requirements based upon system engineering artifacts.
- Appropriately documenting the selected protection measures in the PPP.

Systems security engineering specialists identify adversarial threats and vulnerabilities and the appropriate systems security protection measures within the scope of their systems security engineering specialty. While every program may not have someone associated with each role, some programs may have individuals fulfilling multiple roles. The systems security engineering specialists' responsibilities include:

- Assisting the SSE with technology and program protection analyses.
- Identifying protection measures within their specialty.
- Collaborating with the systems security engineers to adjust protection measures.
- Communicating resource needs to the SSEs.

Security specialists identify the security vulnerabilities and selected security protection measures within the scope of their security specialty. Security specialists' responsibilities for technology and program protection include:

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

Developmental T&E (DT&E) and Operational T&E (OT&E) testers ensure program protection-related test activities are appropriately incorporated into the T&E efforts, as described in DoDI 5000.89.

Contractors are responsible for conducting technology and program protection planning and execution as contractually agreed upon with their government client. The Contractor's responsibilities for systems security vary by contract, but typically include:

- Implementing Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplements (DFARS) in FAR-based contracts.
- Implementing requirements directed in the contract.

3 Technology and Program Protection Practices

S&T managers and engineers employ risk-informed protection measures to mitigate adversary threats and vulnerabilities in technologies, systems, and projects/programs. These include engaging with cybersecurity, security, counterintelligence, and intelligence resources to inform:

- System design and development, modernization, and sustainment, which includes using secure design principles.

- SCRM decisions and mitigations.
- Test objectives.
- Cost, schedule, and performance risk decisions and mitigations.

The following sections address the technology and program protection and cyber activities that DoD Components should perform and how those activities are executed across the life-cycle. The activities include the analyses for identifying and prioritizing what needs to be protected in the information, technology, and system and the methods to select protection measures. The technology and program protection analyses are a part of an iterative process that re-evaluates the adversarial threats and vulnerabilities to information, technology, and the system to provide a cost effective, balanced set of risk mitigations.

3.1 Secure Cyber Resilient Engineering Practices

To reduce the risk of weapon systems being negatively affected by cyber events, it is important for the systems security engineering workforce to understand how to design systems/capabilities that are less vulnerable, and more resilient against cyberattacks. Cyber resilience is not the same as cybersecurity. Cyber resilience is the ability to have a system adapt to changing conditions and withstand and recover rapidly from disruptions due to adversity. This is different from a focus on reducing the risk of cyber intrusion and attack on a system. Cyber resilience is an engineering function and requires a workforce competent enough to be able to architect resiliency in the system design.

Secure cyber resilient engineering (SCRE) practices include skills necessary to specify, design, and realize systems given the protection concerns enabled/induced by or within contested cyberspace. It also involves SSEs being able to address protection concerns associated with the computational, communication, and physical (i.e. cyber-physical) characteristics of systems/capabilities. The protection concerns of contested cyberspace span the entire life-cycle of the system, to include its enabling and supporting systems; the entire life-cycle of technology, data, and technical information associated with the system; and the maintenance, logistics and supply chain.

SCRE activities include allocating cybersecurity and related systems security requirements to the system architecture with consideration of the operational constraints of the system. The system architecture and design will address, at a minimum, how the system:

- Manages access to, and use of, the system and system resources.
- Is structured to protect and preserve system functions or resources, such as through segmentation, separation, isolation, or partitioning.
- Maintains priority system functions under adverse conditions.
- Is configured to minimize exposure of vulnerabilities that could impact the mission, including through application of techniques such as design choice and component choice.
- Monitors, detects, and responds to security anomalies.
- Interfaces with the DoD Information Network or other external services.

The following are examples of technologies that SCRE practices integrate into the system/capability to protect the data in the system:

- **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 National Cross Domain Strategy & Management Office (previously 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 or National Security Agency (NSA)-certified cryptographic products and technologies into systems 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.

The Cyber Resilient Weapon Systems Body of Knowledge (CRWS-BoK) at https://crws-bok.org/ contains a repository of authoritative resources to support secure cyber resilient engineering activities.

3.2 Technology and Program Protection Analyses

Technology and program protection analyses consist of three sets of interrelated analyses that inform design decisions to protect the information, technology, and system: Information Analysis, CPI Analysis, and TSN Analysis. These analyses are the primary activities for identifying and prioritizing what needs to be protected involving the following activities:

- *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 systems security engineering (i.e., HwA, SwA, and supply chain risk management, AT, exportability features, and cybersecurity) and general security specialties to address adversarial threats and attacks. Each specialty has a set of analyses, approaches, and protections that programs can utilize.
- *Engineering Decisions*: Activities, primarily cost/benefit 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 S&T managers and engineers incorporate into the system design.

S&T managers and engineers are not meant to perform the technology and program protection processes, and their constituent activities, in a particular time-dependent sequence. S&T managers and engineers can apply each process iteratively, recursively, and in parallel (where applicable) throughout the technology and system life-cycle to provide safe, resilient, secure systems to the warfighter.

3.3 Information Analyses

The information analysis activities form the foundation for all technology and program protection activities. Information analysis is the set of activities that S&T managers and engineers conduct to identify, understand, and protect technical information and data. These activities include:

- Classification determination.
- Application of marking and distribution statements on CTI.

3.3.1 Information Analyses Activities

Activities related to the identification, classification, and marking of information associated with a DoD-sponsored research or program are driven by DoD policies. The results of these activities drive decisions about protections (or other requirements), which DoD Components must implement to appropriately protect the information.

When conducting information analysis, S&T managers and engineers should pay particular attention to technical information identification and protection. Technical information includes much of the research and engineering associated with DoD-sponsored research and programs; the majority resides on unclassified systems. If stolen, this information provides adversaries with insights into U.S. defense and industrial capabilities and allows them to save time and expense in developing similar capabilities. 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.

Information analysis also includes consideration of data compilation and the protection of 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.

Information analysis activities include:

- **Classification Determination:** This includes the identification of the classification of the information. The classification of the information provides the basis for decisions on protections for system data, and for CUI, which includes CTI. The following issuances provide procedures to determine classification of information: DoDM 5200.01 Volumes 1-3, DoDI 5200.48 and DoDM 5200.45.
    - Classification management procedures call for the timely issuance of comprehensive guidance regarding classification of information owned by, produced by or for, or is under the control of the U. S. Government for information.
    - A Security Classification Guide (SCG) will be issued as early as practical in the life-cycle of the classified system, plan, program, project, or mission. Classification guidance is a prerequisite to effective and efficient information security and assures that DoD Components expend security resources to protect only that which truly warrants protection in the interests of national security. Components should not consider information for classification unless its

unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to national security and it pertains to one or more of the categories specified in DoDM 5200.45. Additionally, Defense Technical Information Center (DTIC) provides an online index and access to most of the SCGs issued within DoD.
  - Distribute SCGs that have been signed by the Original Classification Authority, to organizations and contractor(s) who have, or will have, responsibilities associated with the information in the SCG.
  - The SCG is an appendix to the PPP.

Marking and Distribution Statements on CTI: This includes the identification and application of marking and distribution statements on CTI, which applies to both classified and controlled unclassified technical information. Marking and distribution statements provide the basis for decisions on protection to safeguard the information and the level of sharing (or other requirements) when handling the information. The procedures for identifying and applying marking and distribution statements on technical information can be found in DoDI 5230.24.
  - The intent of the marking and distribution statement framework is to stem the flow of military-related technical information to our adversaries, without inhibiting technological growth or blocking the exchange of technical information that is vital to progress and innovation. When properly applied, the framework reduces flow of CTI to our adversaries but permits it to flow to Government Agencies and private organizations that have legitimate need for it. Technical information includes engineering drawings, engineering data and associated lists, standards, specifications, technical manuals, technical reports, technical orders, blueprints, plans, instructions, computer software and documentation, catalog-item identifications, data sets, studies and analyses, and other technical information that an entity can use or adapt to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment. The information may be in tangible form, such as a model, prototype, blueprint, photograph, plan, instruction, or an operating manual; or may be intangible, such as a technical service or oral, auditory, or visual descriptions.
  - For DoD S&T projects and acquisition programs which only have CUI, consider developing a document similar to the format of the SCG as a mechanism to identify and protect unclassified CTI. This will assist in implementing DFARS requirements for safeguarding CUI when CTI is involved.

- **Fundamental research** not clearly related to national security shall, to the maximum extent possible, remain unclassified, pursuant to National Security Decision Directive 189.

DoD S&T managers and engineers responsible for creating, owning, sponsoring, or directing the creation of technical information have the responsibility to determine the appropriate marking and distribution statements in accordance with DoDI 5230.24 and CUI markings in accordance with DoDI 5200.48. The marking and distribution statements provide information on the restrictions and sharing requirements for the information across research, development,

engineering, test, sustainment, and logistics, before external release (distribution) of the information.

3.3.2 Distribution of CTI

Government and contractor personnel must handle CTI in accordance with the classification and marking and distribution statements applied to the information. This includes further sharing/dissemination of the CTI.

To mitigate risk of losing DoD controlled technical information, DoD S&T managers and engineers should consider limiting the release of government furnished information provided in a solicitation to only what is necessary to perform the work specific to the solicitation/Request for Proposal (RFP).

3.3.3 Marking and Distribution Statements on Technical Information

For FAR-based contracts, instructions to apply marking and distribution statements on newly created information by the contractor are incorporated through CDRLs (at DD Form 1423, Block 9 and 16). It is the responsibility of the S&T managers and engineers to select the correct distribution statement and to ensure that the corresponding code letter ("A," "B," "C," "D," "E," "F," or "X"), described in DoDI 5230.24, is in block 9 on DD Form 1423 and instructions on application of the distribution statement are provided in block 16 on the DD Form 1423.

3.3.4 Implementing Information Protections

For FAR-based contracts handling classified information, FAR Clause 52.204-2, *Safeguarding Classified Information*, applies.

- The Defense Counterintelligence and Security Agency (DCSA) administers the NISP and provides appropriate security education, training, and awareness to industry and government personnel. The NISP is implemented through contracts by applying FAR Clause 52.204-2 in Section I when classified information is involved in the contract.
- Use a Counterintelligence Support Plan (CISP) to coordinate counterintelligence support activities conducted by the appropriate Defense Counterintelligence Component for system/capability organizations. The CISP is an appendix to the PPP.

For non-FAR based legally binding agreements, consider incorporating language similar to FAR Clause 52.204-2 in the agreement to implement protections for classified information.

For FAR-based contracts handling CTI that is processed, stored, or transmitted on an unclassified information system that is owned, or operated by/for, a contractor, the protection requirements in DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, apply.

When DFARS Clause 252.204-7012 is in Section I of the contract, the contractor is required to implement the following when CTI is involved, such as when CTI has a marking and dissemination statement, or when the Component has directed the contractor to apply marking and dissemination statements to contract deliverables:

- Safeguard CTI that resides on or is transiting through a contractor's internal information system or network.
- Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein within 72 hours of discovery to DoD at https://dibnet.dod.mil (A DoD-approved Medium Assurance Certificate is required to report a Cyber Incident.)
- Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center; submit media/information as requested to support damage assessment activities.
- Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve CTI. DoD Components should consider programmatic, strategic, and operational mitigations in determining an appropriate response to risks resulting from a cyber-intrusion.
- Encourage and engage eligible industry counterparts to participate in the Defense Industrial Base Cyber Security (CS) Program, established in Part 236 of Title 32 CFR.

For non-FAR based legally binding agreements, consider incorporating language similar to DFARS Clause 252.204-7012 and/or DoDI 8582.01 in the agreement to implement protections for unclassified CTI.

3.4 CPI Analyses

CPI is the U.S. capability element contributing to the warfighters' technical advantage, which if compromised, undermines 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, dated May 2015.

CPI elements are often DoD-unique capabilities, developed and owned by the U.S., 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.
- Require protection measures to deter, delay, detect, and respond to attempts to compromise CPI.

CPI analysis is the means to identify, protect, and monitor CPI. This analysis should be conducted early and continue throughout the life-cycle of the CPI. Additionally, because CPI is critical to U.S. technological superiority, its value may extend beyond any one program. As a result, CPI analysis should include horizontal identification and protection considerations to ensure consistency on maintaining US technological advantage.

3.4.1 CPI Identification

S&T managers and engineers conduct CPI identification to determine if organic CPI (developed by the program) and/or inherited CPI (developed by another program but incorporated into the program/system) exists or will exist in the operational, deployed system. S&T managers and engineers also conduct CPI identification to identify technology that DoD no longer considers to provide a U.S. technological advantage to the warfighter and may no longer require its current level of protection.

S&T managers and engineers should identify CPI early and reassess it throughout the life-cycle of the program, to include: prior to each acquisition milestone; prior to each systems engineering technical review (SETR); throughout operations and sustainment; and specifically during software/hardware technology updates.

Note that CPI is not:

- Personally Identifiable Information (PII).
- Protected Health Information (PHI).
- Financial information.
- Logistics information.
- Operational information (waypoints and target location data).
- System performance, vulnerabilities, or weaknesses.
- Designs.
- Manufacturing details.
- Unmodified commercial-off-the-shelf (COTS) technology.
- Multi-Level Security Solutions (defined in Committee on National Security Systems Instruction (CNSSI) Number 4009).
- Cross Domain Solutions (defined in CNNSI Number 4009).
- Cryptographic Solutions (defined in CNNSI Number 4009).

While the above may be classified information, or CUI, they are not CPI because one or more of the following apply:

- It is not a capability.
- Its compromise does not result in a transferable technology that adversaries can leverage to bolster their warfighting capability.
- Its compromise does not result in transferable technology that adversaries can use to counter U.S. capabilities based on weaknesses or patterns identified within the transferred technology.
- It does not live on the weapons system, training equipment, maintenance support equipment, or other supporting end-item.

To identify CPI, S&T managers and engineers should consider the following activities:

- Use DoD, DoD Component, and program resources (e.g., intelligence products, SCGs, the Acquisition Security Database (ASDB), the DoD CPI Horizontal Protection Guide, DoD policy, and 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 approval by the appropriate PPP approval authority.

Identification of CPI typically involves collaboration among, and input from the PM, SE, SSEs, S&T representatives, security specialists, AT specialists, intelligence/counter-intelligence representatives, and - when there is inherited CPI - representatives from the program office that is responsible for the inherited CPI.

