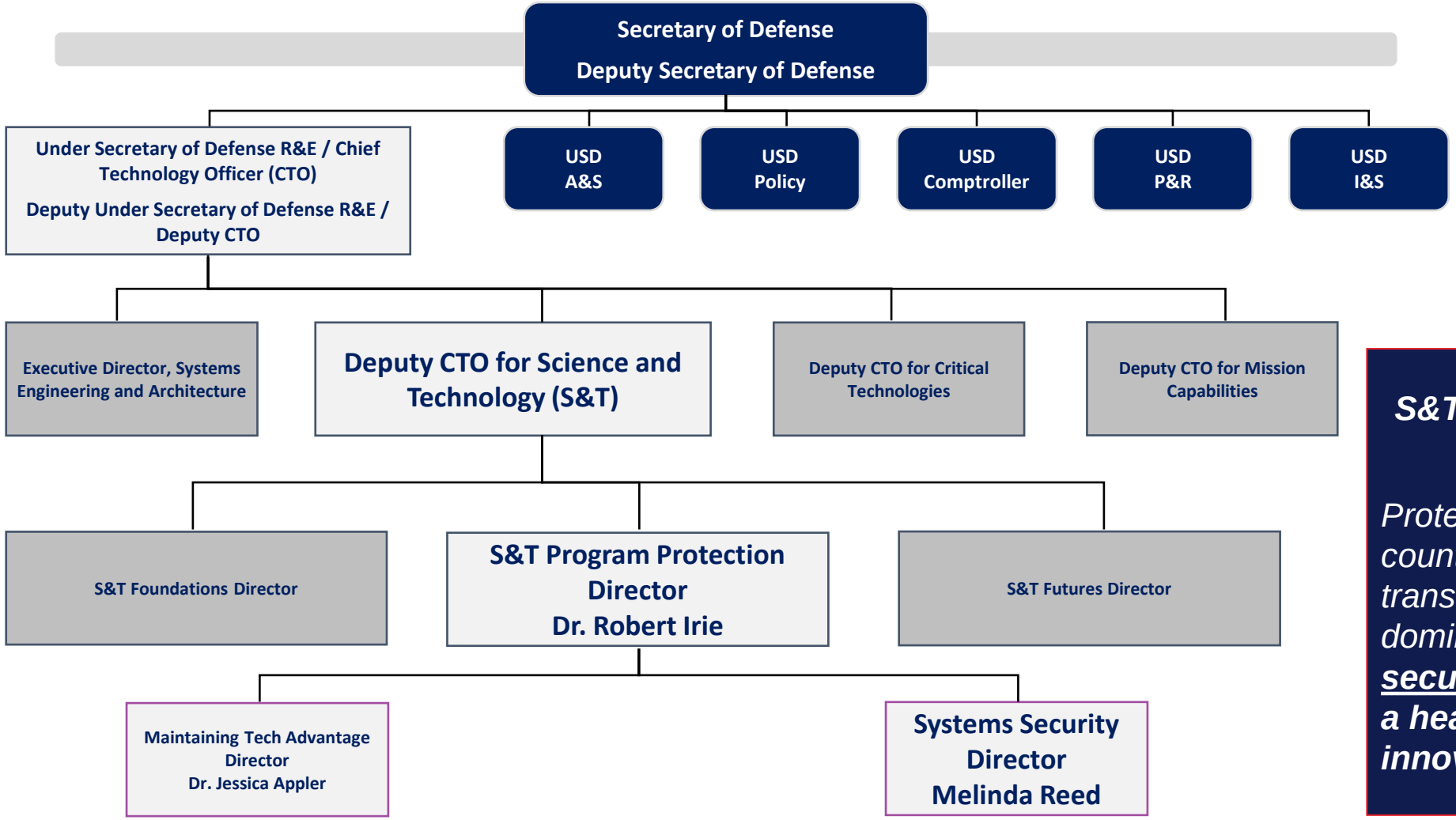
USD(R&E)

Critical Program Information Identification

Mr. Randy Woods
Director, Systems Security Engineering and Anti-Tamper
Office of the Under Secretary of Defense for Research and Engineering
National Defense Industrial Association Systems and Mission Engineering Conference
November 1-3, 2022

OUSD(R&E) Organization



S&T Program Protection (STPP) MISSION:

Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through ***assured, secure and resilient systems*** *and a healthy, viable national security innovation base.*

Three Pillars of Robust Program Protection: Critical Program Information Protection with an Overall Approach to Program Protection

Systems Security Engineering Design and Tradeoffs

Information / Data	Technology	Mission Components
What to Protect: Information and data on the system and about the research and or acquisition program.	**What to Protect:** A U.S. capability element that contributes to the warfighter's technical advantage.	**What to Protect:** Mission critical functions and components.
Protection Activities: • Classification • Information security • Cybersecurity protections and technology solutions • Joint Acquisition Protection and Exploitation Cell (JAPEC) • Damage Assessment Management Office (DAMO)	**Protection Activities:** • Export control • Anti-tamper (AT) • Defense Exportability Features • DoD Horizontal Protection Guide • Acquisition Security Database (ASDB)	**Protection Activities:** • Software assurance (SwA) • Hardware assurance (HwA) • Trusted/assured microelectronics • Supply Chain Risk Management (SCRM) • Anti-counterfeit • Joint Federated Assurance Center (JFAC)
Goal: Safeguard research and / or program information and technical data from adversary collection and disruption.	**Goal:** Prevent compromise or loss of critical technology.	**Goal:** Protect mission-critical components (hardware, software, firmware) from malicious exploitation.

