



# Trusted Systems and Networks and Anti-Tamper in the Adaptive Acquisition Policy Framework

*Randy Woods  
Director, Systems Security Engineering and Anti-Tamper  
Office of the Secretary of Defense for Research and Engineering*

National Defense Industrial Association  
Systems & Mission Engineering Conference  
December 6-8, 2021



# Briefing Overview




- DoD Instruction (DoDI) 5000.83 Role in the Adaptive Acquisition Framework
  - Hardware Assurance / Software Assurance
  - Supply Chain Risk Management (SCRM)
  - Anti-Tamper (AT)
- Adaptive Acquisition Framework (AAF)
  - Designates “Functional Areas” such as cyber and program protection to provide high level responsibilities and procedures supporting the DoD Directive (DoDD) 5000.01
- Trusted Systems and Networks (TSN) and Information and Communications Technology (ICT) Responsibilities in DoDI 5200.44
- Anti-Tamper and Exportability Responsibilities and the Establishment of the Anti-Tamper Executive Agent (ATEA) in DoDD 5200.47E
- Relationship between Program Protection and Anti-Tamper



# Program Protection and Anti-Tamper in the Adaptive Acquisition Framework



  
DoD INSTRUCTION 5000.83  
TECHNOLOGY AND PROGRAM PROTECTION TO MAINTAIN TECHNOLOGICAL ADVANTAGE

**Originating Component:** Office of the Under Secretary of Defense for Research and Engineering  
**Effective:** July 20, 2023  
**Change Effective:** May 21, 2021

**Classified:** Canceled for public release. Available on the Director, Defense Website at <https://www.mil.af.mil/5000>.

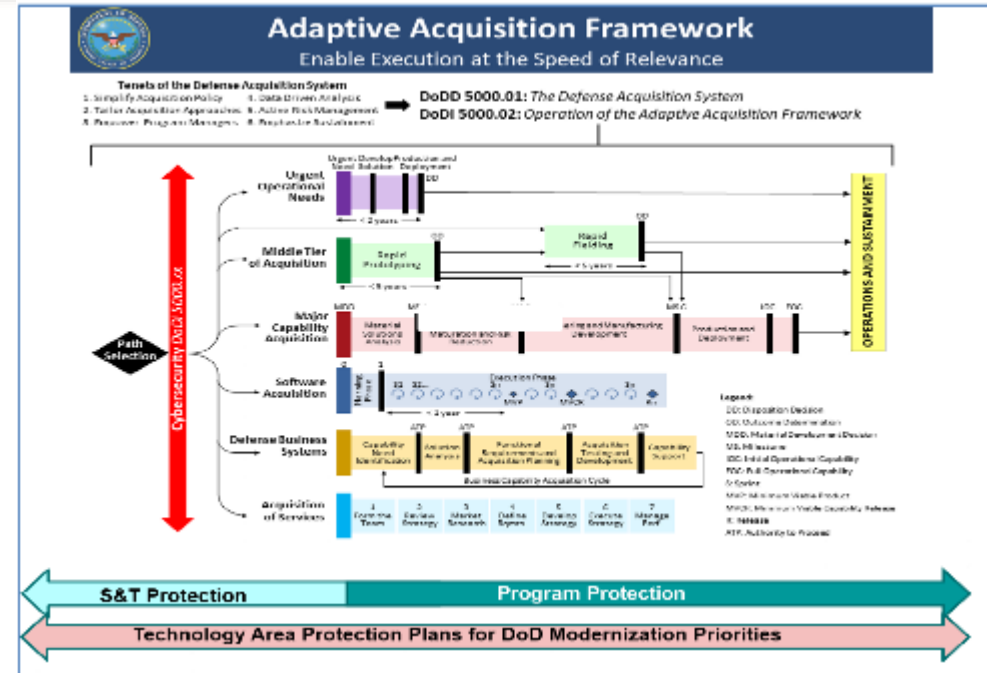
**Supersedes and Cancels:** See Paragraph 1.3.

**Approved by:** Michael D. Griffin, Chief Secretary of Defense for Research and Engineering  
**Change Approved by:** Matthew S. M. Johnson, Under Secretary of Defense for Research and Engineering

**Purpose:** In accordance with the authority in DoD Directive (DDO) 5033.02, the policy in Section 1304 of Title 10, United States Code, and Departmental Memorandum S-01M-14-00, this instruction:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection, hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security;
  - DoD warfighting capabilities;
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPP), S&T protection, program protection plan (PPP), and safeguarding cybersecurity activities.

- DoDI 5000.83 establishes policy, assigns responsibilities, and provides procedures for **science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks** from: foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering.



- DoDI 5000.83 tailors program protection activities for selected Acquisition Pathways and Science and Technology:
  - DoDI 5000.85: Major Defense Programs
  - DoDI 5000.81: Urgent Capabilities
  - DoDI 5000.80: Middle Tier
  - DoDI 5000.87: Software