3.4.2 Selection of CPI Protection Measures

Components should select CPI protection measures soon after Component identifies the CPI. The Component should maintain and reassess these protection measures throughout the life-cycle of the CPI until the protection measures are no longer warranted.

CPI protection measures seek to deter, delay, detect, and react to attempts to compromise CPI on the end item resulting from hands-on, reverse engineering attacks. Protections triggered by the identification of CPI include AT and DEF. Other protection measures, listed under other systems security engineering specialties and security specialties, may also contribute to the protection of CPI; however, CPI identification does not trigger these protections. For example, Components would protect classified information about CPI, including design and manufacturing know-how, in accordance with the classification guidance in the related SCG and through the appropriate protections for classified information. When manufacturing information is considered unclassified CTI, a Component would protect it in accordance with the protections for CTI.

To select the appropriate end-item CPI 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 through export.
- Assessed threat of foreign adversary interest and skill in obtaining CPI.
- Known vulnerabilities of the system.

For more information on the consequences of CPI compromise, system exposure and vulnerabilities, consult the AT Desk Reference Guide and the AT Technical Implementation Guide available at https://at.dod.mil/. For threat information, request a Counterintelligence Threat Assessment from your supporting Defense Counterintelligence Component in accordance with the procedures in DoDI O-5240.24.

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 requirements. Adjust or add protections as needed, given any change to the consequence of CPI compromise, exposure of the system, the assessed threat, and known vulnerabilities. Considerations for modifications might include how the inherited CPI is integrated into the system (e.g., changes affecting the design and interfaces).

3.4.3 Horizontal Protection of CPI

CPI is not always unique to one program (i.e., two programs may contain similar CPI, or one program may inherit CPI from another), and as a result, there is a risk of not protecting CPI consistently across all programs. When Components do not protect similar CPI consistently across programs, CPI is at risk of the following:

- Exposing similar or the same CPI to greater risk.
- Undermining or diminishing the protection investment made by another program.
- Applying an inconsistent level of resources to protect CPI.

To minimize risk to CPI, programs should conduct horizontal protection measures to determine if they need additional protections to protect CPI. 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 have CPI identification 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 within their DoD Component, SCG, or DoD policy (e.g., DoDI 5230.28). The DoD CPI Horizontal Protection Guide contains a list of example CPI to help identify the same or similar CPI associated with other programs. For more information, contact your DoD Component AT lead for more information on the DoD CPI Horizontal Protection Guide.

In support of horizontal protection, OSD encourages programs to work with the DoD EA for AT and their DoD Component AT leads early and often for guidance.

Where horizontal protection disagreements arise, programs should discuss, negotiate, and agree upon the level of protection required to ensure the program achieves an equivalent level of risk across the affected systems, considering potential differences in system exposure. If programs cannot reach agreement, the DoD EA for AT may inform the Low

Observable/Counter-Low Observable (LO/CLO) Tri-Service Committee and the MDA of any AT-related horizontal protection issues per DoDD 5200.47E.

3.4.4 CPI Monitoring

Components should commence CPI monitoring soon after identifying the CPI, and should continue this monitoring throughout the life-cycle of the program.

CPI monitoring is the process for determining if an event has occurred that requires a reassessment of the CPI or its 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.
- **Export status:** Current or future plans for the system to be available to allies or partners through Direct Military Sales or other export programs.
- **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, programs should reassess the CPI to determine if they need to make changes to the CPI's associated protection measures.

3.5 Trusted Systems and Networks Analyses

The goal of TSN analysis is to protect those functions and components 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:

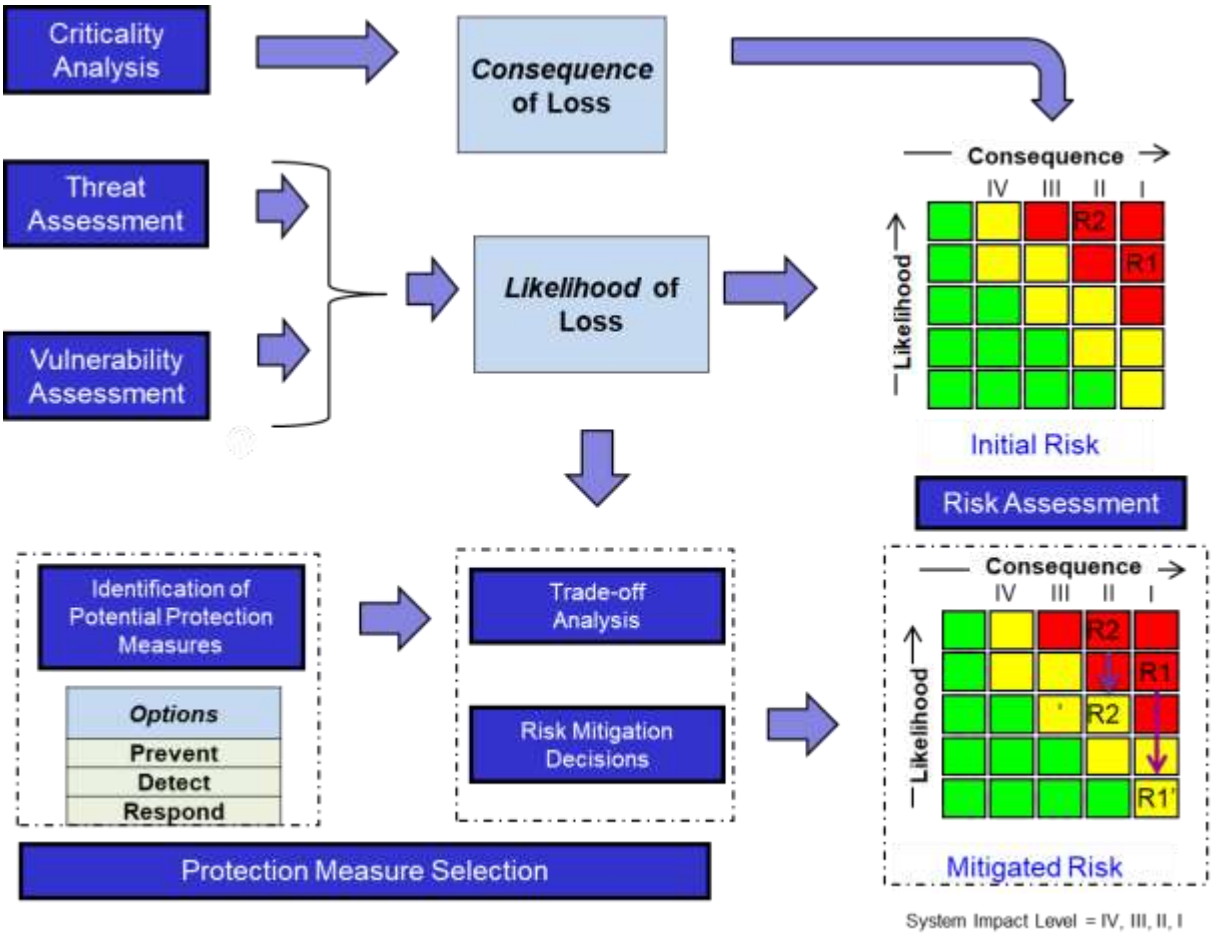
- Identification of the mission-critical functions and the system's critical components, commensurate with the system requirements decomposition.
- Assessment and analysis of threats, vulnerabilities, and risk for identified mission-critical functions and critical components.
- Risk mitigation and protection measures for planning and implementation.
- Proactive planning and implementation of TSN best practices.
- Trade-space considerations for selection of the appropriate protection measures.
- Risk identification after Components implement protection measures, including follow-up mitigation plans and actions as well as assessments of residual risk.

DoD Components complete TSN analysis through conducting the following: criticality analysis, supplier threat assessment, vulnerability assessment, risk assessment, and selection of

appropriate protection measure(s). Components apply the TSN analysis process throughout the acquisition life-cycle, focusing on the systems security risks for the system/capability. As the technical maturity of the system evolves, the program should reconsider the criticality of the functions and components, as well as the evolving vulnerabilities and threats. By periodically repeating the TSN risk management process, Components can identify additional threats and vulnerabilities as the level of detail of the design becomes more defined. The continuous TSN risk management process is one of the methods that inform the system design cost/benefit trade-offs. Discovery of a potentially malicious source from the supplier threat assessment may warrant additional checks for vulnerabilities in other (less critical) products procured from that source. For each critical function and critical component risk that is assessed as "high" or "very high," Components need a risk cube and mitigation plan to manage that risk.

The relationships between the criticality analysis, threat assessment, vulnerability assessment, risk assessment, and protection measures selection are shown in Figure 2.

Figure 2: TSN Analysis Methodology



Components should begin efforts to identify mission-critical functions and critical components and their protection as early in the life-cycle as possible, and will be dependent on the technical maturity of the system/capability when it enters one of the AAF pathways. Components should reassess the protections and related risk assessment for the mission critical functions and critical components as system designs evolve and mature. Iterative application of the 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. Components should update the analysis at each of the SETRs to take into account the latest design and implementation decisions, as well as additional threat and vulnerability information.

Table 2 describes DoD acquisition program level of TSN analysis technical maturity as it progresses through the MCA SETRs. Programs should tailor the TSN analysis as necessary and should make it commensurate with the SRD/system specification level as the system progresses through the life-cycle. In the Production and Deployment (P&D) and the Operations and Sustainment (O&S) phases, DoD expects that Components will update the analysis periodically to the level of technical maturity of the Product Baseline, which is equivalent to the approved technical documentation that describes the configuration of the components at the production, fielding/deployment, and operational support phases. Components should conduct a periodic analysis to support the development of an updated PPP for the Full Rate Production (FRP) Decision Review (DR)/Full Deployment Decision Review (FDDR). For a system upgrade, a program may have to conduct the analyses on the system upgrade at all levels of detail described in the Alternate Systems Review (ASR) through System Verification Review (SVR)/Functional Configuration Audit (FCA), as the system upgrade goes through development and integration.

Table 2: TSN Analysis Level of Technical Maturity

DoD Acquisition Technical Review	Criticality Analysis	Vulnerability Assessment	Risk Assessment	Protection Measure
Alternate Systems Review (ASR)	Mission-based functions	Response to Milestone A, or equivalent decision point, Vulnerability Questionnaire	Objective risk criteria established and applied at function level	Risk-based supply chain, design and software protection measure selection selected via cost/benefit trade-off study
System Requirements Review (SRR)	System requirements level functions	Vulnerability questionnaire and Vulnerability Database (DB) assessment	Risk criteria updated applied at system level	Risk-based system function level protection measure selection

DoD Acquisition Technical Review	Criticality Analysis	Vulnerability Assessment	Risk Assessment	Protection Measure
System Functional Review (SFR)	Subsystem level sub-functions	Vulnerability Questionnaire and DB assessment to critical subsystem level	Risk criteria updated and applied at subsystem level	Risk-based subsystem function level protection measure selection refinement
Preliminary Design Review (PDR) **Allocated Product Baseline**	Assembly/ component	Vulnerability Questionnaire and DB assessment to critical assembly/ component level	Risk criteria updated and applied at assembly/component level	Risk-based assembly level protection measure selection
Critical Design Review (CDR) **Initial Product Baseline**	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 protection measure selection
System Verification Review /Functional Configuration Audit (SVR)/(FCA)	Part (preliminary)	Vulnerability DB, static analysis and diversity assessment to critical **part** level	Risk criteria updated and applied at preliminary part level of critical components	Risk-based Component level protection measure selection
Production Readiness Review/ Physical Configuration Audit (PRR)/(PCA)	Component (Final)	Review final Component analysis	Review Risk Assessments	Review Component level protection measure selection

DoD Components incorporate selected protection measures into relevant solicitations, to include the SRD/System specifications, and Statement of Work (SOW). The solicitation/Request For Proposal (RFP) should incorporate the results and decisions from the SETRs immediately

preceding the solicitation/RFP release. For example, it would be expected that for the MCA pathway, the solicitation/RFP for the Technology Maturation and Risk Reduction (TMRR) phase would be based on the ASR analysis results; the solicitation/RFP for the Engineering and Manufacturing Development (EMD) phase would be based on the SFR analysis results; and the solicitation/RFP for the P&D phase would be based on the CDR analysis results.

3.5.1 TSN Analysis: 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 to the mission of the system. 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. They 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.

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

Table 3: TSN Criticality Levels

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

- Microelectronics and software components are especially susceptible to malicious alteration that affect the mission critical functions of the system.
- Engineers should use dependency analysis 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 access to critical components (e.g., implement least-privilege restrictions).

Once S&T managers and engineers have identified critical functions and components through the criticality analysis process, they may use the results along with the vulnerability assessment and threat assessment to determine the systems security risk to the system, and its associated mission(s).

Programs should perform a criticality analysis, at a minimum, before each SETRs and when there is a change to a critical component.

3.5.2 TSN: Threat Analysis

All-source intelligence is available to the S&T managers and engineers to understand the threats to the system and the threats posed by specific suppliers of critical components. DoD uses multiple sources of intelligence to feed into this analysis.

For TSN, the Defense Intelligence Agency's (DIA) DoD SCRM Threat Analysis Center (TAC) provides supplier threat information. DoD has designated the DIA to be the DoD enterprise focal point for threat assessments that DoD acquisition programs need 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 the supplier threat assessments to assist in developing appropriate mitigations for supply chain risks. The program should submit SCRM TAC requests for all Level I and Level II critical components, as identified by a criticality analysis. At a minimum, the program should create a list of suppliers of critical components. Programs may submit SCRM TAC requests as soon as they identify sources of critical components.

SSEs can request SCRM threat analysis of supply chain risk through their respective DoD Component PPP leads. For the policy and procedures regarding the request, receipts, and handling of supplier SCRM TAC reports, refer to DoDI O-5240.24. SSEs expect the number of supplier threat assessment requests will grow as the system’s criticality analysis becomes more refined and the system architecture and boundaries are specified. As a result, SSEs should expect to submit a greater number of requests to the TAC following a PDR and CDR, or equivalent review.

In the absence of threat information, a program should assume a medium threat for Level I and Level II critical components 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.