Protecting Warfighting Capability throughout the Lifecycle

Identification of Critical Program Information (CPI) as Part of Technology and Program Protection

- **Technology and Program Protection (T&PP) responsibilities are assigned in the DoD Instruction (DoDI) 5000.83, Technology and Program Protection to Maintain Technological Advantage" for program managers and lead systems engineers:**
  - Hardware and software assurance
  - Cyber and cyberspace
  - Supply chain exploitation
  - Reverse engineering
- **Additional T&PP policy and responsibilities for anti-tamper are further refined in specific policies such as:**
  - DoD Directive (DoDD) 5200.47E: "Anti-Tamper"
  - DoDI 5200.39: "CPI Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)"
  - DoDI 5230.28: "Policy for Low Observable (LO) and Counter Low Observable (CLO) Programs"
- **Critical Program Information (CPI) elements are identified utilizing sources such as:**
  - Acquisition Security Database (ASDB)
  - CPI Horizontal Protection Guidance
  - Expert questions
  - Program-specific and anti-tamper Security Classification Guides (SCG)

Updated guidance is available in the newly published T&PP Guidebook

Guidebook accessible at: https://rt.cto.mil/wp-content/uploads/TPP_Guidebook_Jul2022_cleared.pdf

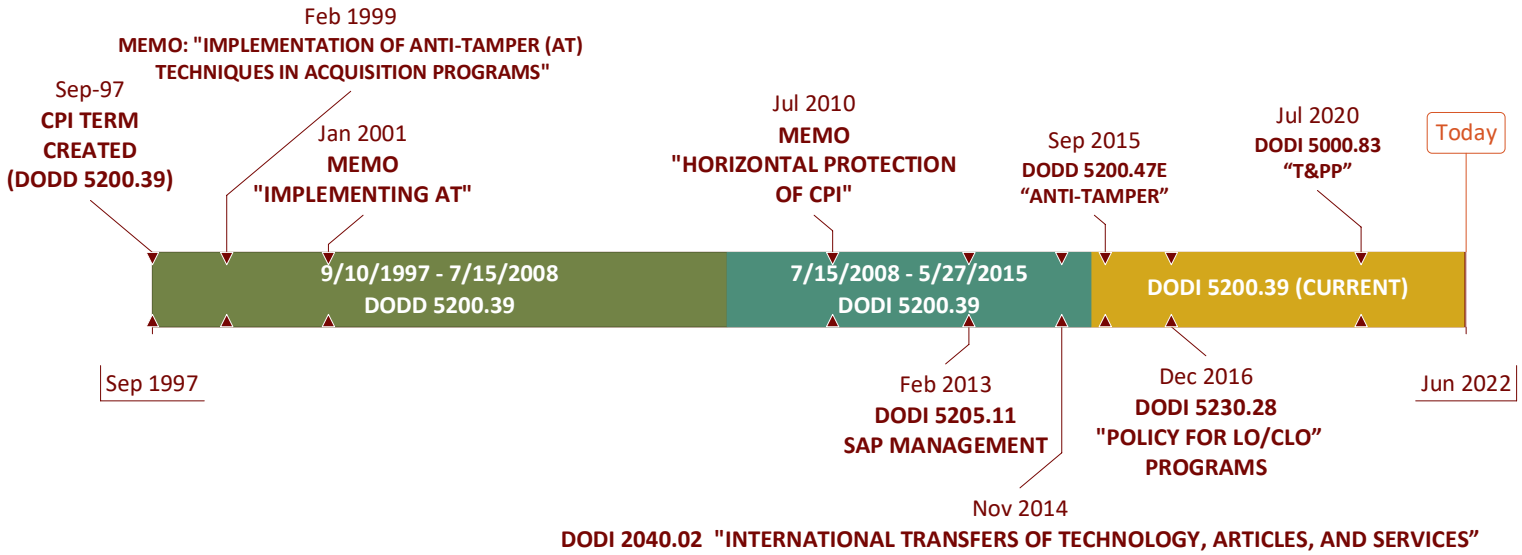
Industry Perspective on DoD Challenges to CPI Identification

- **The National Defense Industrial Association (NDIA) provided a briefing regarding CPI Identification Challenges to Offices of the Under Secretary of Defense (OUSD):**
  - OUSD for Acquisition and Sustainment
  - OUSD for Intelligence and Security
  - OUSD for Research and Engineering
- **DoD's senior leadership has also expressed an interest in streamlining the CPI Identification and protection process for programs**

- **Challenges (as provided by NDIA):**
  1. DoD has multiple CPI definitions
     a. How to constrain the expanding definition of CPI (as it relates to AT)
  2. Differing chains of command use different CPI processes
     a. Inconsistent policy, understanding, and education undermine horizontal protection
     b. CPI identification is often not accurate, consistent, or repeatable
  3. Lack of CPI-focused intelligence support

Every dollar spent on protecting old technology robs the warfighter of new and necessary capability – unnecessary anti-tamper hurts the warfighter