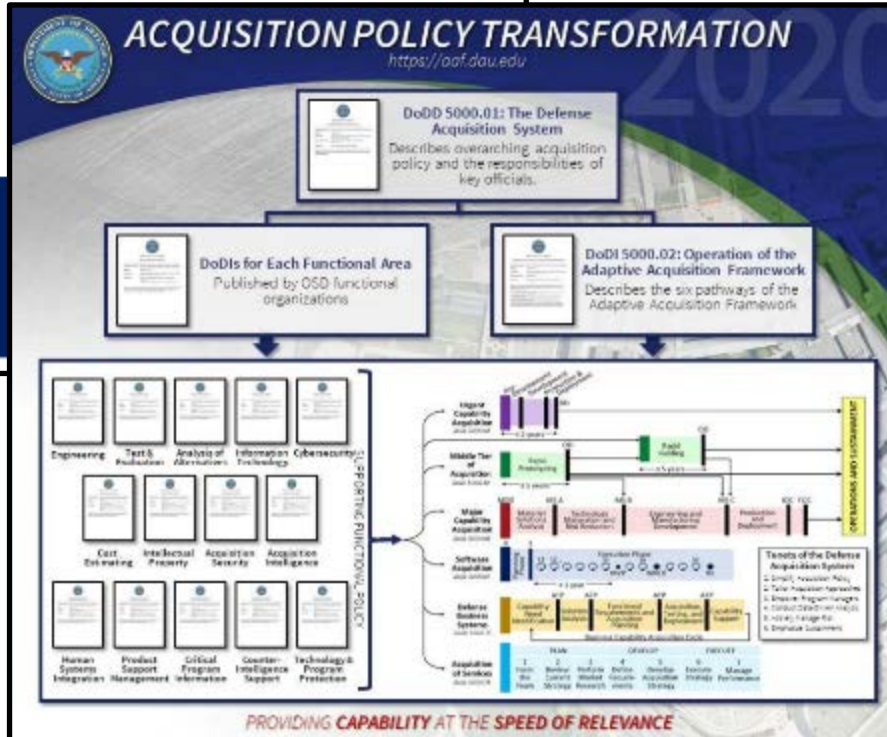




# Adaptive Acquisition Framework



DoD 5000 SERIES  
ACQUISITION POLICY TRANSFORMATION  
**HANDBOOK**



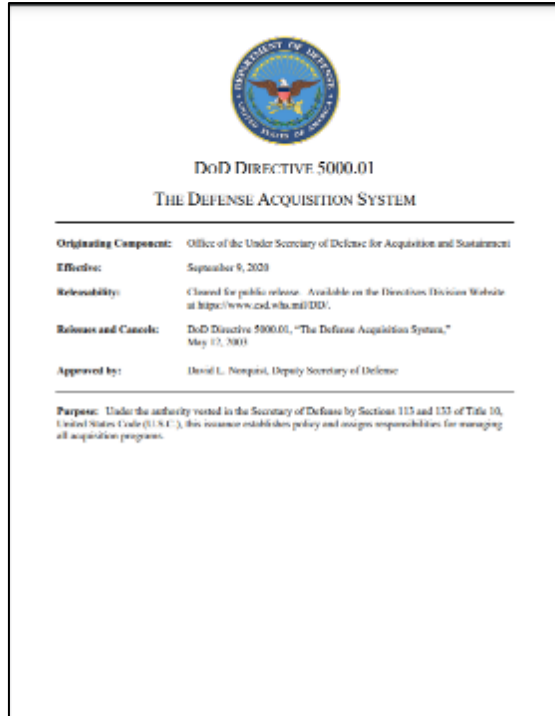
- DoDD 5000.01 “The Defense Acquisition System” instantiates 25 overarching policy statements supporting the National Defense Strategy (NDS)
- DoDI 5000.02 “Operation of the Adaptive Acquisition Framework” assigns responsibilities for employing the AAF to:
  - OUSD and DoD component heads
  - Specific program management responsibilities and authorities:
    - Milestone Decision Authority (MDA)
    - Program Executive Officer (PEO)
    - Program Manager (PM)
  - Procedures for utilizing the AAF Pathways

“MULTIPLE PATHWAYS FOR TAILORED SOLUTIONS”

[HTTPS://WWW.DAU.EDU/AAF/](https://www.dau.edu/AAF/)



# DoD Directive 5000.01 “The Defense Acquisition System”



## d. Develop and Deliver Secure Capabilities.

Security, cybersecurity, and protection of critical technologies at all phases of acquisition are the foundation for uncompromised delivery and sustainment of warfighting capability. Acquisition managers, in coordination with security and counterintelligence (CI) professionals, will implement initiatives and processes for the identification, integration and continual evaluation of security and CI requirements throughout the life cycle of a system, service, or critical technology.

## q. Deploy Interoperable Systems.

Joint concepts, standardization, and integrated architectures will be used to the maximum extent possible to characterize the exchange of data, information, materiel, and services to and from systems, units, and platforms to assure all systems effectively and securely interoperate with other U.S. forces and coalition partner systems.

## t. Plan for Coalition Partners.

To enable allies and partners to enhance U.S. military capability, collaboration opportunities, potential partnerships, and international acquisition and exportability features and limitations will be considered in the early design and development phase of acquisition programs.

**These three policy statements anchor program protection and anti-tamper into the Defense Acquisition System in support of the National Defense Strategy**



# DoD Instruction 5000.83 Responsibilities: System Security Engineering and Anti-Tamper

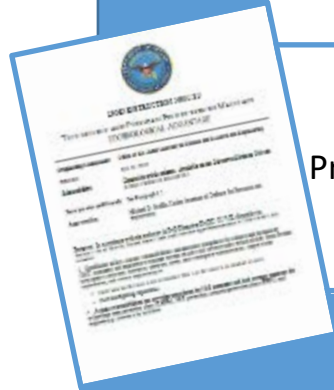


USD(R&E) – Establish and maintain S&T and program protection policy, guidance, education and training to manage technical risk

1. Anti-Tamper/Exportability Features
2. Hardware and Software Assurance
3. Supply Chain Risk Management
4. System Assurance
5. Engineering Secure Cyber Resilient Systems