3.5.3 TSN: Vulnerability Assessment

Vulnerability is any weakness in a system design, development, production, or operation that an adversarial threat can exploit to defeat the mission objectives of the system or significantly degrade its operational performance. DoD Component decisions about which vulnerabilities to address and which protection measures or mitigation approaches to apply are based on an overall understanding of risks and program priorities. The search for vulnerabilities begins with the systems mission-critical functions and its 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 protection measures applied to functions and components identified in earlier criticality analyses.
- Investigation of vulnerabilities may also identify additional threats, or opportunities for threats, that programs did not consider in earlier vulnerability assessments.
- Vulnerabilities inform the risk assessment and protection measures.
- 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, and inform vulnerability assessments.

S&T managers and engineers should consider potential malicious activities that could interfere with a system's operation throughout a system's design, development testing, production, and maintenance. Programs that identify vulnerabilities early in a system's design can often eliminate them 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 programs can identify 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 the adversary's 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.
- Single points of failure.

The supply chain includes any access point during a system's design, engineering and manufacturing development, production, configuration in the field, system updates, and maintenance periods. Supply chain 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 that programs use to obtain and maintain hardware, software, and firmware components in the system.

Several techniques and tools available for identifying vulnerabilities are:

- Vulnerability assessment questionnaire: A set of 'yes' or 'no' questions to assist in incorporating appropriate mitigations in the SOW and SRD/system performance specification prior to release of the solicitation.
- Vulnerability database assessment: Includes the Common Attack Pattern Enumeration and Classification (CAPEC) database, which programs use for the analysis of common destructive attack patterns; the Common Weakness Enumeration (CWE) database, which programs use to examine software architecture/design and source code for weaknesses; and the Common Vulnerability Enumeration (CVE) database, which programs use 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, making it necessary for programs to determine which analyzer(s) is/are best suited for specific application.
- Component diversity analysis: Examines the critical function designs for common components to assess the impact of malicious insertion to a component that a program uses to implement multiple critical functions or sub-functions.
- Fault Tree Analysis: Assumes a top-down analysis that uses Boolean logic to identify system failures. An important twist in applying fault free analysis to system engineering processes 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. Fault tree analysis 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, a program should consider the possible access paths and opportunities that a threat would have to exercise to introduce the vulnerability or trigger the failure.
- 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.

3.5.4 TSN: Risk Assessment

S&T managers and engineers should perform a TSN risk assessment, at a minimum, for each Level I and Level II critical function or component identified in its criticality analysis. Components should use the criticality level generated through the criticality analysis 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. Programs can use a similar approach to combine multiple threats into threat likelihood.
“

3.5.5 Trusted Systems and Networks: Protection Measures

TSN protection measures are cost-effective activities and attributes that manage risks to the system’s mission critical functions and critical components. They vary from process activities (e.g., using a blind buying strategy to obscure end use of a critical component) to design attributes to mitigate particular risks. Programs should use a risk burn-down plan to monitor the implementation of the selected mitigation.

Programs may apply a selection of protection measures for Level I and Level II critical functions and critical components that they have identified after conducting a TSN risk assessment. This also applies against other parts of the system, not just those that they identified as criticality Level I and Level II. There are “good hygiene” activities within each of the systems security engineering specialties that may also contribute to mitigating TSN risk. The program should consider preparing a full list of mitigations and protection measures to inform and provide options for trade-off decisions between cost, schedule and technical risk. The best set of mitigations and protection measures depends on the system, its environment, mission, and threats. Additionally, each mitigation or protection measure may have a phased implementation plan.

3.6 Systems Security Engineering Specialties

This section provides an overview of the systems security engineering specialties and how each contributes to program protection. The systems security engineering specialties include AT, DEF, HwA, SwA, SCRM, and cybersecurity. Each specialty brings a unique perspective, methods, skills, and protections that contribute to the overall protection scheme.

To achieve the intended technology and program protection objectives, a program must select the most appropriate set of protection measures within the program’s cost, schedule, performance, and operational constraints.

Beyond the systems security engineering specialties described in this section, systems security engineering also considers protections that security specialists implement. The security specialists include the traditional aspects of security, which are usually under the responsibility of the security manager in the government program office and under the facility security manager at the contractor facilities. These traditional security aspects include physical security, information security, industrial security, personnel security, and any unique security associated with DoD Information Security Program (e.g. DoDM 5200.02 Volumes 1-3). The security specialists provide protection measures that complement the systems security engineering activities when it is in the interest of national security.

3.6.1 AT Specialty

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 identified using the CPI analysis process. Properly implemented AT should reduce the likelihood of CPI compromise resulting from reverse engineering attacks for systems outside of U.S. control (i.e., those lost or left on the battlefield, or exported).

Upon the identification of CPI, it is important for programs to contact their DoD Component AT representative for AT guidance. Table 4 provides the expectations for the identification and implementation of AT requirements and delivery of AT protections when programs identify CPI. Programs should repeat CPI analysis activities when events occur that trigger a reassessment of CPI protection measures.

Table 4: AT Activities throughout the DoD Acquisition Life-cycle

DoD Acquisition Technical Review	AT Activities
ASR	• Assess AT implementation costs, vulnerabilities, and the impact on system performance and/or maintenance. • Incorporate AT requirements and design activities in the SOW.
SRR	• Develop AT requirements for the SRD/system performance specification.
SFR	• Update AT requirements addressed via the SFR. • Draft AT requirements to incorporate into SRD/system performance specification. • Update AT requirements for incorporation into the SOW.
PDR	• Update AT requirements addressed via the Allocated Baseline.
CDR	• Finalize AT requirements via the Initial Product Baseline. • Implement analysis and document AT implementation costs and residual vulnerabilities. • Incorporate final AT requirements in the SRD. • Incorporate final AT implementation activities in the SOW.
SVR/FCA/ PRR/PCA	• Complete AT verification and validation; use evaluation results to inform risk decision. • Monitor AT requirements to accommodate upgrades, changes, and resolutions to obsolescence as appropriate. • Monitor AT requirements for changes to system threats, export status, and operational environment.

Table 5 provides the necessary AT products that DoD Components must complete for review and concurrence by the DoD EA for AT (the AT Plan is submitted as an appendix to the PPP, when CPI is identified) or by the DoD Component AT representative (as delegated by the DoD EA for AT).

Table 5: AT Products and Timeline

AT Product:	AT Concept Plan	Initial AT Plan	Final AT Plan	AT Evaluation Plan	AT Evaluation Plan/Report
Domestic Cases	105 days prior to Milestone A	60 days prior to Milestone B	60 days prior to CDR	60 days after CDR	60 days prior to Milestone C
Foreign Military Sales (FMS) Direct Commercial Sales and International Cooperative Program	105 days prior to Pricing and Availability (P&A) or Letter of Offer and Acceptance Signature	60 days post contract award	60 days prior to CDR	60 days after CDR	60 days prior to System Export

DoD Components must document exemptions or exceptions to AT requirements, submit them for review to the DoD EA for AT, include them in the PPP, and have the program PPP approval authority approve them.

The following AT reference documents are available via the DoD EA for AT website at https://at.dod.mil/, or DoD programs can obtain them from the respective DoD Component AT lead:

- 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 SCG: Provides classification requirements for AT deliverables.
- AT Plan Template: Provides the outline and guidance to assist with AT work product development.

3.6.2 DEF Specialty

Prior to international involvement in a program, there are two basic technology security and foreign disclosure (TSFD) security requirements to consider and resolve as a first order of business. These are access and protection. This is the case whether the transaction is related to cooperative research and development; information or personnel exchange; and/or foreign sales (either FMS of Direct Commercial Sales) and whether the issue involves foreign government or international organization representatives. These requirements evolve from law, Executive Orders, and DoD Directives and Instructions.

Early consideration of TSFD requirements – the pre-vetting and advanced export control planning in international programs – help enable a U.S. program to achieve maximum potential benefit from international involvement, while avoiding negative impacts on cost, schedule and performance. Export control is one of the major factors in any program with an international aspect.

DEF includes AT protection measures suitable for export and differential capability modifications, to include removal of technologies and/or capabilities that U.S. laws and regulations prohibit for export. DEF also provides a means of protecting CPI in export configurations.

As early as possible, DoD Components should assess the following to determine the application of DEF: (1) the feasibility of designing and developing 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 planning supports the Department'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 DEF activities, refer to:

- Office of the Under Secretary of Defense for Acquisition and Sustainment website (https://www.acq.osd.mil/ic/def.html).
- Office of the Under Secretary of Defense for Acquisition, Technology And Logistics Memorandum for DoD Component Acquisition Executives (CAEs), *Defense Exportability Features Policy Implementation Memorandum and Guidelines* (https://www.acq.osd.mil/ic/docs/def/DEF-Policy-Implementation-Memo-and-Guidelines-Final-4-29-15.pdf).

3.6.3 HwA Specialty

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, to include those either intentionally or unintentionally designed or inserted in the system's hardware and/or its embedded software during the microelectronics life-cycle.

HwA protection measures reduce the likelihood that an adversary will successfully:

- Exploit vulnerabilities built into microelectronics, to include their embedded software.
- Insert malicious logic in microelectronics during development, fabrication, and programming.

- Introduce counterfeit microelectronics or unauthorized or tainted embedded software or tools into the supply chain, impacting the functionality of the critical component.

The TSN analysis should identity if DoD programs will use/are using any of the following types of microelectronics in the system/capability:

- 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 and COTS components.

Each type of microelectronics has a corresponding set of HwA protection measures that programs can apply.

DoD Components can acquire ASICs with a DoD end use from a Defense Microelectronics Activity (DMEA)-accredited supplier. Components can include the requirement for a trusted process flow in the solicitation, directing the use of a DMEA-accredited Trusted Supplier.

During source selection for ASICs and GOTS, the PM should require, based on criticality, 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, PMs can pursue independent verification and validation options based on perceived residual risk.

Mitigations for COTS programmable microelectronics, when DoD end use is apparent, include the use of security keys and verification of field programmable gate array (FPGA) hardware and programming to avoid malicious reprogramming. DoD Components should consider procuring critical components that are COTS programmable microelectronics, if available, 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 for microelectronics that DoD Components identify as critical components. It should also require the contractor to use configuration management, parts management, and purchasing systems to manage the sourcing decisions and custody controls for microelectronics to reduce the likelihood of malicious attacks.

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 bill of material, provide the PM with a disciplined way of coordinating SCRM considerations (to include HwA) during microcircuit selection, acquisition, and sustainment. They also facilitate the monitoring of the supply chain for possible product or source changes requiring the reassessment of HwA risk.

Additionally, these processes convey special sourcing and handling considerations, e.g., chain of custody recording and bonded storage, for critical components to the logistics and purchasing communities.

The Joint Federation Assurance Center (JFAC) includes subject matter experts from across the Department who are available to advise programs on options to mitigate vulnerabilities related to microelectronics.

Table 6 provides an overview of HwA activities that DoD programs should consider throughout the DoD acquisition life-cycle. The HwA activities, used in combination with the SCRM activities listed in Table 8 in Section 3.6.5, can mitigate vulnerabilities involving microelectronics. In the P&D and O&S phases, DoD expects that programs will update the analysis periodically to the level of detail of the Product Baseline as upgrades to the system are made.

Table 6: HwA Activities throughout the DoD Acquisition Life-cycle

DoD Acquisition Technical Review	HwA Activities
ASR	• Identify notional critical functions to implement with microelectronics. • 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 DoD requires for program critical components.
SFR	• Identify all microelectronic critical components as well as the embedded software, intellectual property, interfaces, and tools that suppliers use to program the component. • Select protection measures to include selective testing, vetting of intellectual property, and tools. • Update SOW for critical microelectronics suppliers, as well as for verification and validation acceptance criteria.

DoD Acquisition Technical Review	HwA Activities
PDR	• Confirm use of DMEA-accredited Trusted Suppliers for ASICs for microelectronics designed for DoD custom end use, as appropriate. • 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 are in place. • Identify all microelectronic critical components as well as the embedded software, intellectual property, tools, etc., used to program them. • Confirm and revise protection measures, to include selective testing, vetting of intellectual property, tools, etc., that programs can use as needed.
CDR	• Update list of microelectronic critical components, to include the embedded software, intellectual property, tools, etc., used to program them. • Revise protection measures, as needed. • Initiate selective testing for malicious insertions where practicable, to include vetting and verification and validation of embedded software, intellectual property, and tools.
SVR/FCA, PRR/PCA	• Update list of microelectronics critical components to include the embedded software, intellectual property, tools, etc., used to program them. • Revise protection measures as needed. • Continue selective testing for malicious insertions. • When changes occur that could impact HwA, conduct an assessment of their impact and update the list of microelectronics and critical components and revise protection measures as needed. Example of such changes include: – Modifications to the capability. – Implementation of diminishing manufacturing sources and material shortages (DMSMS) resolutions. – Changes to the supply chain. – Changes to maintenance providers. – New vulnerabilities and weaknesses.

3.6.4 SwA Specialty

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 of the software.

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. Software vulnerabilities may be difficult and even take significant time and resources 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. Adversaries can target any software, most importantly those that perform mission critical functions.

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

- Undertake during development, integration, and test.
- Design to mitigate attacks against the operational system (i.e., the fielded system).
- Undertake to address threats to the development environment.

Table 7 illustrates a sequence of SwA activities that DoD Components can take across the DoD acquisition life-cycle of the software. In the P&D and O&S phases, DoD expects that programs will update the analysis periodically to the level of detail of the Product Baseline. Programs should tailor the SwA activities outlined in the system/capability specific characteristics, needs, and the development/operational environments. For example, some programs may use automation to produce SwA artifacts as part of a development, security, or operations pipeline, while others perform independent testing as part of a milestone/technical/gate review. Where appropriate, DoD encourages automated software vulnerability analysis tools and remediation techniques. Programs should consider protections inherited through the use of cloud infrastructure, platform, and software services as part of requirements definition, SwA activity selection, and cost/benefit trade-off analysis.

Table 7: SwA Activities throughout the DoD Acquisition Life-cycle

DoD Acquisition Technical Review	SwA Activities
ASR	• Contribute to selection of secure design and coding standards for software. • 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 DoD systems may be attacked via software (i.e., attack patterns). • Develop plan for software threat modeling, static analysis, software composition analysis (SCA), and dynamic analysis. • Identify technical expertise needed to assist with SwA activities.
SRR	• Select automated tools and establish toolchains for design, vulnerability scan/analysis, etc.