Challenge 1: DoD Has Multiple CPI Definitions – Deviation in the CPI Definition

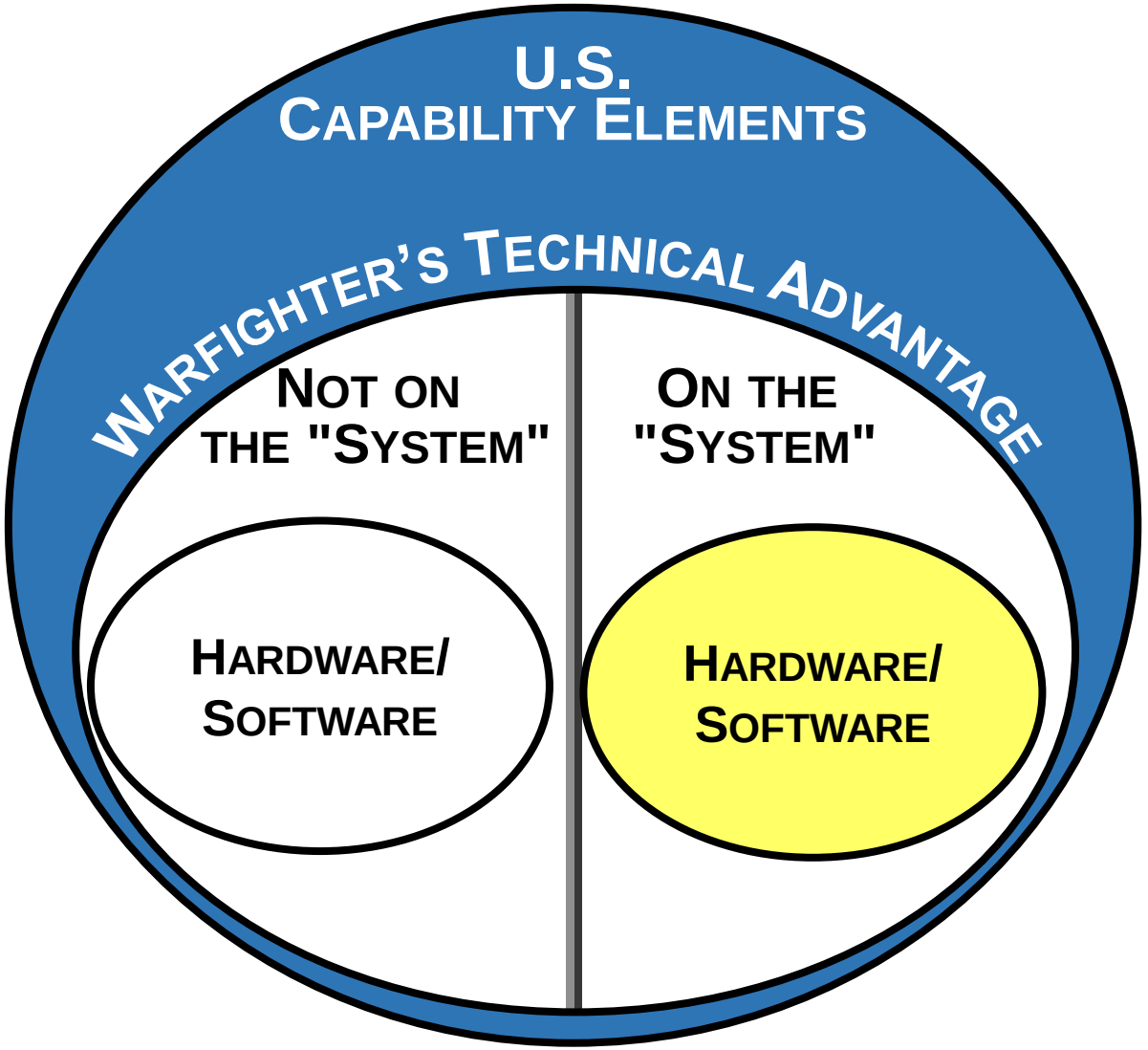


- **1997: CPI term was created as part of the DoDD 5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection"**
- **2008 – 2015: CPI definition included "elements or components of a Research, Design, or Acquisition (RDA) Program"**
  - DoDI 2040.02 (2014) "International Transfers of Technology, Articles, and Services"
  - DoDI 5205.11 (2013) "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)"
- **2015 – Current: CPI definition aligned to "warfighter's technical advantage" that may include but is not limited to specific software and hardware "residing on the system"**
  - DoDD 5200.47E (2015) "Anti-Tamper" (utilizes 2015 DoDI 5200.39 definition)
  - DoDI 5230.28 (2016) "Policy for LO/CLO Programs" (utilizes 2015 DoDI 5200.39 definition)

DoD CPI Definitions

- **DoDI 5200.39, *"CPI Identification and Protection within RDT&E" (issued 2015)* and DoDI 5230.28 *"Policy for LO/CLO Programs" (published 2016; defines CPI and ref. to 5200.39)***
  - U.S. capability elements that contribute to the **warfighter's 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,** its training equipment, or maintenance support equipment.
- **DoDI 5205.11, *"Management, Administration, and Oversight of DoD SAPs" (issued 2013; almost identical to the first part of DoDI 5200.39 2008 definition)***
  - **Elements or components of a SAP** that, if compromised, could cause significant degradation in mission effectiveness, shorten the expected combat-effective life of the system, reduce technological advantage, significantly alter program direction, or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.
- **DoDI 2040.02, "International Transfers of Technology, Articles, and Services" *(issued 2014; identical to the first part of DoDI 5200.39 2008 definition)***
  - **Elements or components of a RDA program** that, if compromised, could cause significant degradation in mission effectiveness, shorten the expected combat-effective life of the system, reduce technological advantage, significantly alter program direction, or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. This includes information about applications, capabilities, processes, and end-items, elements or components critical to a military system or network mission effectiveness, and technology that would reduce the U.S. technological advantage if it came under foreign control.

DoDI 5200.39 (2015) Definition of CPI

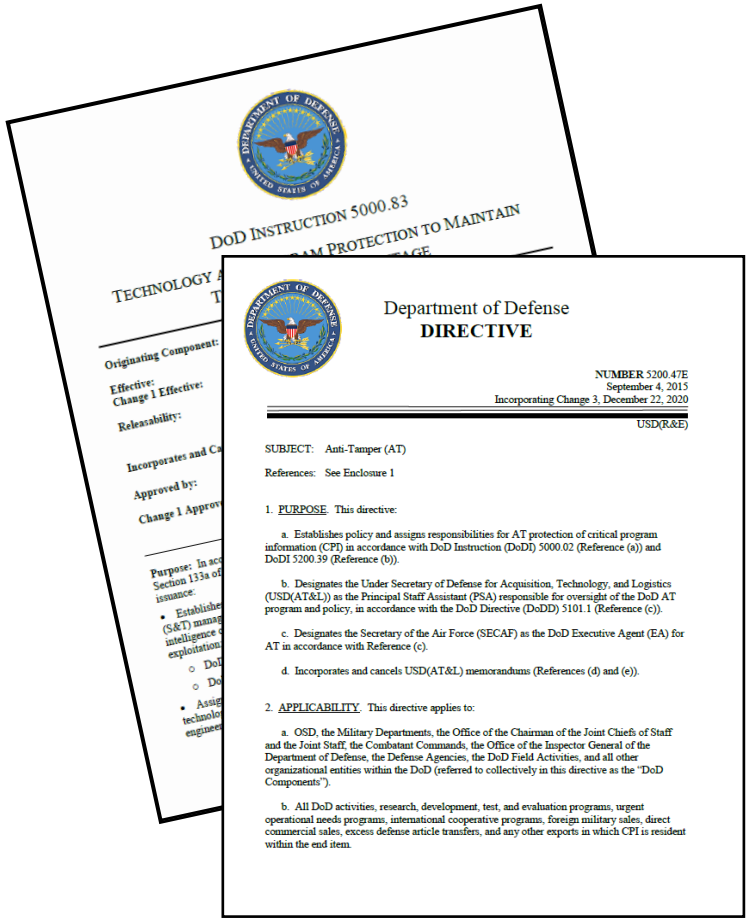


- **CPI definition in DoDI 5200.39 uses and defines "U.S. capability elements":**

  CPI - U.S. capability elements that contribute to the warfighter's 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, its training equipment, or maintenance support equipment

- **Objective (highlighted): Create a specific term for the warfighter's technical advantage when the capability is "on the system" and subject to reverse engineering attacks**

DoDD 5200.47E: Anti-Tamper



Department of Defense
DIRECTIVE

NUMBER 5200.47E
September 4, 2015
Incorporating Change 3, December 22, 2020
USD(R&E)

SUBJECT: Anti-Tamper (AT)

References: See Enclosure 1

1. PURPOSE. This directive:

a. Establishes policy and assigns responsibilities for AT protection of critical program information (CPI) in accordance with DoD Instruction (DoDI) 5000.02 (Reference (a)) and DoDI 5200.39 (Reference (b)).

b. Designates the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) as the Principal Staff Assistant (PSA) responsible for oversight of the DoD AT program and policy, in accordance with the DoD Directive (DoDD) 5101.1 (Reference (c)).

c. Designates the Secretary of the Air Force (SECAF) as the DoD Executive Agent (EA) for AT in accordance with Reference (c).