5200.47E

5200.44



**DoDI 5000.83**  
Technology and Program Protection (T&PP) to Maintain Technology Advantage  
OPR: USD(R&E)/STPE/RS

Direction to S&T Managers and Engineers

Chairman Joint Chief of Staff (CJCS) – SCRM, Export Control and AT Requirements to achieve T&PP

1. Included in Capability Requirement in Joint Capabilities Integration Development System (JCIDS)
2. Addressed during Capability Development

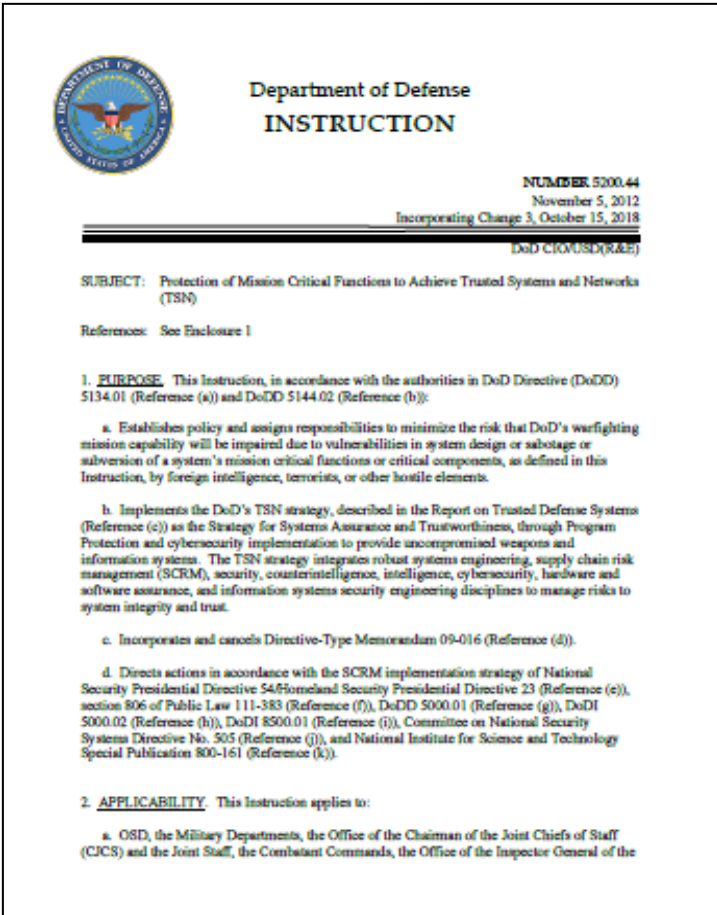
USD(A&S) - Include Technology Area Protection Plans and Program Protection Planning in:

1. The Defense Acquisition System (DAS) to inform programs and sustainment risk decisions
2. When developing and implanting international acquisition and exportability
3. In DAU education and training





# DoD Instruction 5200.44 (Oct. 2018 Version) Protection of Mission Critical Functions to Achieve Trusted Systems and Networks



- **Implements the DoD’s TSN Strategy**
- **Manage risk of mission critical function and component compromise throughout lifecycle of key systems by utilizing:**
  - Criticality Analysis (based on mission’s criticality) as the systems engineering process for risk identification
  - Countermeasures: SCRM, software assurance, hardware assurance, and secure design procedures
  - Intelligence and counterintelligence analysis to inform program management
  - Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)
- **Document planning and accomplishments in program protection and cybersecurity activities**

**Resilient Systems has close partnership with Office of DoD Chief Information Officer (CIO) and is currently working to update DoDI 5200.44**