DoD Acquisition Technical Review	SwA Activities
	• Determine security requirements for programming languages, architectures, tool deployment and maintenance, development environment, and operational environment. • Develop plan for correlation and prioritization of SwA findings. • 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.
SFR	• Assess system requirements for inclusion of SwA. • Establish baseline architecture and review for weaknesses (e.g. CWEs) and susceptibility to attack (e.g. CAPEC); refine architecture to reduce potential attack surfaces and mission impacts.
PDR	• Review architecture and design against secure software design principles, which include, but are not limited to system element isolation, least-common mechanism, least privilege, fault isolation, input checking, and validation. • Confirm that SwA requirements are mapped to module test cases and to the final acceptance test cases. • Determine automated software security checks throughout the Software Development Life-Cycle (SDLC) and establish verification procedures and tools as a core process.
CDR	• Enforce secure coding practices through Code Inspection augmented by automated Static Analysis tools. • Analyze and track software composition including known vulnerabilities. • Detect vulnerabilities, weaknesses, and defects in the software; prioritize; and remediate. • Assess chain-of-custody from development through sustainment for any known remaining vulnerabilities and weaknesses and planned mitigations. • Confirm hash checking for delivered products. • Establish processes for timely remediation of known vulnerabilities (e.g., CVEs) in fielded commercial, COTS, and open source components. • Confirm planned and automated SwA testing provides variation in testing parameters and system configurations to maximize coverage. • Confirm that critical function software and critical components receive rigorous analysis and test coverage.
SVR/FCA, PRR/PCA	• Verify test resources, test cases, test scenarios, and test data. • Continue to enforce secure design and coding practices through inspections and automated scans for vulnerabilities and weaknesses.

DoD Acquisition Technical Review	SwA Activities
	• Maintain automated code vulnerability scans, reporting, and 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. • Review chain-of-custody across development, from development to sustainment, and during sustainment for the record of remaining weaknesses and vulnerabilities remaining and planned mitigations, as appropriate.

DoD Components should develop a SwA plan and statement of requirements for the software early in the life-cycle, and incorporate these requirements into the solicitation/RFP at each milestone. Components should then use that plan to track and measure SwA activities throughout the software life-cycle. Components should measure the progress toward achieving the plan by actual accomplishments/results that they report at each of the SETRs or other appropriate milestones as defined by the program.

Additional references and resources for SwA include the following:

- JFAC: The JFAC website (https://jfac.navy.mil/), contains a growing body of knowledge, expertise, and tools to support the Department's use of SwA.
- State of the Art Resource (SOAR) for Software Vulnerability Detection, Test, and Evaluation: This resource (https://www.ida.org/research-and-publications/publications/all/s/st/stateoftheart-resources-soar-for-software-vulnerability-detection-test-and-evaluation-2016) Discusses families of tools available for use in the implementation of SwA across the life-cycle.
- Software State of the Art Matrix (https://www.ida.org/research-and-publications/publications/all/s/st/stateoftheart-resources-soar-for-software-vulnerability-detection-test-and-evaluation-2016-app-e): This tool (https://www.ida.org/research-and-publications/publications/all/s/st/stateoftheart-resources-soar-for-software-vulnerability-detection-test-and-evaluation-2016-app-e) outlines the intended uses of various families of tools and the vulnerabilities they detect.
- NIST Secure Software Development Framework (SSDF) Version 1.1: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218-draft.pdf
- DoD Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRG): Security Technical Implementation Guides and SRGs (https://public.cyber.mil/stigs/) provide best practices for secure configuration and use of information systems/software that might otherwise be vulnerable to malicious attack.

- Open Web Application Security Project (OWASP): The OWASP (https://owasp.org/) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain trustworthy applications.
- CWE Portal: This is a community-developed dictionary (https://cwe.mitre.org/) of software weaknesses and types.
- CVE Portal: This is a community-developed dictionary (https://cve.org) of software vulnerabilities.
- CAPEC: This is a community-developed dictionary (https://capec.mitre.org/) of software attack patterns.
- DoD Developer's Guidebook for Software Assurance: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538756
- Program Manager's Guidebook for Software Assurance: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538771
- DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs: https://www.dau.edu/cop/risk/DAU%20Sponsored%20Documents/RIO%20Guide%20January2017%2017.pdf
- Department of Commerce, National Telecommunications and Information Administration The Minimum Elements for a Software Bill of Materials (SBOM): https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

3.6.5 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. SCRM is a means for understanding and managing these supplier risks. It can also identify 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, DoD Components should develop a set of SCRM practices and protection measures that minimizes intentional malicious activities and also detects and responds to supply chain attacks to hardware, software and firmware. These practices and protections include procurement activities as well as HwA and SwA activities for critical components in the system/capability.

DoD Components can incorporate SCRM practices and protection measures into solicitation through the DFARS Clause on Supply Chain Risk found in Section I of the FAR-based contract, and through requirements in the SOW. Example protection measures include use of secure shipping practices, exclusion of suppliers, and obscuring the intended end use of the component.

Table 8 provides activities to assess supply chain vulnerabilities and implement processes to increase supply chain security. In the P&D and O&S phases, DoD expects that programs will

update the analysis periodically to the level of detail of the Product Baseline. For any system upgrades, programs should give consideration to repeat analyses at the appropriate level of technical maturity detail.

Table 8: SCRM Activities throughout the DoD Acquisition Life-cycle

DoD Acquisition Technical Review	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. • 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 the SRD/system, performance specification, SOW, and other contract documents for the solicitation/RFP.
CDR	• Reassess supply chain vulnerabilities. • Update SCRM requirements for components based on the maturation of the system design. • Update SRD/system performance specification and relevant documents for future contract releases to reflect updated SCRM requirements.
SVR/FCA, PRR/PCA	• 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 National Institute of Standards and Technology (NIST) SP 800-161, current revision, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* located on the NIST website at https://pages.nist.gov/NIST-Tech-Pubs/SP800.html.

3.6.6 Cybersecurity Specialty

The RMF for DoD IT manages the life-cycle cybersecurity risk to DoD IT in accordance with the NIST Federal Information System and Organization information system policies, to include DoDI 8500.01 and DoDI 8510.01.

These are the activities related to selecting and implementing protections for information residing in, processed by, or transiting through the DoD system (either owned and operated by DoD, or on its behalf). These protections aim to ensure the confidentiality, integrity, and availability of information to preserve the assurance of the system/capability.

Table 9 lists activities over 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 9: RMF for DoD IT Activities throughout the DoD Acquisition Life-Cycle

DoD Acquisition Technical Review	RMF for DoD IT Activities
ASR	• Categorize the information types. • Select baseline requirements and potential cyber defense tools. • Incorporate cybersecurity requirements into the SRD/system performance specification and SOW, as appropriate.
SRR	• Refine derived system-level requirements. • Incorporate into specifications for the technical solution.
SFR	• Tailor the requirements. • Tailor and allocate requirements into system requirements. • Ensure the updated tailored requirements are included in the system functional baseline. • Incorporate functional requirements and verification methods into the initial RFP.
PDR	• Tailor and allocate requirements to the hardware and software design. • Incorporate tailored requirements into the SRD/system performance specification, SOW, and other contract documents for RFP.
CDR	• Tailor and allocate requirements to the hardware and software design. • Incorporate tailored requirements into the SRD/system performance specification, SOW, and other contract documents for RFP.

DoD Acquisition Technical Review	RMF for DoD IT Activities
	• Align the security assessment plan with the TEMP to ensure inclusion of testing.
SVR/FCA, PRR/PCA	• Monitor cyber defense tools and services. When changes occur that could impact the security of the cyber defense tools, conduct an assessment of their impact and determine mitigation approaches.

For more guidance on RMF for DoD IT, refer to:

- Department of the Air Force: Air Force Instruction 17-130.
- Department of the Army: Army Pamphlet 25-2.
- Department of the Navy: Secretary of the Navy Instruction 5239.3C.

3.7 Systems Security Engineering Cost/Benefit Trade-off Analyses

The program protection analyses and effort within each systems security engineering specialty provide the requisite knowledge for identifying risks and selecting protections. S&T managers and engineers should translate these analyses into an effective set of engineering requirements and reflect them in the design. One way of ensuring that security is properly incorporated into the system is through SCRE design principles. Additionally, programs should drive their decisions related to protection-measure selection by cost/benefit trade-off analyses, just as they are for any other design considerations.

Systems security engineering activities provide the means for analyzing and integrating the protections offered by each systems security engineering specialty to determine the most appropriate set of protection measures with the given cost, schedule, and performance constraints, which includes operational constraints.

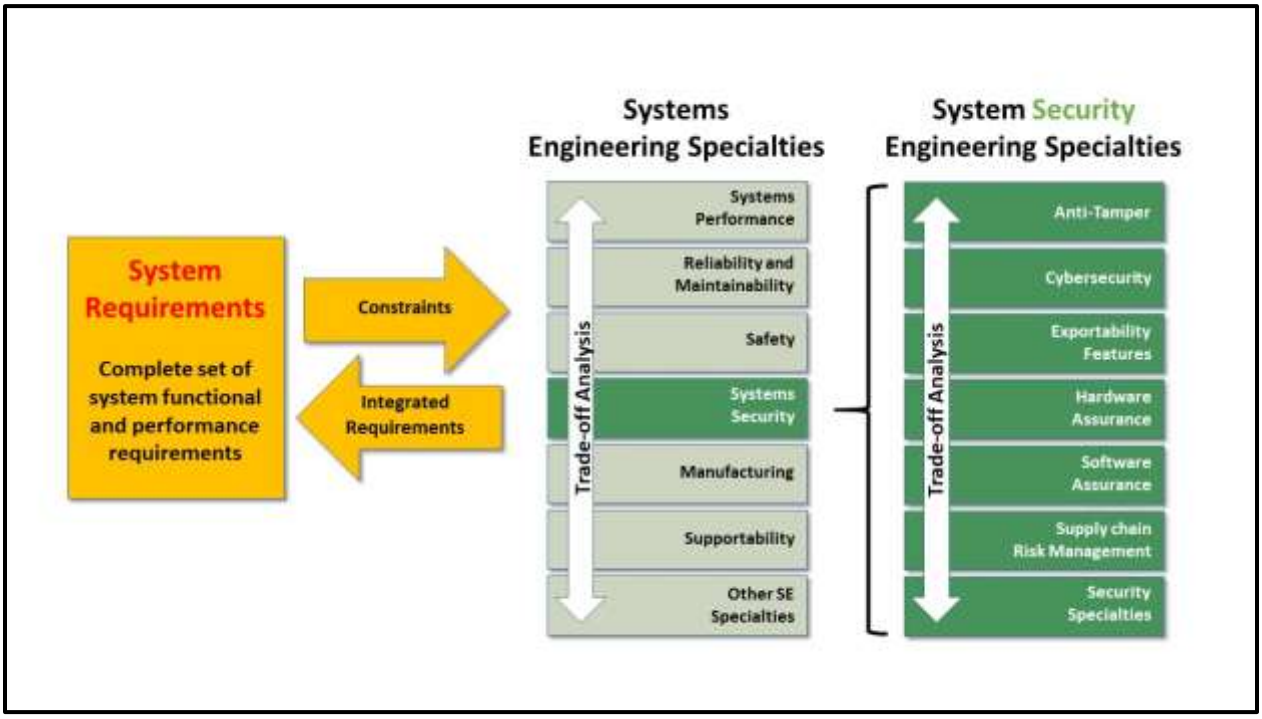
The typical method that S&T managers and engineers use for performing this analysis and integration is design cost/benefit trade-off analyses. Design cost/benefit trade-off analyses can assist SSEs in making tough choices among competing technology and program protection system requirements and protections in order to design a system solution within the constraints of cost, schedule, and performance - while still maintaining an acceptable level of risk.

There are two levels of cost/benefit trade-off analyses that include systems security as shown in Figure 3:

- At the systems security engineering level, the SSE performs trade-off analyses to integrate the proposed protection measures from each systems security engineering specialty into a single set of protection measures that most cost-effectively addresses the risks identified through technology and program protection analysis processes. This set becomes the systems security engineering input to the engineering requirements.

- At the system level, the engineer performs cost/benefit trade-off analyses to balance overall system performance, system attributes/design considerations (which includes systems security engineering as one consideration), cost, and schedule.

Figure 3: Systems Security Cost/Benefit Trade-off Analysis



There may be multiple iterations of these analyses, as the initial systems security engineering input (or portions of it) to the engineer's analysis may require reassessment due to a new constraint that the engineer must incorporate in the systems security engineering analysis. The integration of systems security engineering into the engineering requirements occurs regularly across the life-cycle of the system as the design matures. Throughout the analysis, the SSE will ensure that programs establish and incorporate testable requirements and derived requirements into the corresponding system requirements and test documents, as appropriate.

4 Program Protection Planning Activities in the MCA Life-Cycle Phases

Systems security engineering activities analyze the threats, vulnerabilities, risks and their vulnerability mitigations to CPI, mission-critical functions and critical components, CTI, and system data, with the results of these activities documented in the PPP. DoD expects the level of detail is commensurate with the level of the system specification, design, and implementation.

4.1 PPP Life-Cycle Expectations

The PPP is a living document, required at Milestones A, B, C, the Development RFP Decision Point, and the FRP DR or FDDR as described in the MPIR tables found at the MDID for the MCA and equivalent decision points for the other AAF pathways. It is a best practice to update the PPP when there is a change to the protection activities of the program, such as after contract award to reflect the contractor's approved technical approach; before export decisions; when the system transitions to operations and sustainment; and prior to each SETR event.

DoD Components should establish key systems security engineering criteria for each phase leading up to a major program milestone/decision event, and it is important to establish these criteria across the full life-cycle to build security into the system. PPP life-cycle considerations, in general, include the following:

- Iteratively perform program protection analyses to assess and manage systems security 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 systems security engineering 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 the SOW and the SRD/system performance specification.
- Identify PPP life-cycle resources needed to ensure sustainability of protection measures in operations.

4.2 Systems Security Engineering Activities in Life-Cycle Phases

Within each acquisition life-cycle phase, the maturity of the system/capability drives program protection activities and outcomes. As the system/capability matures, programs iteratively update program protection analyses and support the development of the PPP for each major milestone and the appropriate decision point.

The technical maturity, design flexibility, operational constraints, and operational needs will inform the systems security engineering activities and actions that programs take for each of the AAF pathways.