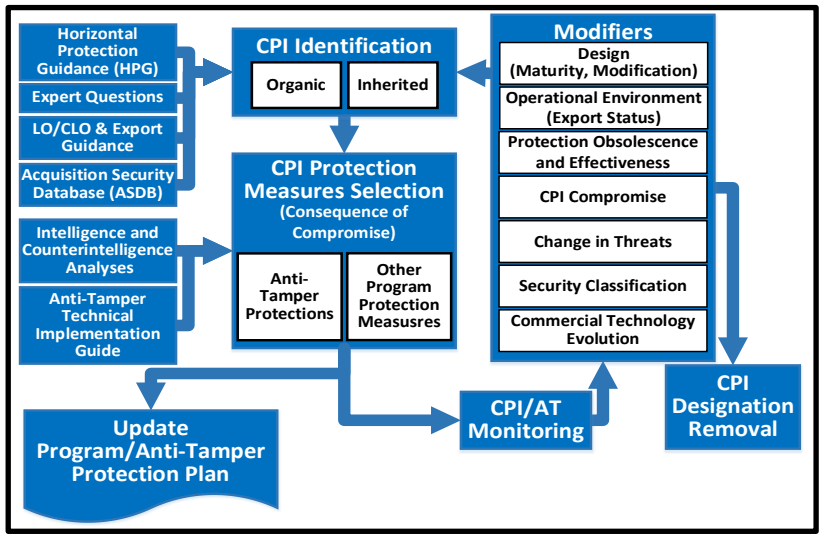
d. Incorporates and cancels USD(AT&L) memorandums (References (d) and (e)).

2. APPLICABILITY. This directive applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this directive as the "DoD Components").

b. All DoD activities, research, development, test, and evaluation programs, urgent operational needs programs, international cooperative programs, foreign military sales, direct commercial sales, excess defense article transfers, and any other exports in which CPI is resident within the end item.

- **Establishes AT Program:**
  - Designates Secretary of the Air Force as the DoD Executive Agent for AT
  - Requires DoD Component heads to establish Offices of Primary Responsibility for AT
- **Requires DoD Component heads in alignment with guidance from the DoD Executive Agent for AT to:**
  - Conduct AT planning
  - Implementation
  - Evaluations
- **Uses DoDI 5200.39, CPI Identification and Protection within Research, Development, Test and Evaluation (RDT&E), to identify CPI**



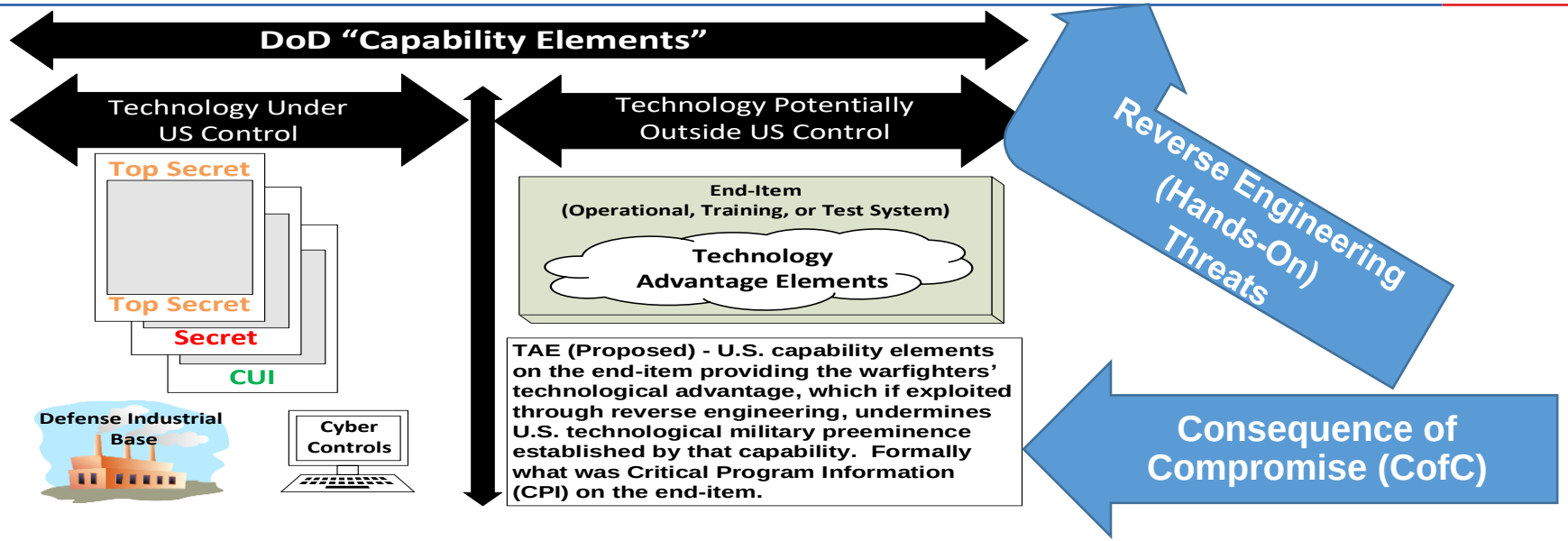
Provides policy for AT activities for the end item, to include identification of the end item; requires identification of Critical Program Information

Current Alignment of CPI with Anti-Tamper

DoD Instruction 5200.39	CPI	DoD Directive 5200.47E
"CPI Identification and Protection within RDT&E"		*"Anti-Tamper"*
Establishes policy and assigns responsibilities for the **identification** and **protection** of **CPI**	(DoDD 5200.47E utilizes CPI definition from current 5200.39)	Establishes policy and assigns responsibilities for **Anti-Tamper (AT) protection** of **CPI**