# Trusted Systems and Networks Approach to Technology and Program Protection

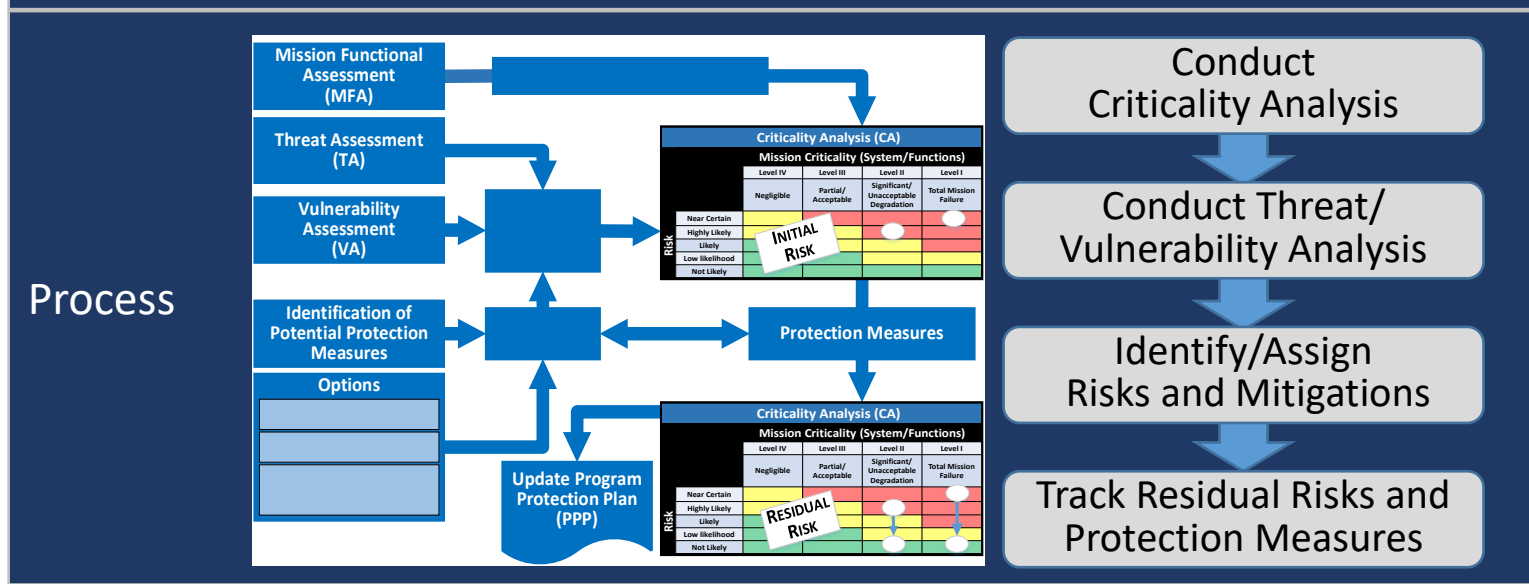


## DoDI 5200.44 – Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

**Applicable Systems**

- National Security Systems (NSS) as defined by Section 3552 U.S.C 44
- DoDI 8510.01: Risk Management Framework (RMF) high impact for Confidentiality/Integrity/Availability (C/I/A)
- Other DoD systems that the DoD Component Acquisition Executive (CAE) or Chief Information Officer (CIO) determines are critical

Manage Risk



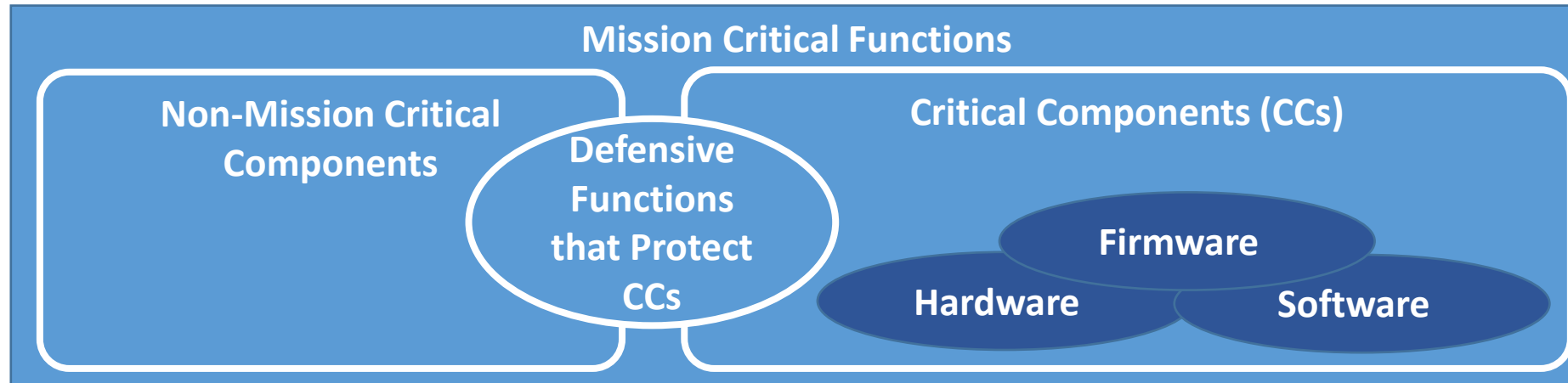
Technology and program protection activities occur throughout the lifecycle of the system