4.2.1 Pre-Materiel Development Decision

Based on the technical maturity of the system/capability, the focus of program protections is to begin to identify systems security risks based on the range of candidate materiel solution approaches. This program protection information supports the MDA's decision to authorize

entry into the acquisition life-cycle and pursue a materiel solution. A PPP is not required for the MDD.

4.2.2 Materiel Solution Analysis Phase

Based on the technical maturity of the systems/capability, the focus of program protection is to document the repeatable processes, methodologies, and resources to identify and mitigate systems security risks. This program protection information supports the Milestone A (MS A) or equivalent decision by providing evidence that the program has adequately addressed systems security risks, given the technical maturity point.

During this phase, the program develops an MDA approved PPP for the MS A or equivalent decision, which meets the systems security engineering objectives described in the ASR.

Additionally, DoD Components should incorporate program protection requirements into the SRD/system performance specification and SOW during the development of the draft RFP supporting the TMRR phase, or equivalent, as appropriate.

4.2.3 Technology Maturation and Risk Reduction Phase

Based on the technical maturity of the system/capability, the focus of the PPP is to describe and document the plan, repeatable processes and methodologies, performed analyses, and resources to identify and mitigate systems security risks. This key program protection information is to support the Milestone B (MS B) or equivalent decision by providing evidence that the program has adequately addressed systems security risks, given the technical maturity point.

During this phase, DoD requires the program to develop an updated DoD Component-approved draft PPP for the Development RFP Release Decision Point that meets the SRR and SFR systems security engineering objectives. DoD also requires the program to have an approved PPP for the MS B decision, which meets the PDR level systems security engineering objectives.

Additionally, Components should incorporate program protection requirements into the SRD/sub-system specifications and SOW to support the EMD phase and LRIP, or equivalent, solicitation RFP as appropriate.

4.2.4 Engineering and Manufacturing Development Phase

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

During this phase, DoD requires the program to have an approved PPP for the MS C or equivalent decision that meets the CDR systems security engineering objectives, even if the program did not conduct a formal CDR. DoD Components should deliver and maintain intermediate products supporting systems security engineering activities, such as the product requirements and architecture, 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 during this phase.

Additionally, DoD programs should continue to incorporate program protection requirements into the SRD/system performance specification and SOW to include the parts selection processes when developing the P&D phase or equivalent solicitation/RFP, as appropriate.

4.2.5 Production and Deployment Phase

Based on the system technical maturity of the system/capability, the focus of the PPP is to describe and document the plan, repeatable processes and methodologies, results of the performed analysis, and resources to identify and mitigate systems security risks. The key program protection information is to support the FRP decision, FDD, or equivalent Decision by providing evidence the program has adequately addressed systems security risks given the technical maturity point.

During this phase, DoD requires the program to have an updated PPP that supports the FRP, FDD, or equivalent Decision Review that reflects the PCA-verified product baseline. The PPP should include content to the level of detail provided in a Bill of Materials (BOM), as well as the systems security engineering objectives described in the PCA. The PPP should describe plans to phase in any needed systems security risk mitigations resulting from risk based on updated threat, vulnerability, and critical component selection changes prior to Initial Operational Capability and Full Operational Capability.

Additionally, DoD programs should continue to incorporate program protection requirements into the SRD/system performance specification and SOW during the development of the solicitation/RFP in support of the FRP DR or FDD (or equivalent) as appropriate.

4.2.6 Operations and Sustainment Phase

While the primary emphasis of program protection is the activities and protections that S&T managers and engineers incorporate during the design and acquisition phases of a system/capability, it is also important to consider the protections needed when programs maintain and sustain the system during the O&S phases. The focus of the PPP is to support the maintenance and sustainment of the CPI, critical components, and the CTI that S&T managers and engineers use during this phase of the program. Repair depots, for example, should be aware of the cyber defense technology used in the system, the CPI, mission-critical functions and components, as well as the marking and distribution statements on CTI and the system data they are maintaining so that the depots can appropriately protect these items from compromise and unauthorized disclosure.

Sustainment planning and execution span across the life-cycle for each of the AAF pathways, from MS A analysis to disposal. Sustainment planning should be flexible, and it should accommodate modifications, upgrades, and re-procurement. The sustainment plan should be a part of the program's Acquisition Strategy, and programs should integrate it with other key program planning activities, as appropriate (e.g. PPP and Life-Cycle Sustainment Plan).

5 Program Protection in Technical Reviews and Audits

S&T managers and engineers use SETRs and audits to measure the technical health of the program, measure technical maturity progress to plan, establish the technical baseline, and assess technical risks. The following subparagraphs provide the systems engineering criteria for use as part of the SETR and audit entrance/exit criteria to assess and ensure that S&T managers and engineers consider an appropriate level and discipline of systems security engineering activities in the design, development and fielding of the system/capability.

5.1 Alternative Systems Review

The objectives for the ASR are defined in Table 10.

Table 10: ASR Objectives

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
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 MS A or equivalent criteria.

5.2 System Requirements Review

The objectives for the SRR are defined in Table 11.

Table 11: SSR Objectives

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
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, or equivalent; (2) plan for technology maturation; and (3) maturity of interdependent systems.

5.3 System Functional Review

The objectives for the SFR are defined in Table 12.

Table 12: SFR Objectives

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
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.

5.4 Preliminary Design Review

The objectives for the PDR are defined in Table 13.

Table 13: PDR Objectives

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

5.5 Critical Design Review

The objectives for the CDR are defined in Table 14.

Table 14: CDR Objectives

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
CDR	Recommendation to start fabricating, integrating, and testing test articles with acceptable risk.	Product design is stable. Initial product baseline established.	Initial product baseline established by the system detailed design documentation; affordability/should-cost goals confirmed. Government assumes control of initial product baseline as appropriate. Configuration Management Process for a description of baselines.

5.6 System Verification Review/Functional Configuration Audit

The objectives for the SVR/FCA are defined in Table 15.

Table 15: SVR/FCA Objectives

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

5.7 Production Readiness Review

The objectives for the PRR are defined in Table 16.

Table 16: PRR Objectives

DoD Acquisition Technical Review	Objective	Technical Maturity Point	Additional Information
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.

5.8 Physical Configuration Audit

The objective for the PCA is defined in Table 17.

Table 17: PCA Objectives

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

6 Technology and Program Protection Planning Considerations

The activities to execute systems security engineering for technology and program protection are closely coupled with other planning activities in the conduct of defense research and acquisition. This section provides information on how technology and program protection informs or is informed by other aspects of defense acquisition.

6.1 Contracting for Program Protection Planning

The SSE has a key role in ensuring program protection-related requirements (i.e., features in the system design, or methods and processes that S&T engineers used to develop the technology and/or the system/capability) are included in contracts and solicitations. The content of the most current PPP, results of related technology and program protection analyses, and the SRD/system performance specification drive the content of the solicitation/RFP.

Solicitations/RFPs may be issued for each AAF path and acquisition life-cycle phase. Align the systems security engineering content to the technical maturity of the system engineering baselines established at the most recent technical review.

Section C: Description/Specification/Work Statement. The following are ways in which DoD Components can incorporate protection measures into Section C of the solicitation/RFP:

- Protection measures that specify the system requirements are in the SRD/system performance specification, and found in Section J.
- Protection measures that describe how the contractor will develop the system (i.e., supply chain protections or software development standards) are added to the contract in the

SOW. This includes describing program protection analysis (e.g. TSN and CPI, as applicable) that the contractor will perform during the contract to identify additional protection measures are added in the SOW.

- Protection measures requiring the contractor to provide supporting documentation to the government become a CDRL, with a DID that provides the expected content; the requirement is in the SOW, the CDRL is included in Section J.

Section I: Contract Clauses. Table 18 contains relevant FAR and DFARS clauses for DoD Components to consider in Section I of the solicitation/RFP and their application in the contract. Components can also apply the requirements contained in these regulations, when applicable, to legally binding instruments other than procurement contracts, such as grants, cooperative agreements, and cooperative research and development agreements.

Table 18: Relevant FAR and DFARS Provisions for Program Protection

Relevant FAR and DFARS Provisions/Clauses for Program Protection and Associated Contractor Requirements	
Requirements for Federal/ DoD Systems	**FAR clause 52.204-2, Security Requirements** • Applies when Federal Government information classified as "Confidential," "Secret," or "Top Secret" is released to contractors, licensees, and grantees of the U.S. Government. • The contractor shall comply with the Security Agreement DD Form 441, including the NISPOM (32 CFR part 117); and any revisions to that manual, notice of which the Federal Government has furnished to the Contractor.
	DFARS provision 252.239-7009, Representation of Use of Cloud Computing and DFARS clause 252.239-7010, Cloud Computing Services • Applies when using cloud computing to provide DoD with IT services in accordance with the Cloud Computing SRG (https://dl.dod.cyber.mil/wp-content/uploads/cloud/zip/U_Cloud_Computing_SRG_V1R4.zip). • The contractor shall implement/maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing SRG (https://dl.dod.cyber.mil/wp-content/uploads/cloud/zip/U_Cloud_Computing_SRG_V1R4.zip). • The contractor shall report all cyber incidents that are related to the cloud computing service to DoD via https://dibnet.dod.mil/.
Requirements for Non-Federal/ Contractor Systems	**DFARS provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls and DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting** • Requirements apply to all covered contractor information systems – unclassified system owned, or operated by or for, a contractor and that processes, stores, transmits DoD CUI. • Require contractors to provide adequate security to safeguard DoD CUI on a contractor's internal information system or network and to report cyber incidents (and support damage assessment as required) that affect contractor system or DoD CUI residing therein, or that affect contractor's ability to provide operationally critical support.

	DFARS Provision 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements and DFARS Clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements • Apply when contractor must implement NIST SP 800-171 as directed in DFARS 252.204-7012. • If offeror/contractor is required to implement NIST SP 800-171, it must have summary level scores of current NIST SP 800-171 DoD Assessment of relevant information systems/networks posted in Supplier Performance Risk System (SPRS), and must provide Government access to facilities, systems, and personnel necessary for DoD to conduct a Medium or High NIST SP 800-171 DoD Assessment. • Requires the contractor to include the substance of the clause, in all subcontracts and other contractual instruments, including subcontracts for commercial items but excluding COTS items. • Contractor shall not award a subcontract or other contractual instrument that is subject to the implementation of NIST SP 800-171, in accordance with DFARS clause 252.204-7012, unless the subcontractor has completed at least a Basic NIST SP 800-171 DoD Assessment.
Requirements for SCRM	**DFARS provision 252.239-7017, Notice of Supply Chain Risk and DFARS 252.239-7018, Supply Chain Risk and DFARS clause 252.239-7018** • Applies to IT procurements for services or supplies as a covered system (i.e., National Security System NSS), as a part of a covered system, or in support of a covered system. • Implements the use of supply chain risk as an evaluation factor to minimize the potential risk for supplies and services purchased by DoD to maliciously degrade the integrity and operation of sensitive IT systems.
	DFARS clause 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System (Contractors subject to Cost Accounting Standards only) • Applies when procuring electronic parts; end items, components, parts, or assemblies containing electronic parts; or services where the contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the service. • The contractor shall establish and maintain an acceptable counterfeit electronic part detection and avoidance system. Failure to maintain an acceptable counterfeit electronic part detection and avoidance system, as defined in this clause, may result in disapproval of the purchasing system by the Contracting Officer and/or withholding of payments.
	DFARS 252.246-7008, Sources of Electronic Parts • Applies when procuring electronic parts; end items, components, parts, or assemblies containing electronic parts; or services, if the contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the service. • Addresses required sources of electronic parts for defense contractors and subcontractors, to include 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.

Section J: List of Documents, Exhibits, and Other Attachments. Section J lists the solicitation/RFP attachments. The following are examples of documents, exhibits, and other attachments that can be found in Section J:

- CDRLs. In each CDRL, the government indicates the distribution statement with which to mark the contractor's deliverable.
- Government Furnished Information (GFI). For each GFI that the Federal Government provides to the contractor that involves CTI, the engineer is responsible for applying the appropriate marking and dissemination statements. Examples of GFI includes the SEP, SRD, PPP.
- DD Form 254. This form provides necessary security requirements for the contractor when the contractor will be handling classified information, as required by the NISP policy.
- Relevant SCG. Use the relevant SCG the contract involves 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.

6.2 Intelligence, Counterintelligence and Security Support

Technology and program protection processes and analyses rely on intelligence, counterintelligence, and security inputs to better understand adversary warfighting capabilities, technological maturity, and Foreign Intelligence Entities (FIE) capabilities. The inputs provide a more complete description of:

- Threats to CTI, 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 to inform:

- Information, CPI, and TSN analysis – What measures are most effective against a perceived or actual threat?
- TSN analysis – What components are affected by a threat to a supplier?
- CPI analysis – What capabilities are above and beyond those of our adversaries? What capabilities have the adversaries compromised?
- Information analysis – What classified information and CTI has been affected by a cyber incident? What information has the incident compromised? What information has been lost? Are there threats to facilities with classified, unclassified CTI, and/or unclassified information, and are these facilities adequately protecting the technical information in accordance with the applicable requirements in the FAR/DFARS?

DoD Components should request these intelligence, counterintelligence, and security products/reports throughout the technology and system 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).

6.3 Joint Acquisition Protection and Exploitation Cell

The Joint Acquisition Protection and Exploitation Cell (JAPEC) in OUSD(R&E) facilitates collaboration with the intelligence, counterintelligence, law enforcement, and acquisition communities on technology protection and analysis of CTI protection gaps. This analysis informs S&T managers and engineers on the courses of action that they must take to mitigate the risks associated with losing CTI.

The JAPEC integrates and coordinates analyses of gaps in protection of CTI. The JAPEC enables increased efforts across DoD to proactively mitigate future losses and exploit opportunities to deter, deny, and disrupt adversaries that may threaten U.S. military advantage. JAPEC activities include:

- Integrating all-source intelligence, counterintelligence, law enforcement, and acquisition information to improve protection of CTI, which is common across projects, programs and capabilities, and provide scalable options for providing protection measures to address the increasing adversary threat to technologies used in DoD capabilities.
- Facilitating the identification of essential technology elements to maintain DoD advanced capabilities in technologies and programs.
- Providing referrals to the Military Departments' Counterintelligence Organizations (MDCO) or other Defense Agencies providing counterintelligence support for incidents involving compromised CTI.
- Incorporating best practices for CTI protection.