- **2015 updates of DoDI 5200.39 and DoDD 5200.47E definitions and responsibilities are complementary and were synchronized:**
  - DoDI 5200.39 - CPI: Hardware and software algorithms that **may be** residing on the system
  - DoDD 5200.47E - AT: Systems engineering activities to prevent or delay exploitation, alteration, or countermeasure development of (or to) CPI in U.S. defense systems due to reverse engineering
- **Other communities utilize CPI definitions other than the DoDI 5200.39 CPI definition**
  - DoDI 2040.02 (2014) "International Transfers of Technology, Articles, and Services"
  - DoDI 5205.11 (2013) "Management, Administration, and Oversight of DoD SAPs"

Potential Solution 1: Create Different Definition for the Anti-Tamper Community

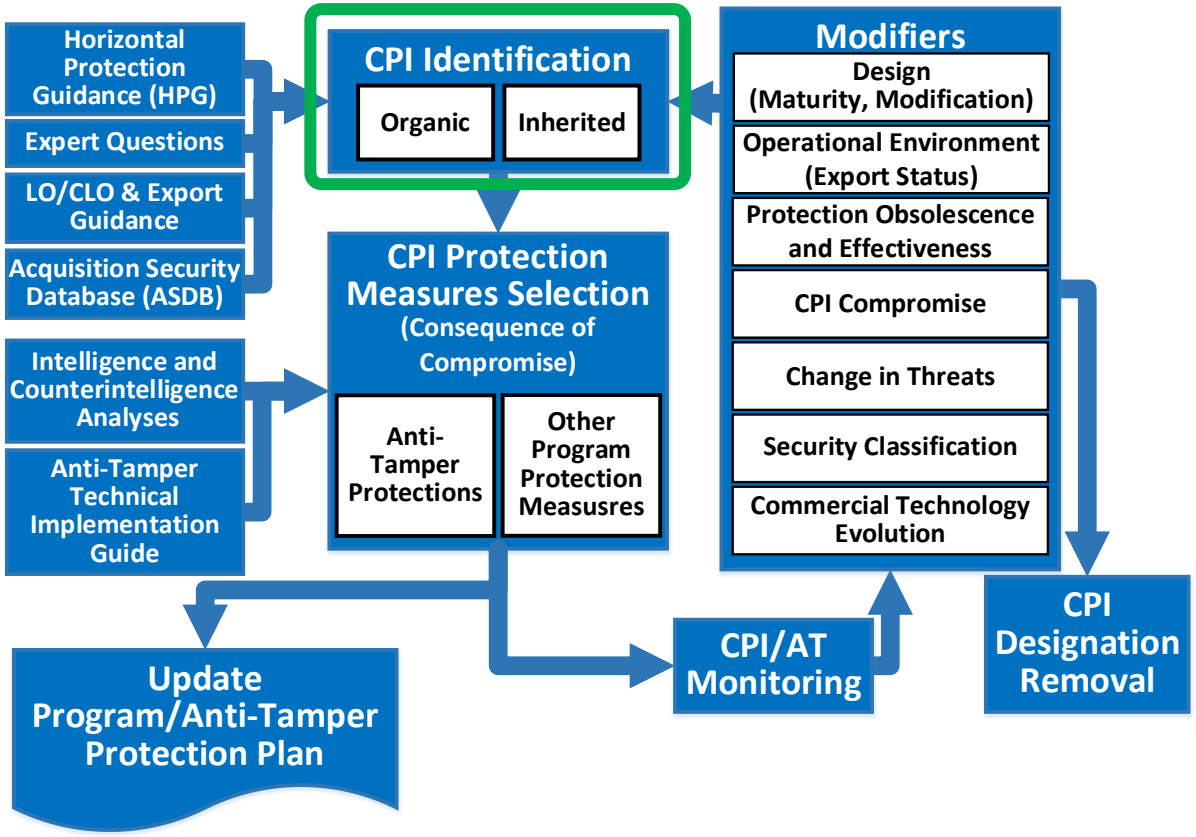


- **DoD's technical advantage needs protection across the development and operational lifecycle. However, systems exposed to reverse engineering attacks exhibit unique vulnerabilities that need to be protected utilizing AT techniques**
- **DoDD 5200.47E is being updated to clarify AT responsibilities for reverse engineering (hands-on) threats encountered when the end-item (system, maintenance, and test equipment) may be outside of U.S. control**
- **Technology Advantage Elements (TAE): A proposed term to identify specific warfighter advantages on the end-item eligible for AT protections from the unique vulnerabilities presented from reverse engineering**

Challenge 2: Differing Chains of Command Use Different CPI Processes

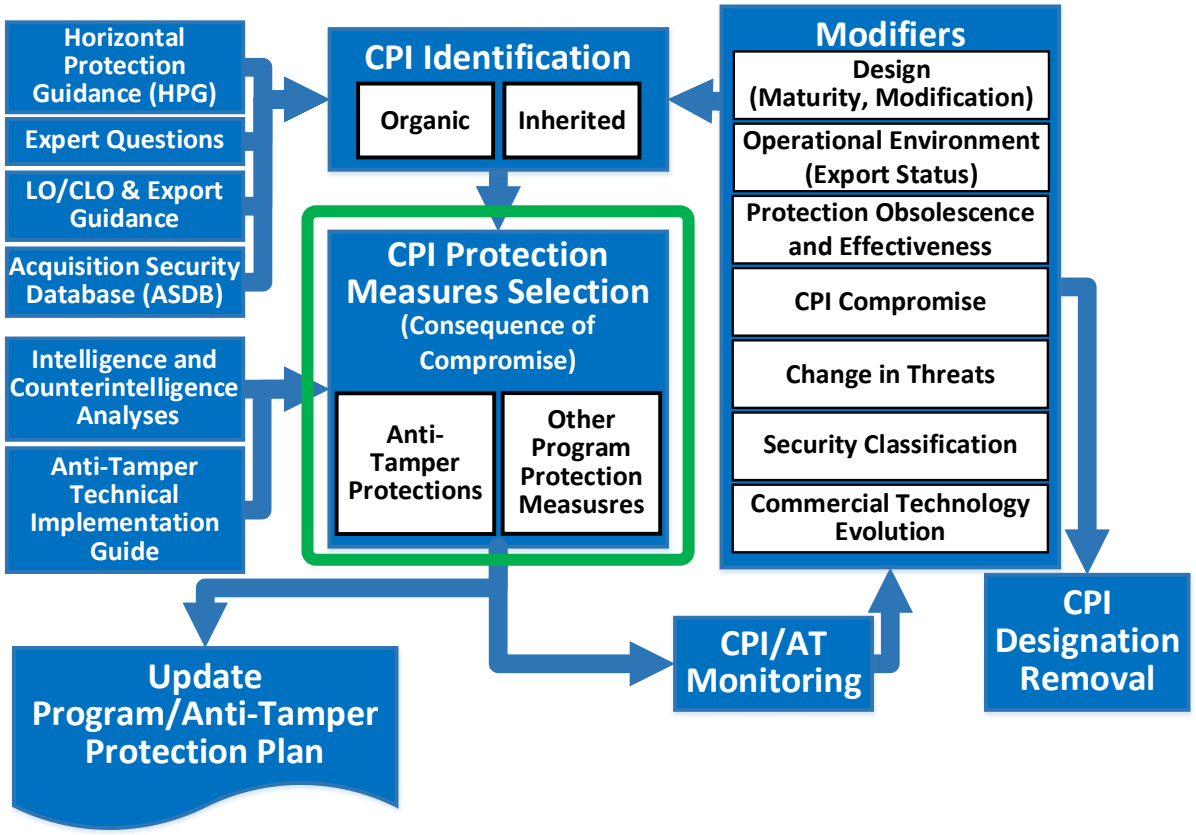
- **The OUSD for Research and Engineering (OUSD(R&E)) is running a working group to clarify the CPI processes**
  - Goals:
    - Align AT as a technology protection activity
    - Clarify AT processes
    - Clarify identification (and removal) criteria for CPI
  - Completed:
    - Mapping and identification of working group members
    - Mapping of the CPI identification process