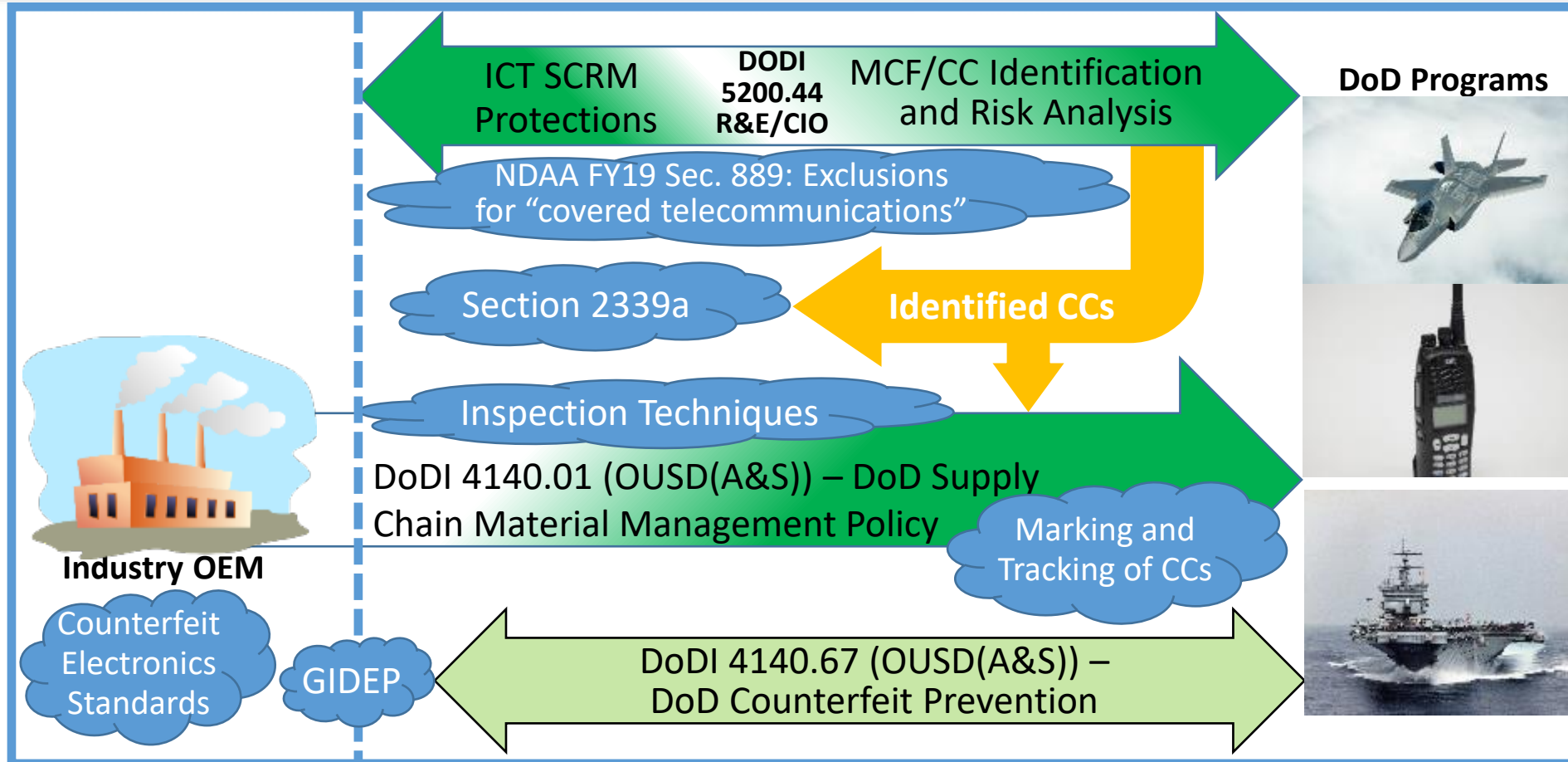
# DoD Instruction 5200.44

## Mission Critical Functions and Components



- **Mission Critical Functions (MCFs):**
  - Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed (Source: DoDI 5200.44)
- **Critical Components (CCs):**
  - **A component which is or contains information and communications technology (ICT) including hardware, software, and firmware**, whether custom, commercial, or otherwise developed and **delivers or protects** mission critical functionality of a system or which, because of the system's design, **may introduce vulnerability** to the mission critical functions of an applicable system (Source: DoDI 5200.44, 4140.01, and 4140.67)

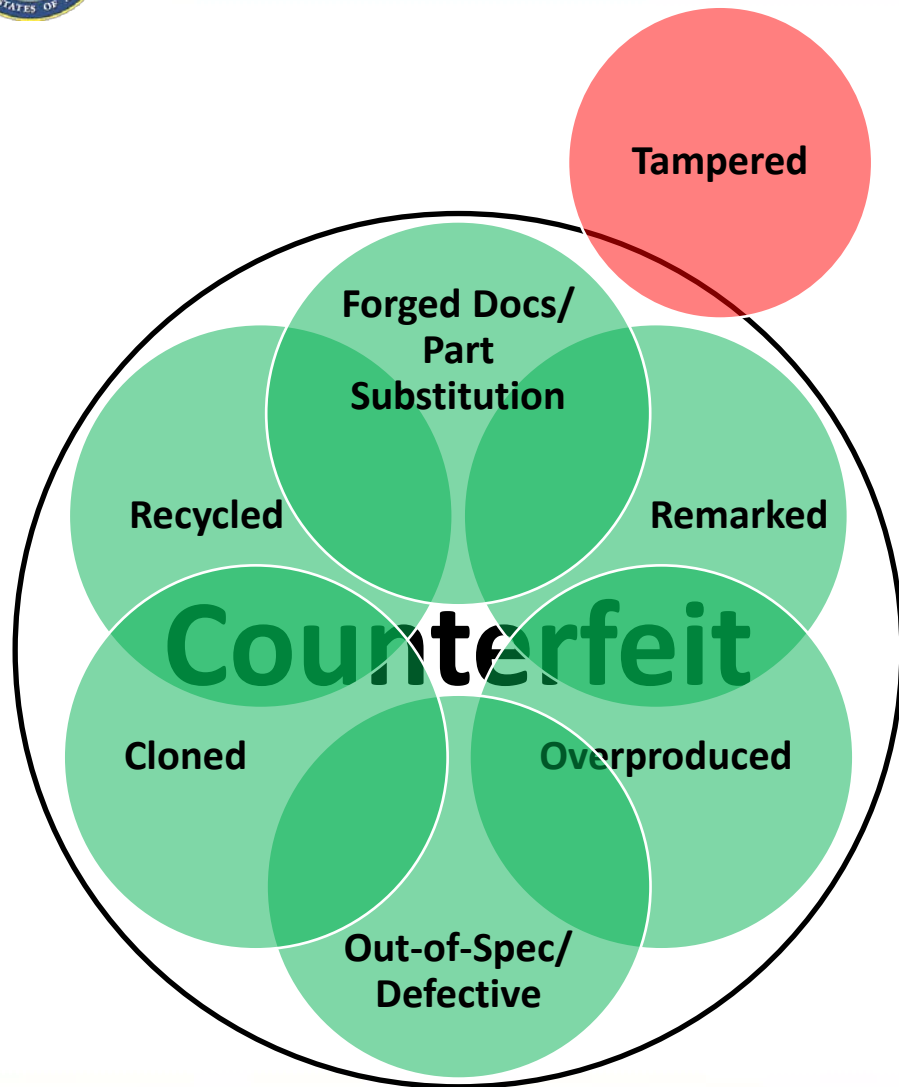
# Criticality Analysis and Supply Chain Risk Management (SCRM) in Policy



**SCRM:** A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (Source: DoDI 5200.44)



# DoD Instruction 5200.44 Counterfeit and Tampered Devices



- **Counterfeit electronic part:**

- An unlawful or unauthorized reproduction (**cloned/overproduced**), substitution (**part substitution**), or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer (**forged docs**), or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new (**recycled/remarked**), or the false identification of grade, serial number, lot number, date code, or performance characteristics (**out-of-spec/defective**).