The JAPEC assists in information analysis and provides recommendations to projects and programs addressing the risks associated with compromised controlled technical information. The JAPEC expertise is available to projects and programs to support analyses and recommendations on protection methodologies. JAPEC analysis and recommendations include:

- Project and program adjustments, including accelerating alternative technologies.
- Warfighting updates (e.g., updating tactics, techniques, and procedures).
- Capability requirements adjustments to address a change in threat.
- Education and training in threats or counterintelligence.
- Recommendations on increased or enhanced protective features.

Additional information on JAPEC can be found on the OUSD(R&E) website: https://rt.cto.mil/stpe/mta/.

6.4 Joint Federated Assurance Center

The Joint Federated Assurance Center (JFAC), which resides under OUSD(R&E), is a federation of DoD organizations that have a variety of SwA and HwA capabilities to support programs. The JFAC facilitates vulnerability detection, analysis, and remediation capabilities through a federation of organizations and facilities from the Military Departments, Defense Agencies, and other federal departments and agencies.

Program offices have access to assurance best practices, automated analysis tools, S&T assurance capabilities, and common vulnerability mitigations from across the Military Departments, Defense Agencies, and other federal departments and agencies through the JFAC website: https://jfac.navy.mil.

6.5 TAPPs

TAPPs are management tools to establish technology and program protection measures applied to critical technology areas established by OUSD(R&E). The OUSD(R&E) establishes and maintains a TAPP for each critical technology area to inform technology and program protection activities involving emerging and disruptive research trends, and to horizontally reduce compromise or loss of critical technologies and protect against unwanted technology transfer.

OUSD(R&E) critical technology areas are located at: https://www.cto.mil/modernization-priorities/.

Additional information on TAPPs can be found at: https://www.dodtechipedia.mil/dodc/x/U6OEKQ.

6.6 S&T Protection Plan

The S&T Protection Plan is a management tool to guide S&T protection activities involving applicable critical technology areas and applicable horizontal protection guidance.

S&T protection activities and the implemented protection measures inform the program protection activities and protection measures when they transition to an acquisition program. S&T protection activities include:

- Including S&T protection requirements in legally binding agreements such as FAR-based solicitations, broad agency announcements, and Other Transaction Authority agreements, as appropriate.
- Preparing updates to the S&T Protection Plan as technology matures, when the threat changes, or there is a compromise.

The DoD Component determines the S&T Protection Plan approval authority.

Additional information on the S&T Protection Guide, S&T Protection Plan, and expectations for S&T protections can be found at the following link: https://www.dodtechipedia.mil/dodc/download/attachments/696558266/S%26T%20Protection%20Plan%20Template_Updated_20210331_cleared.docx?version=1&modificationDate=1625852583000&api=v2.

6.7 PPP

The PPP is a living plan to manage the risks to U.S. capability element that contributes to the warfighter's technical advantage, mission-critical functions and components, CTI, and system data. This acquisition document captures the systems security engineering activities, to include secure cyber resilient engineering, and the results of the analyses across the life-cycle.

Programs should employ systems security engineering practices to prepare a PPP using the PPP Outline and Guidance (https://acqnotes.com/wp-content/uploads/2018/04/PPP-Outline-and-Guidance-v1-July2011.pdf). Components should tailor the PPP as necessary to meet the characteristics of the system the Component is acquiring. Engineers should also ensure that they incorporate security considerations 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 Component should submit cybersecurity strategy as an appendix to the PPP in accordance with DoDI 5000.82. At a minimum, the Component should update the PPP to reflect: the systems security and cyber risks and related mitigations assessed at each technical review; after contract award to reflect contractor implementation; and after identification of any significant threat activity or compromise.

For MCA programs where the Defense Acquisition Executive (DAE) is the MDA, the programs should submit PPPs to Director, S&T Program Protection not less than 45 calendar days before the relevant review for USD(R&E) approval. DoD Component PPPs will follow the DoD Component approval process.

Addressing the systems security risks to a program and system does not stop once the design ends; the program is responsible for minimizing risk using program protection techniques throughout the life-cycle, including when the system is in operation. The vulnerabilities and threats to the operational environment, supply chains, and components are constantly changing, impacting the operational risk to the warfighter. To manage the risks to the warfighter, it is important that the program protection planning responsibilities transition after the FRP DR or FDD to the PM responsible for system sustainment and disposal.

6.8 System Engineering Plan

The Systems Engineering Plan (SEP) is used to describe the systems engineering and engineering management approach and processes that guide the program's technical activities. The technology and program protection activities are consistent with the program's engineering and technical management processes.

Additional information on the SEP can be found at the following link: https://ac.cto.mil/erpo/.

6.9 Test and Evaluation Master Plan

The Test and Evaluation Master Plan (TEMP), test strategy, or other pathway-appropriate test plan/strategy document are the planning and management tools for the integrated test and

evaluation of the system. The technology and program protection activities inform the program's DT&E and OT&E requirements. The results of program protection analyses, which are documented in the PPP, may generate requirements that the T&E should address.

The PPP informs the T&E activity's understanding of system requirements, including the system's mission-critical functions and critical components, such as software vulnerabilities and cyber defense tools. When developmental testing begins, the DT&E test lead provides the SSE with test results, which programs should analyze to determine if the system meets the specified requirements. The results of the analysis may suggest the need to refine requirements or make engineering changes to improve program protection.

Additional information on T&E can be found at the following link: https://www.dote.osd.mil/Publications/DOT-E-TEMP-Guidebook/ .

6.10 Life-Cycle Sustainment Plan

The Life-Cycle Sustainment Plan (LCSP) describes the program's planning and execution for O&S. The LCSP informs the technology and program protection activities involving:

- Maintenance concept, including where and by whom maintenance will be performed.
- Supply support, including supply sources.
- Packaging, handling, storage, and transportation concepts.
- Facilities and infrastructure where product support is provided.
- Support equipment, including test equipment directly interfacing with the system/capability.

Additional information on the LCSP contents can be found on the following link: https://www.dau.edu/tools/Lists/DAUTools/Attachments/12/LCSP Plan Outline Version 2.0 - 19 Jan 2017.pdf for expected LCSP contents.

7 Technology and Program Protection in the AAF

The purpose of the Defense Acquisition System is to deliver effective and affordable solutions to the end user while enabling execution at the speed of relevance. To achieve that objective, DoD employs an AAF comprised of acquisition pathways (provided at https://aaf.dau.edu/aaf/), each tailored for the unique characteristics and risk profile of the capability the program is acquiring.

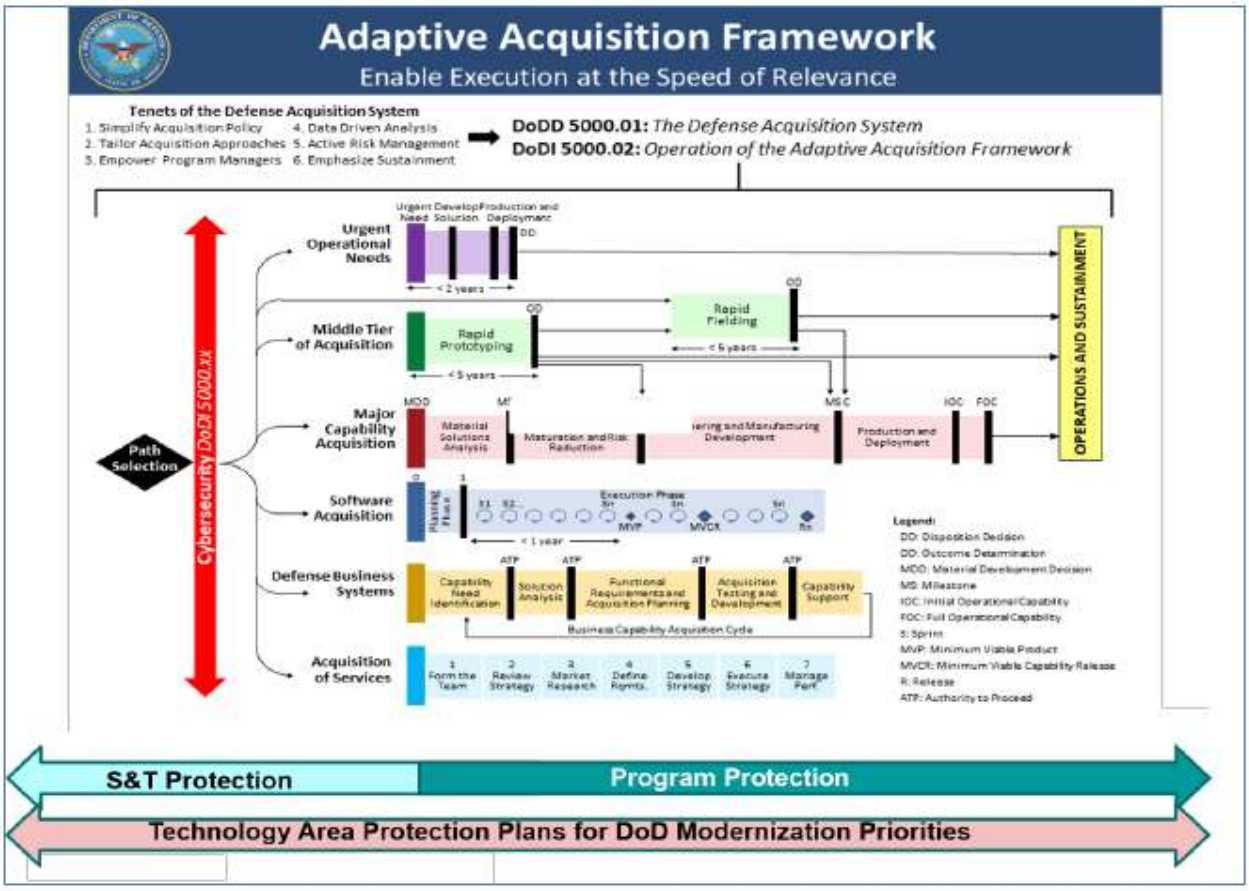
Technology and program protection planning activities, which includes information analysis, TSN analysis, and CPI analysis (inherited or organic) will be tailored for the:

- Selected acquisition pathway.
- Anticipated risks the program will encounter.

Engineers will tailor program protection planning and oversight, content, timing, and scope of protection measures based on the characteristics of the capability they are acquiring, including complexity, risk, and urgency to satisfy user requirements.

The following sections provide expectations for the AAF pathways. The AAF pathways are shown in Figure 4.

Figure 4: The AAF Pathways

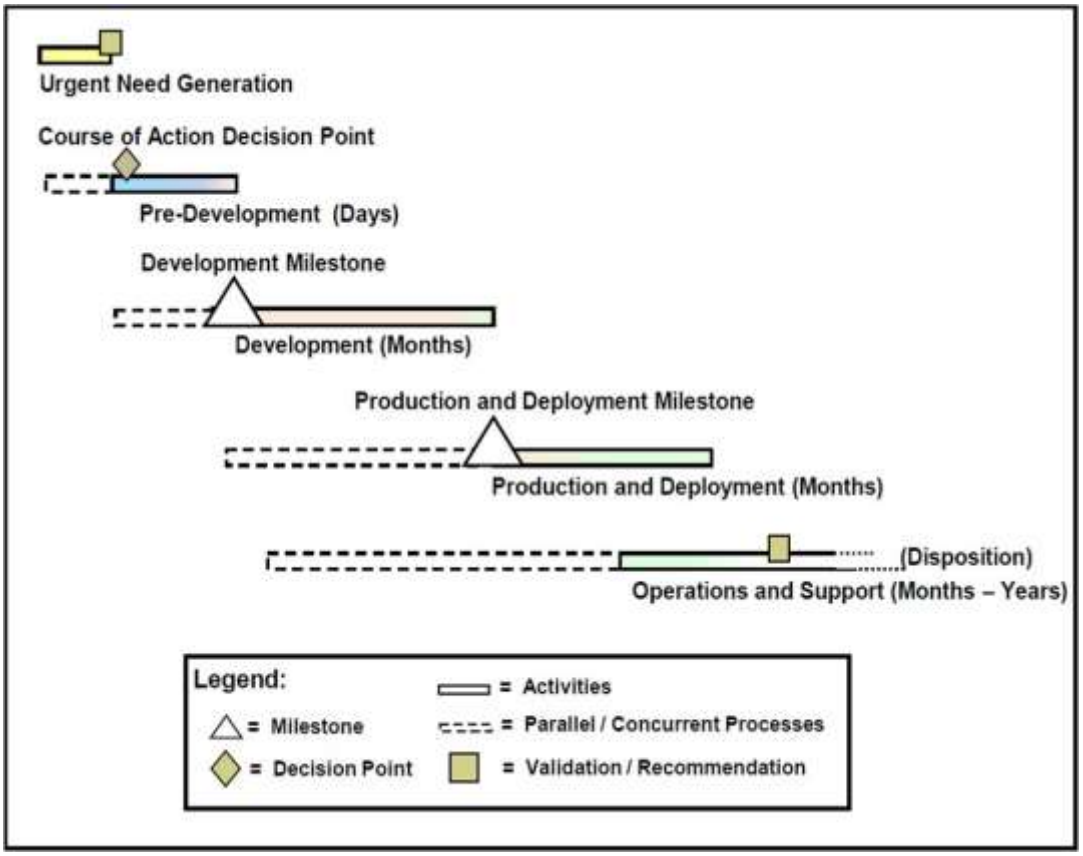


7.1 Urgent Capability Acquisition

The Urgent Capability Acquisition pathway, DoDI 5000.81, is intended to fulfill urgent operational needs and other quick reaction capabilities with a capability that can be fielded in less than two years.

Figure 5 depicts representative urgent capability acquisition activities to support fielding a quick reaction capability.

Figure 5: Urgent Capability Acquisitions



Development includes an assessment of the performance, safety, suitability, survivability, supportability, including software, and lethality, if appropriate. It does not require that all identified deficiencies, including those related to safety, be resolved prior to production or deployment. The MDA will, in consultation with the user community and the requirements validation authority, determine which deficiencies programs must resolve and what risks they can accept. The accepted risks will allow the user community to develop tactics, techniques, and procedures to help minimize the operational risks. Designated approval authorities will expeditiously make certification determinations and issue interim authorization to test or authorization to operate.