CPI Process: CPI Identification



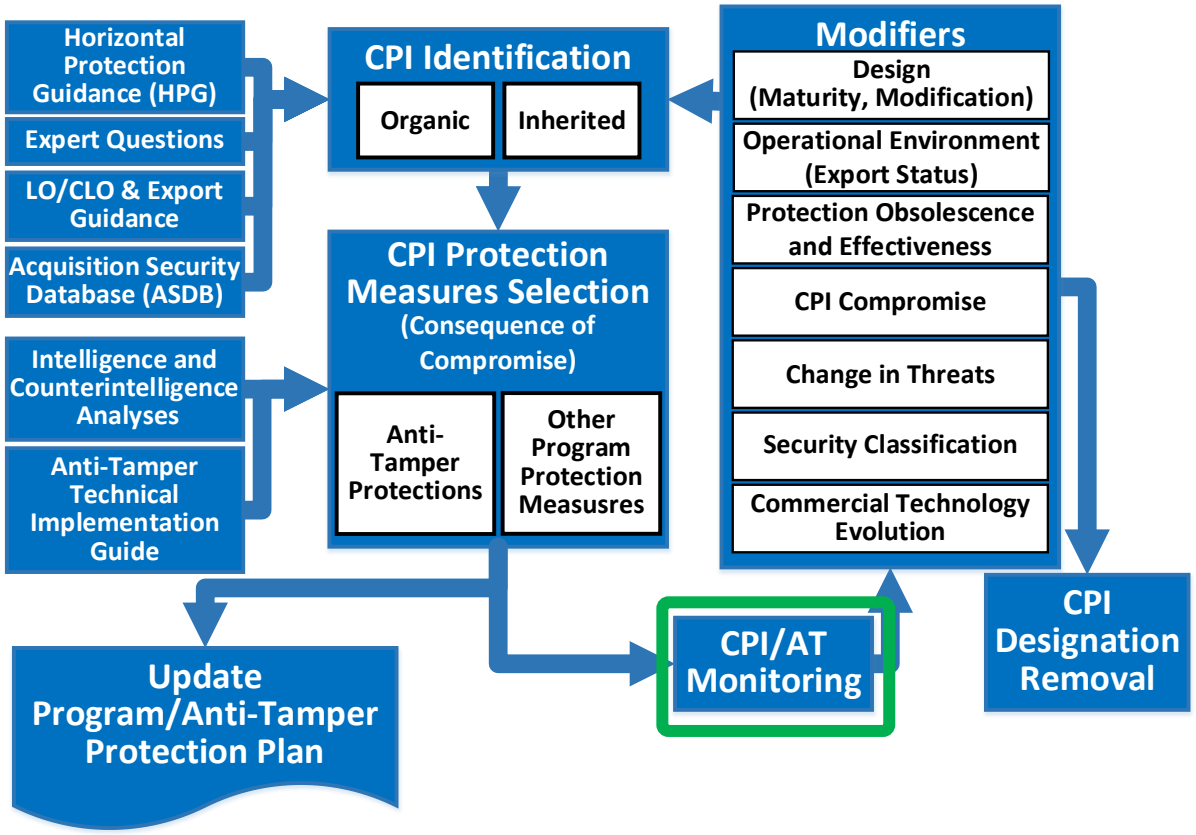
- **Stakeholders should:**
  - Identify CPI to determine if it is:
    - Organic CPI (developed by the program), and/or
    - Inherited CPI (developed by another program but incorporated into the program/system) exists or will exist in the operational, deployed system
  - Identify technology that DoD no longer considers to provide a U.S. technological advantage to the warfighter
- **S&T managers and engineers should identify CPI early and reassess the CPI throughout the lifecycle of the program, to include:**
  - Prior to:
    - Each acquisition milestone, or
    - Systems Engineering Technical Review;
  - Operations and sustainment; and
  - Software/hardware technology updates