- DFARS 252.246-7007 or SAE AS6171 definition are not designated for the detection of tampered devices.
- DoDI 5200.44 SCRM Practices are tailored to **identify and exclude** potential suppliers who present an unacceptably high risk to procurement for DoD.

# DoD Instruction 5000.83 Procedures: Activities to Mitigate Adversary Threats to Technology and Programs



## Foreign Military Sales



Section 3.3.c.(6) - Identification and Protection of the warfighters' technical advantage

## Combat Losses

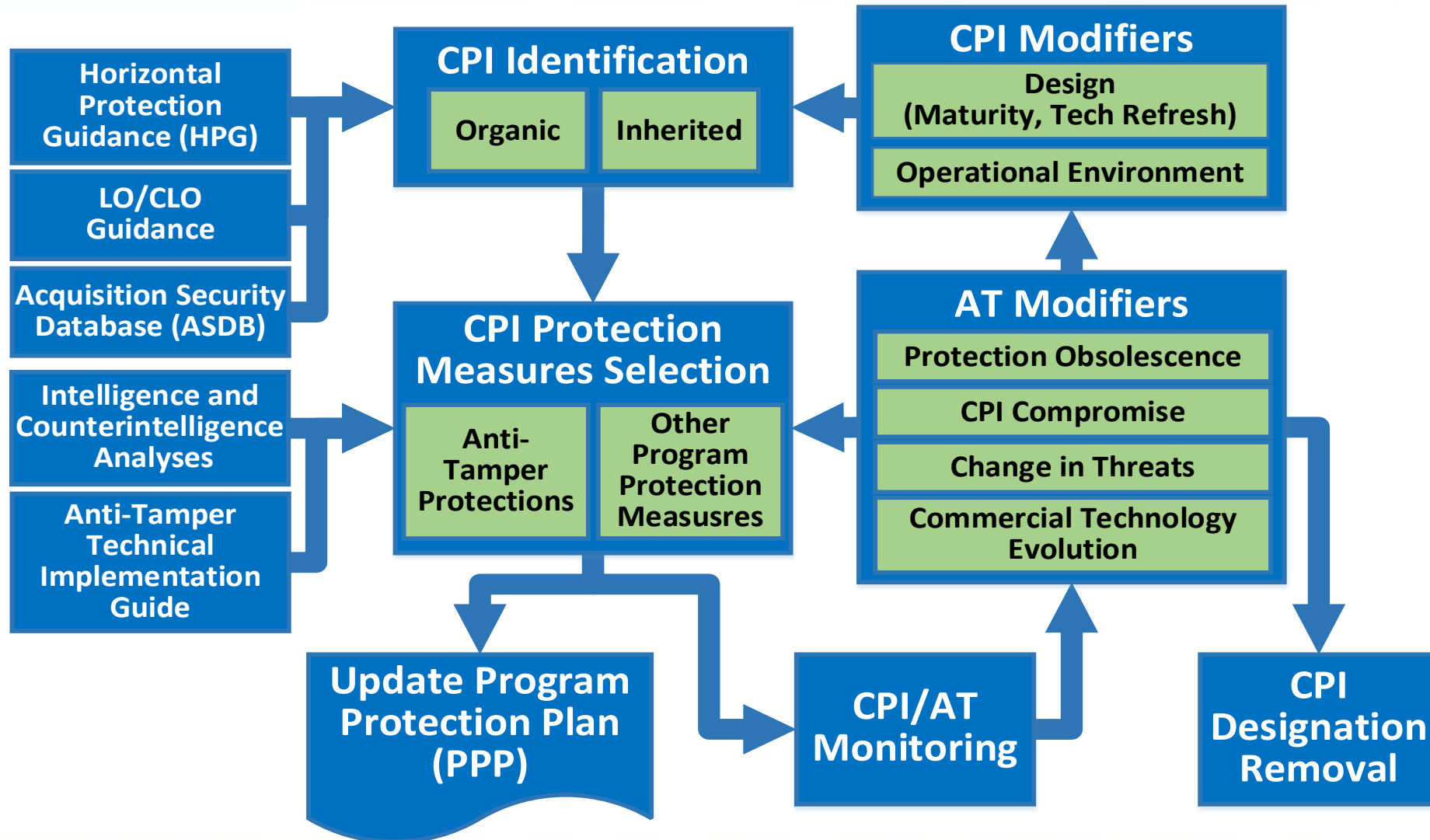


Section 3.3.c.(6).a – Apply Horizontal Protection Guidance (HPG) to determine requirements for designing and implementing exportability features when outside U.S. control

Section 3.3.c.(6).b – Coordinate with applicable DoD component's Office of Primary Responsibility (OPR) for DoD AT to mitigate reverse engineering opportunities.