This pathway should utilize the activities in information analysis, TSN analysis and CPI analysis, which incorporate activities necessary for cybersecurity. TSN analysis should be commensurate with the level of technical maturity of the system, the availability of the threat, and known vulnerabilities.

7.2 Middle Tier of Acquisition

The Middle Tier of Acquisition (MTA) pathway, DoDI 5000.80, is intended to fill a gap in the DAS for those capabilities that have a level of maturity to allow DoD Components to rapidly prototype or field them within an acquisition program or within five years of MTA program start. Components may use the MTA pathway to accelerate capability maturation before transitioning to another acquisition pathway, or may use it to minimally develop a capability before rapidly fielding. The MTA pathway includes two paths: Rapid Prototyping and Rapid Fielding. The level of maturity enables MTA rapid prototyping within five years and rapid fielding initiation within six months (unless waived by the DAE) and completion of rapid fielding within five years. PMs will ensure that their programs identify and reduce operational, technical, and security risks so that fielded systems are capable, effective, and resilient. PMs will comply with statutory requirements unless waived in accordance with relevant provisions.

Major systems intended to satisfy requirements that are critical to a major interagency requirement or are primarily focused on technology development, or have significant international partner involvement, are discouraged from using the MTA pathway.

MTA programs will not be subject to the guidance in Operations of the Joint Capabilities Integration and Development System (JCIDS) and the Defense Acquisition System. MTA programs will follow their DoD Component streamlined process that results in a succinct requirement document no later than six months from the time the Component initiates the operational needs process.

DoD Component-required procedures will be compliant with applicable statutes and be consistent with the requirements for acquisition programs stated in this issuance. When necessary, Components will submit requests for waivers to the provisions of this issuance to the DAE.

7.2.1 Rapid Prototyping Path

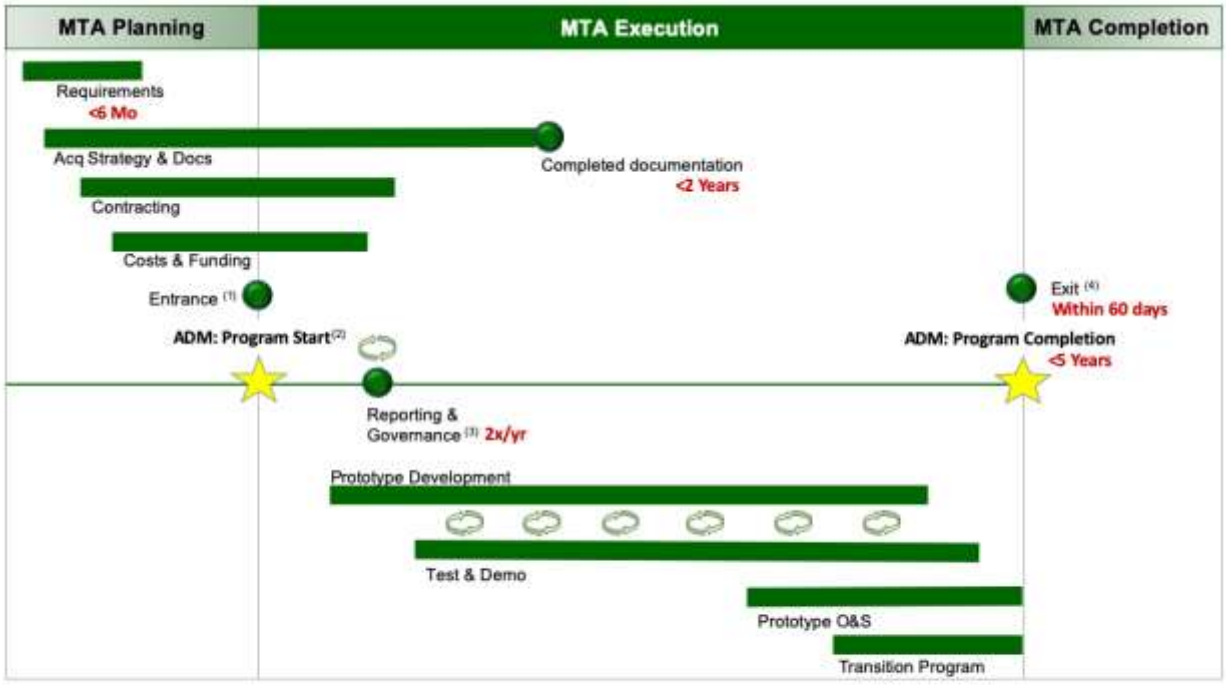
The rapid prototyping path provides for the use of innovative technologies to rapidly develop fieldable prototypes to demonstrate new capabilities and meet emerging military needs. The objective of an acquisition program under this path will be to field a prototype, meeting defined requirements that the program can demonstrate in an operational environment and provide for a residual operational capability within five years of the MTA program start date. Virtual prototyping models are acceptable if they result in a fieldable residual operational capability.

DoD Components may not plan MTA programs to exceed five years to completion and, in execution, will not exceed five years after MTA program start without DAE waiver.

This pathway should utilize the activities in information analysis, TSN analysis and CPI analysis, which incorporate activities necessary for cybersecurity. TSN analysis should be commensurate with the level of technical maturity of the system, and the availability of the threat and known vulnerabilities.

Figure 6 outlines key activities and artifacts of the two phases that enable rapid prototyping development and delivery.

Figure 6: MTA Rapid Prototyping Path



(1) *Major Systems*: Acquisition Decision Memorandum(ADM) signed by the Decision Authority (DA), Acquisition Strategy (which includes [1] Security, Schedule & Production Risks; [2] Test Strategy/Results; and [3] Transition Plan), and Program Identification Data (PID)
Non-Major Systems: ADM signed by the DA, PID
(2) Major Defense Acquisition Programs (MDAPs) require Under Secretary of Defense for Acquisition & Sustainment (USD(A&S)) Prior Written Approval
(3) Updated PID submitted twice a year with President's Budget and Program Objective Memorandum submissions to Office of Secretary of Defense (OSD)
(4) Signed Outcome ADM, Final PID, Assessment of Test Results

7.2.2 Rapid Fielding Path

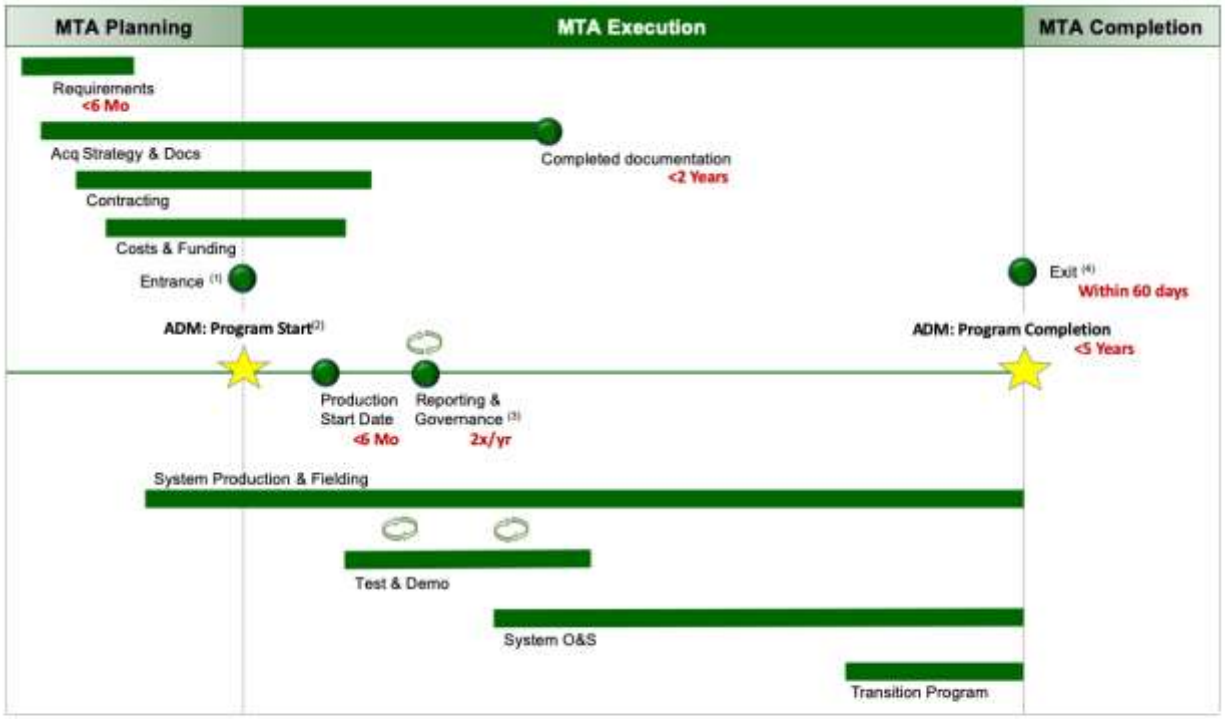
The rapid fielding path provides for the use of proven technologies to field production quantities of new or upgraded systems with minimal development required. The objective of an acquisition program under this path will be to begin production within six months and complete fielding within five years of the MTA program start date. MTA program production start date will not exceed six months after MTA program start date without DAE waiver. DoD Components may

not plan MTA programs to exceed five years to completion and, in execution, will not exceed five years after MTA program start without DAE waiver.

This pathway should utilize the activities in information analysis, TSN analysis and CPI analysis, which incorporate activities necessary for cybersecurity. TSN analysis should be commensurate with the level of technical maturity of the system, and the availability of the threat and known vulnerabilities.

Figure 7 outlines key activities and artifacts of the two phases that enable rapid fielding development and delivery.

Figure 7: MTA Rapid Fielding Path



(1) Major Systems: Acquisition Decision Memorandum(ADM) signed by the Decision Authority (DA), Acquisition Strategy (which includes [1] Security, Schedule & Production Risks; [2] Test Strategy/Results; and [3] Transition Plan), and Program Identification Data (PID)
Non-Major Systems: ADM signed by the DA, PID
(2) Major Defense Acquisition Programs (MDAPs) require Under Secretary of Defense for Acquisition & Sustainment (USD(A&S)) Prior Written Approval
(3) Updated PID submitted twice a year with President's Budget and Program Objective Memorandum submissions to Office of Secretary of Defense (OSD)
(4) Signed Outcome ADM, Final PID, Assessment of Test Results

7.3 Major Capability Acquisition

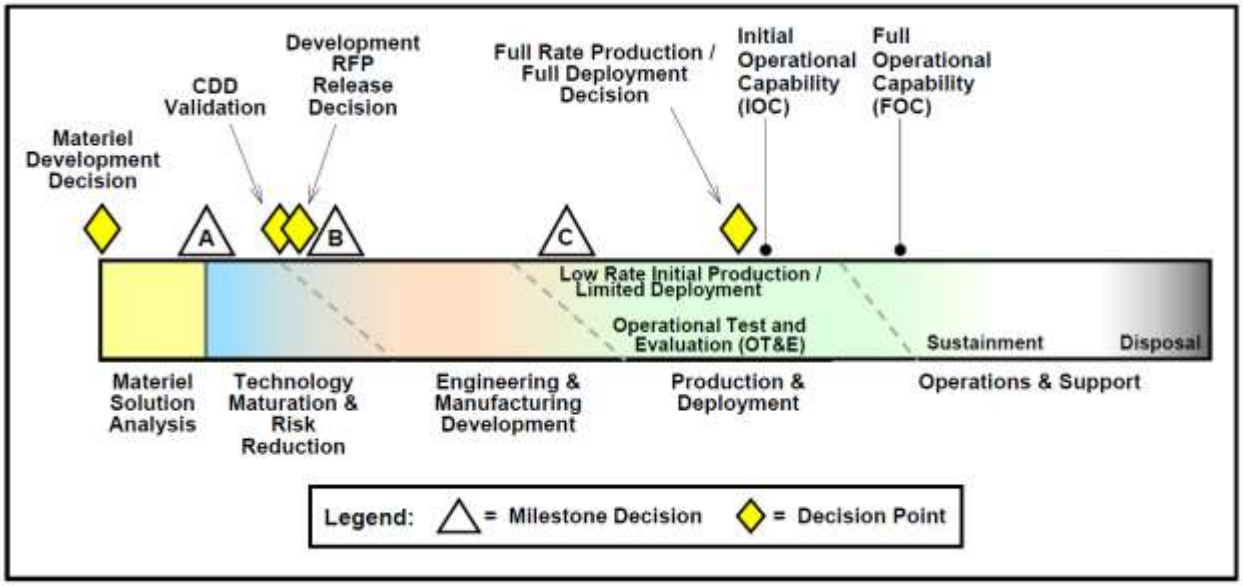
The major capability acquisition path, established in DoDI 5000.85, is intended for a rapid, iterative approach to capability development to reduce cost, avoid technological obsolescence, and reduce acquisition risk. Consistent with that intent, acquisitions will rely on mature, proven technologies and early testing. Planning will capitalize on commercial solutions and non-

traditional suppliers, and expand the role of warfighters and security, counterintelligence, and intelligence analysis throughout the acquisition process.

This pathway utilizes validated requirements to define the products that programs will acquire through the acquisition system. MDAs will structure program strategies and oversight, phase content, the timing and scope of decision reviews, and decision levels based on the specifics of the product the program is acquiring, including complexity, risk, security, and urgency to satisfy validated capability requirements.

Figure 8 depicts the major capability acquisition model.

Figure 8: Major Capability Acquisition Path



This pathway should utilize the activities in information analysis, TSN analysis and CPI analysis, which incorporate activities necessary for cybersecurity. TSN analysis should be commensurate with the level of technical maturity of the system, and the availability of the threat and known vulnerabilities.

7.4 Software Acquisition

The software acquisition pathway, established in DoDI 5000.87, is intended for the timely acquisition of custom software.

There are two paths within the software acquisition pathway: applications and embedded software.