CPI Process: CPI Protection Measure Selection



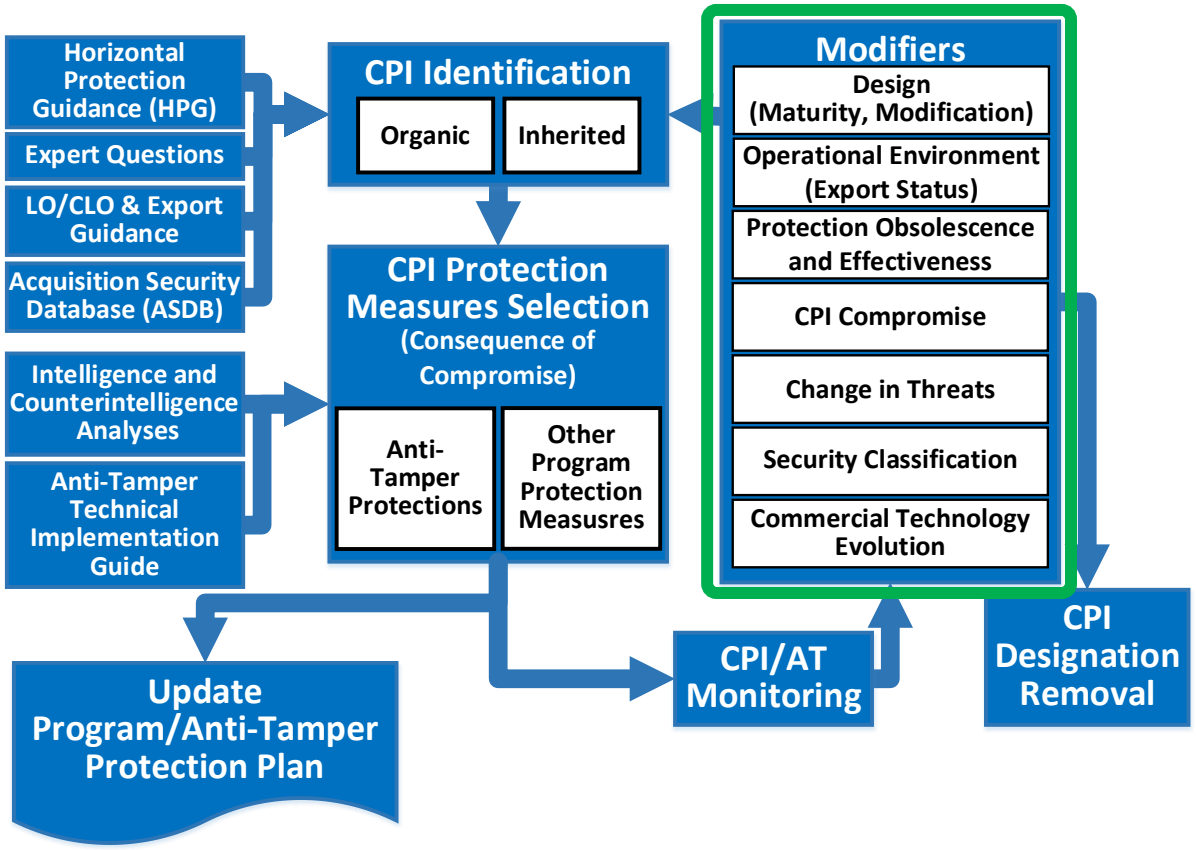
- **Stakeholders should:**
  - Select CPI protection measures soon after identification of the CPI
- **Protection measures seek to protect the warfighter's technical advantage by deterring, delaying, detecting, or reacting to:**
  - Reverse engineering attempts, or
  - Other attacks on the warfighter's technical advantage
- **Other protection measures, listed under other systems security engineering specialties and other security specialties, may also contribute to the protection of CPI**
  - Design and manufacturing know-how is protected in accordance with the classification guidance and protection mechanisms
  - When manufacturing information is considered unclassified controlled technical information (CTI), a Component would protect it in accordance with the protections for CTI

CPI Process: Monitoring



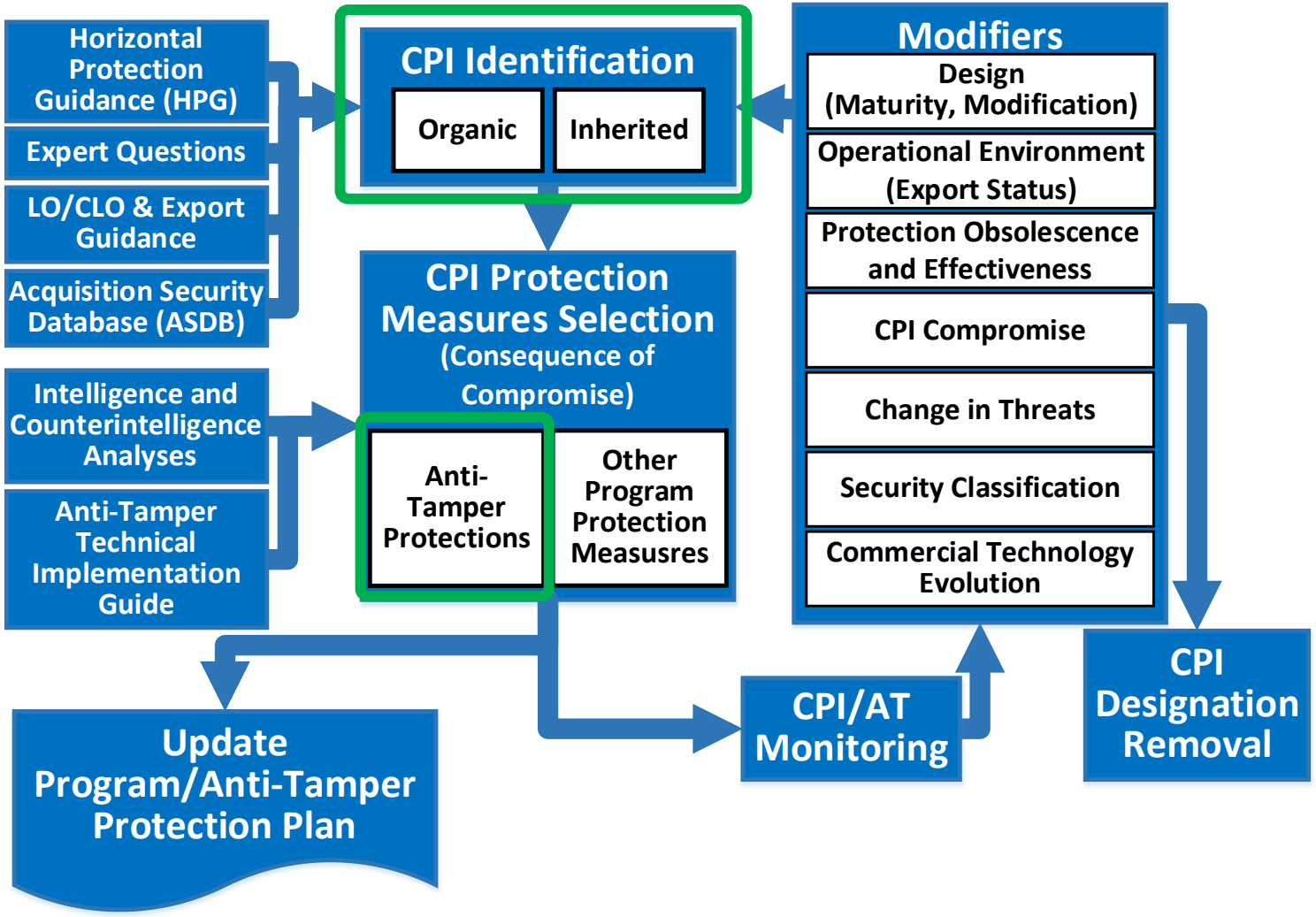
- **Stakeholders should:**
  - Commence CPI monitoring soon after identifying the CPI
  - Continue this monitoring throughout the lifecycle of the program
- **CPI monitoring determines:**
  - If an event has occurred that requires a reassessment of the CPI or its protection measures
  - Removal of the CPI designation
- **If (or when) these events occur, programs should reassess the CPI and protection measures to determine if they can or need to make changes to the CPI's associated protection measures**