# Critical Program Information (CPI) Identification Methodology



# DoD Instruction 5000.85 "Major Capability Acquisition" Relationship to Foreign Military Sales and Anti-Tamper



## DoD INSTRUCTION 5000.85 MAJOR CAPABILITY ACQUISITION

**Originating Component:** Office of the Under Secretary of Defense for Acquisition and Sustainment  
**Effective:** Aug 6, 2010  
**Relatability:** Cleared for public release. Available on the Directives Division Website at <http://www.acd.osd.mil/DCI/>.  
**Incorporates and Cancels:** Sections 1, 4, and 5, and Enclosures 1, 2, 5, and 8 of DoDI 5000.02L, "Operation of the Defense Acquisition System," January 7, 2015, as amended.  
**Approved by:** Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment

**Purpose:** In accordance with DoD Directive (DoDD) 5135.02, this issuance establishes policy and general procedures that guide the acquisition of major capability acquisition programs, including major defense acquisition programs (MDAPs), other programs categorized as acquisition category (ACAT) II major systems, usually categorized as ACAT II, automated information systems (AIS) (not managed by other acquisition pathways) and other capabilities developed via the major capability acquisition pathway. Wholly and majority National Intelligence Program-funded acquisition programs will be executed in accordance with Intelligence Community policy.

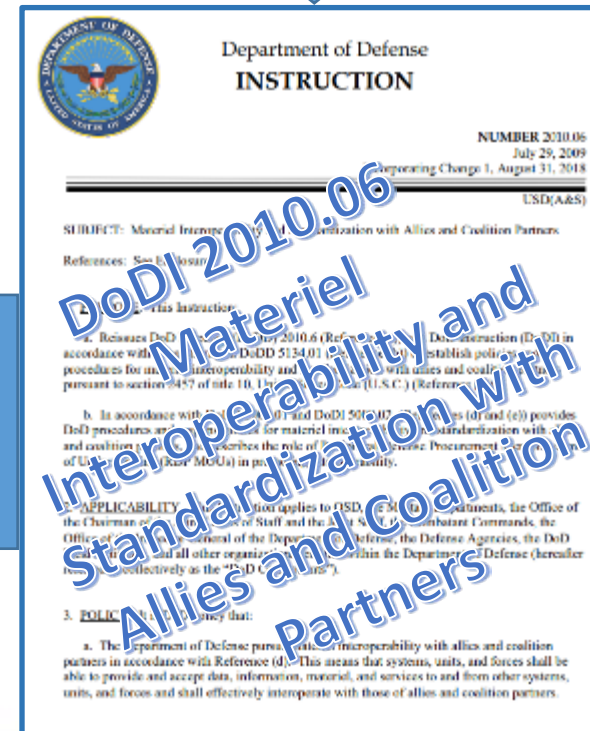
(3) Pursue cooperative opportunities and international involvement throughout the acquisition lifecycle to enhance international cooperation and improve interoperability in accordance with DoDI 2010.06.

### Responsibilities:

3. DIRECTOR, DEFENSE SECURITY COOPERATION AGENCY (DSCA)
  - a. Serve as the focal point for all requests and as the approval authority for foreign military sales (FMS).
5. SECRETARIES OF THE MILITARY DEPARTMENTS AND DIRECTORS OF THE DEFENSE AGENCIES
  - b. Ensure that weapon system design takes into account potential future transfers to allied nations, **incorporates needed anti-tamper features**, and accommodates modifications that make export possible and affordable.

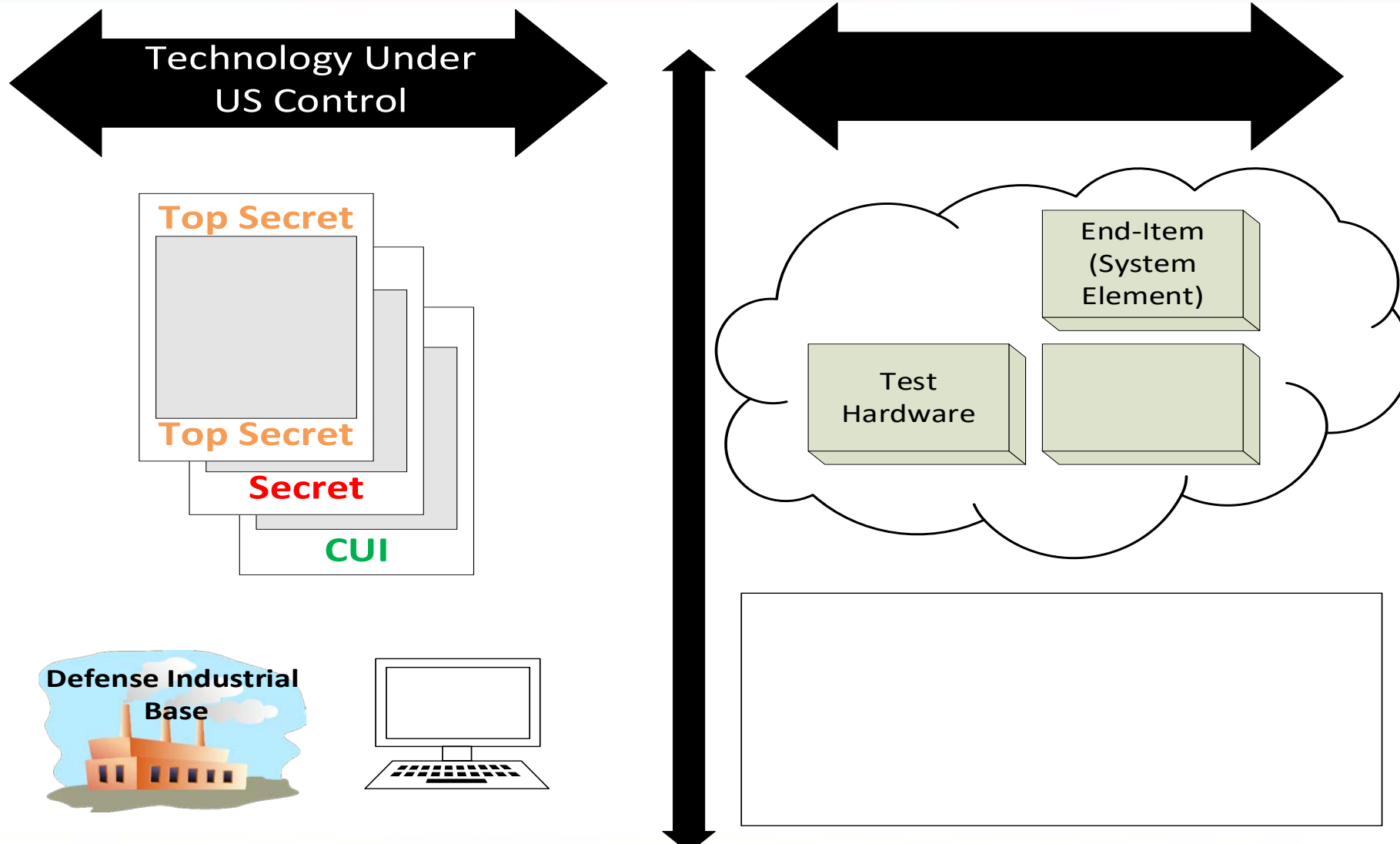
### Procedures:

- c. During the production and deployment phase of systems acquisition through
  - (2) FMS of military systems or equipment and support involving the use of FMS procedures and commercial licenses to transfer to a foreign nation, under DoD Manual 5105.38-M, the ability to produce U.S. defense articles developed and fielded by the Department of Defense. **Anti-tamper measures during the acquisition process need to be considered** to provide allies with U.S. origin defense articles developed and fielded by the Department of Defense.





# Concepts for Technology Advantage Elements (TAE)

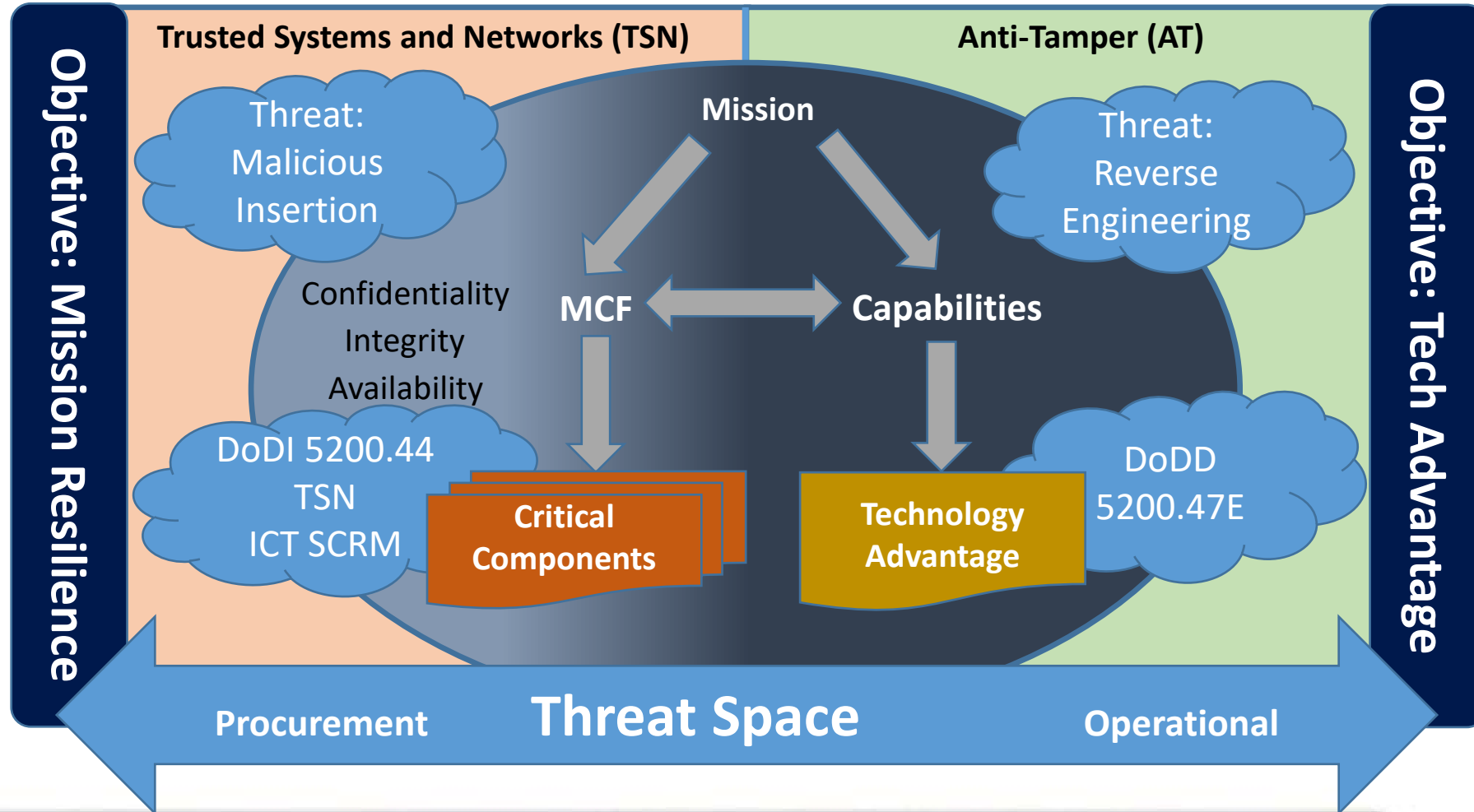




# TSN and AT Summary



**TSN and AT support the AAF across the program lifecycle to secure and maintain the warfighters' technology advantage**







# Questions