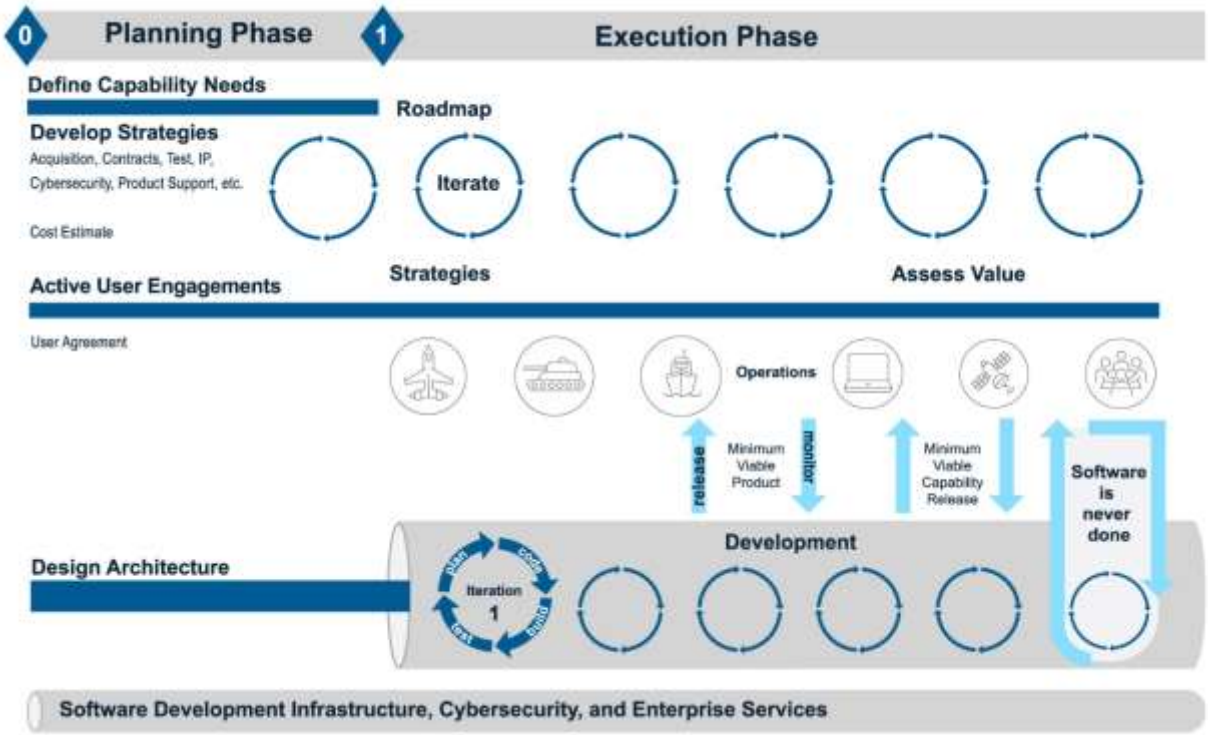
- The application's path provides for rapid development and deployment of software running on commercial hardware, including modified hardware, and cloud computing platforms.

- The embedded software path provides for the rapid development, deployment, and insertion of upgrades and improvements to software embedded in weapon systems and other military-unique hardware systems. Programs could acquire the system in which the software is embedded via other acquisition pathways (e.g., major capability acquisition).

A rapid, iterative approach to software development reduces costs, technological obsolescence, and acquisition risk. To allocate resources to the most relevant capability needs, DoD or DoD Component leadership will make software acquisition and development investment decisions within a framework that addresses trade-offs between capabilities, affordability, risk tolerance, and other considerations.

The two paths in the software acquisition pathway have two phases: planning and execution. Figure 9 outlines key activities and artifacts of the two phases that enable rapid and iterative software development and delivery.

Figure 9: Software Acquisition Pathway



This pathway uses a capability needs statement and encourages the use of existing enterprise services. Enterprise services can implement protections in the infrastructure, the platform, or through the software service providers. These enterprise services are typically considered inherited protections. The inherited protections should consider the results of the information analysis and TSN analysis to determine if there are any protection gaps.

This pathway should utilize the activities in information analysis, TSN analysis and CPI analysis, which incorporate activities necessary for cybersecurity. TSN analysis should be commensurate with the level of technical maturity of the system, and the availability of the threat and known vulnerabilities.

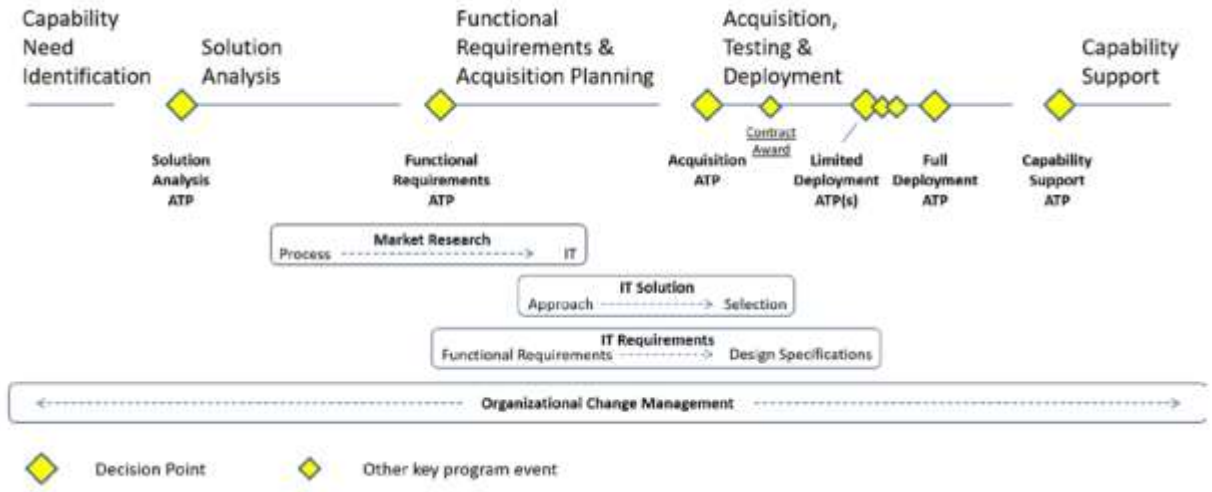
7.5 Defense Business Systems

The Defense Business System (DBS) pathway, established in DoDI 5000.75, is intended for acquisition and business decisions in the life-cycle and may be tailored as necessary to contribute to successful delivery of business capabilities.

The DBS pathway applies to information systems that are operated by, for, or on behalf of DoD, including: financial systems, financial data feeder systems, contracting systems, logistics systems, planning and budgeting systems, installations management systems, human resources management systems, and training and readiness systems. A business system does not include a national security system or an information system used exclusively by and within the defense commissary system or the exchange system, or other DoD instrumentality conducted for the morale, welfare, and recreation of members of the Armed Forces using non-appropriated funds.

Figure 10 provides the framework for acquisition and business decisions in the life-cycle, and DoD Components may tailor it as necessary to contribute to successful delivery of business capabilities.

Figure 10: Defense Business Capability Acquisition Path



This pathway should utilize the activities in information analysis, and TSN analysis which incorporates activities necessary for cybersecurity. The TSN analysis should be commensurate

with the level of technical maturity of the system, and the availability of the threat and known vulnerabilities.

Programs should follow the TSN Analysis activities to identify the critical components to examine potential risks and vulnerabilities of COTS and open source software.

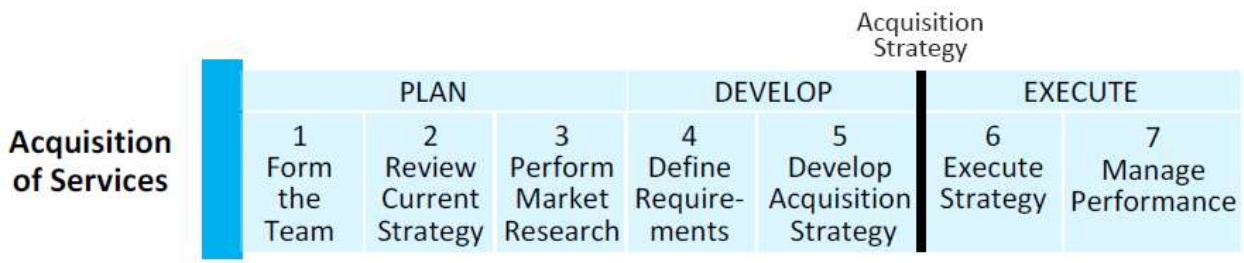
7.6 Defense Acquisition of Services

The Defense Acquisition of Services pathway, established in DoDI 5000.74, is intended for the appropriate, efficient, and effective acquisition of services by their organizations. Acquisition of services is a command responsibility: unit, organization, and installation commanders are responsible for the appropriate, efficient, and effective acquisition of services by their organizations.

DoD Components should consider the evolving nature of industry-provided services capabilities, including innovative processes for services and the use of technology in delivering services outcomes, when acquiring services. These capabilities include, but are not limited to, automation, improved or re-engineered processes (both internal and external to DoD), and the use of tools and techniques to improve the services management.

Figure 11 outlines the steps that Components will use to ensure the use of proven, repeatable processes and procedures contributing to successful services acquisitions.

Figure 11: Seven Steps to the Services Acquisition Process



Glossary

G.1. Acronyms

Acronym	Meaning
AAF	Adaptive Acquisition Framework
ADM	Acquisition Decision Memorandum
ASDB	Acquisition Security Database
ASIC	Application-specific Integrated Circuit
ASR	Alternative Systems Review
AT	Anti-tamper
ATEA	Anti-Tamper Executive Agent
ATTR SSG	Arms Transfer and Technology Release Senior Steering Group
BOM	Bill of Materials
CAC	Common Access Card
CAPEC	Common Attack Pattern Enumeration and Classification
CC	Critical Component
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CF	Critical Functions
CFR	Code of Federal Regulations
CI	Counterintelligence
CISP	Counterintelligence Support Plan
CNSSI	Committee on National Security Systems Instruction
CONOPS	Concept of Operations
COTS	Commercial off-the-shelf
CPI	Critical Program Information
CRWS	Cyber Resilient Weapon Systems
CRWS-BoK	Cyber Resilient Weapon Systems Body of Knowledge
CS	Cyber Security
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DA	Decision Authority
DAG	Defense Acquisition Guidebook
DAMO	Damage Assessment Management Office
DAS	Defense Acquisition System
DAU	Defense Acquisition University
DB	Database
DBS	Defense Business Systems
DCSA	Defense Counterintelligence and Security Agency
DEF	Defense Exportability Features
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency

DIB	Defense Information Base
DMEA	Defense Microelectronics Activity
DMSMS	Diminishing Manufacturing Sources and Material Shortages
DoD	Department of Defense
DoD EA	DoD Executive Agent
DoD ISRMC	DoD Information Security Risk Management Committee
DoDD	DoD Directive
DoDI	DoD Instruction
DT&E	Developmental Test and Evaluation
DTIC	Defense Technical Information Center
EA	Executive Agent
EMD	Engineering and Manufacturing Development
FAR	Federal Acquisition Regulation
FCA	Functional Configuration Audit
FDD	Full Deployment Decision
FDDR	Full Deployment Decision Review
FFRDC	Federally Funded Research and Development Center
FIE	Foreign Intelligence Entities
FOC	Full Operational Capability
FPGAs	Field Programmable Gate Array
FMS	Foreign Military Sales
FOCI	Foreign Ownership, Control or Influence
FRP	Full Rate Production
FRP DR	Full Rate Production Decision Review
GFI	Government Furnished Equipment
GOTS	Government off-the-shelf
IV&V	Independent Verification and Validation
JAPEC	Joint Acquisition Protection and Exploitation Cell
JCIDS	Joint Capability Integration and Development System
JFAC	Joint Federated Assurance Center
LCSP	Life-Cycle Sustainment Plan
LO/CLO	Low Observable / Counter Low Observable
MCA	Major Capability Acquisition
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MDCO	Military Departments' Counterintelligence Organization
MDD	Materiel Development Decision
MDID	Milestone Document Identification Tool
MPIR	Milestone and Phase Information Requirements
MS A	Milestone A
MS B	Milestone B
MS C	Milestone C
MTA	Middle Tier of Acquisition
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual

NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
O&G	Outline and Guidance
O&S	Operations and Sustainment
OCM	Original Component Manufacturer
OPSEC	Operational Security
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
OWASP	Open Web Application Security Project
P&A	Pricing and Availability
P&D	Production and Deployment
PAO	Principal Authorizing Official
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PHI	Protected Health Information
PID	Program Identification Data
PII	Personally Identifiable Information
PM	Program Manager
PPP	Program Protection Plan
PPP O&G	PPP Outline and Guidance
PRR	Production Readiness Review
QML	Qualified Manufacturers List
QSLD	Qualified Supplier List of Distributors
R&D	Research and Development
RDT&E	Research, Development, Test, and Evaluation
RFP	Request for Proposal
RMF	Risk Management Framework
RTVM	Requirements Traceability Verification Matrix
S&T	Science and Technology
SAP	Special Access Program
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SCRE	Secure Cyber Resilient Engineering
SCRM	Supply Chain Risk Management
SDLC	Software Development Life-Cycle
SE	Systems Engineer
SEI	Software Engineering Institute
SEP	Systems Engineering Plan
SETR	Systems Engineering Technical Review
SFR	System Functional Review
SISO	Senior Information Security Officer
SOAR	State of the Art Resource
SOW	Statement of Work

SPRS	Supplier Performance Risk System
SRD	System Requirements Document
SRG	Security Requirements Guide
SRR	System Requirements Review
SSDF	Secure Software Development Framework
SSE	Systems Security Engineer
STIG	Security Technical Implementation Guides
STIP	Scientific and Technical Information Program
STTP	Science Technology Program Protection
SVR	System Verification Review
SwA	Software Assurance
T&E	Test & Evaluation
TAC	Threat Analysis Center
TAPP	Technology Area Protection Plan
TEMP	Test and Evaluation Master Plan
TMRR	Technology Maturation and Risk Reduction
TSFD	Technology Security and Foreign Disclosure
TRR	Test Readiness Review
TSFD	Technology Security and Foreign Disclosure
TSFDO	Technology Security and Foreign Disclosure Office
TSN	Trusted Systems and Network
U.S.	United States
USC	United States Code
UARC	University Affiliated Research Centers
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(R&E)/CTO	Under Secretary of Defense for Research and Engineering/Chief Technology Officer
UON	Urgent Operational Need/Urgent Capability Acquisition
USG	U.S. Government

G.2. Definitions

Unless otherwise noted, a complete glossary of this issuance's terms is maintained on the Defense Acquisition University Website at https://www.dau.edu/ and the Joint Publication Doctrine for the Armed Forces of the United States DoD Dictionary of Military and Associated Terms at https://www.jcs.mil/Doctrine/DOD-Terminology-Program/.