CPI Process: Modifiers



- **Design:**
  - **Capability maturation**: A change in the state-of-the-art for a particular capability and thus the thresholds used for CPI identification
  - **System modification**: A change to the system architecture and/or designs
- **Operational Environment**: A change in the physical location of the system with CPI other than that for which it was originally designed
  - **Export status:** Current or future plans for the system to be available to allies or partners through Direct Military Sales or other export programs
- **Protection Obsolescence or Effectiveness**: A change in the ability of the CPI protections to deter, delay, detect, and respond to attempts to compromise CPI
- **CPI Compromise:** A known loss of the capability can result in a change in the need to protect the capability
- **Change in Threats**: A change in foreign adversary interest and skill in obtaining CPI
- **Security Classification:** A change to a relevant SCG
- **Commercial Technology Evolution:** Improvements in the state-of-the-art can erode technical advantage over time

Ongoing CPI Process Improvement Working Groups



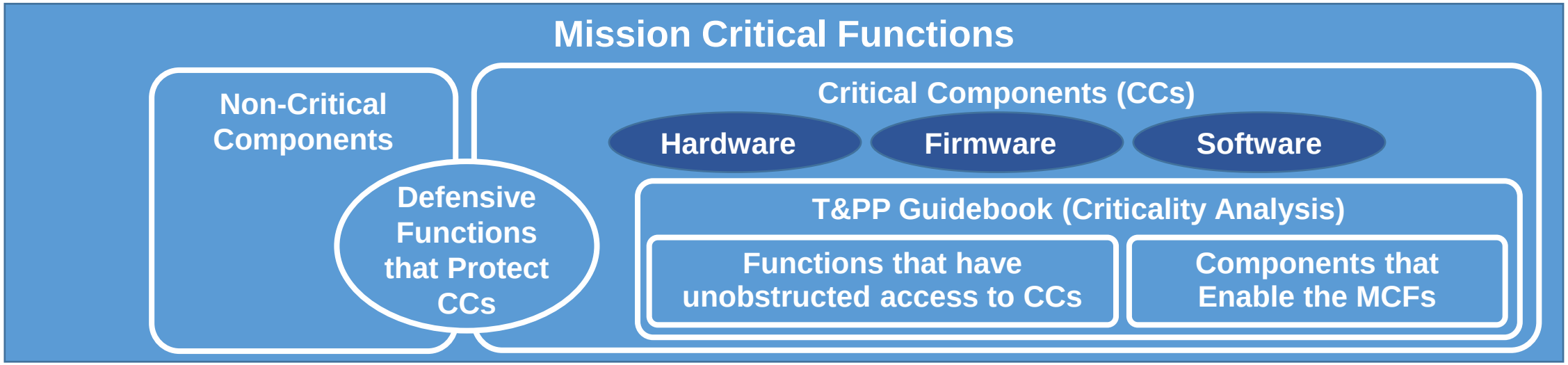
CPI Identification Working Group

- **Working within the larger DoD Community:**
  - Clarify and refine the identification process
  - Discuss and develop criteria for CPI designation removal

AT Processes Tiger Team

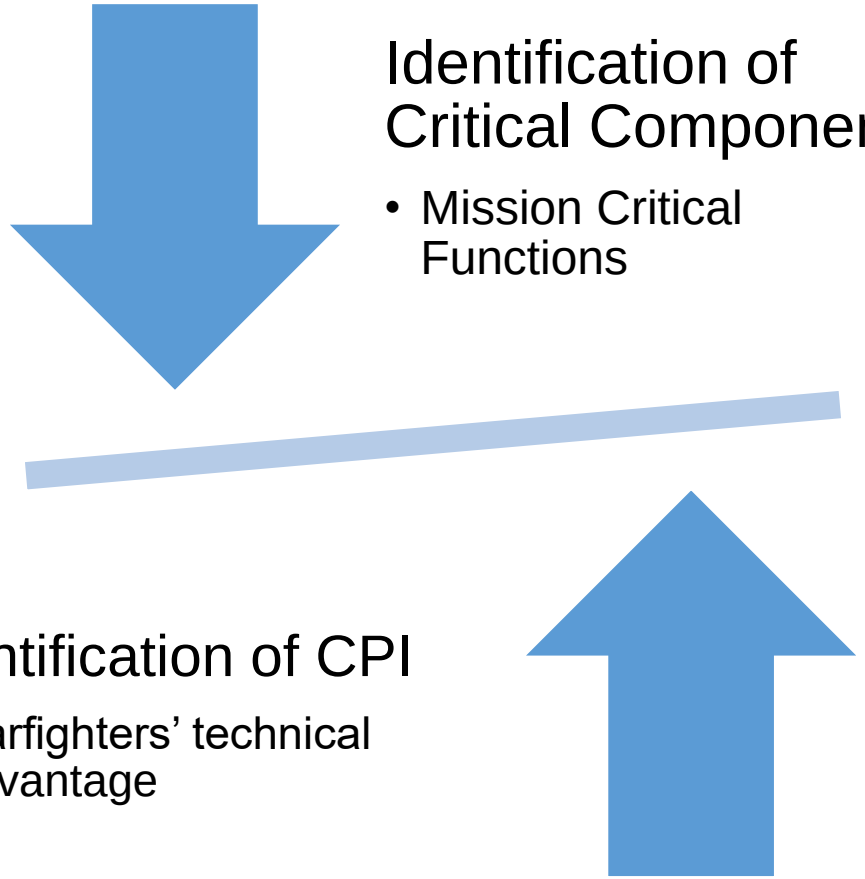
- **Working within the AT community:**
  - Identify potential efficiencies in applying AT to identified technologies

DoDI 5200.44 and T&PP Guidebook: Mission Critical Functions and Components



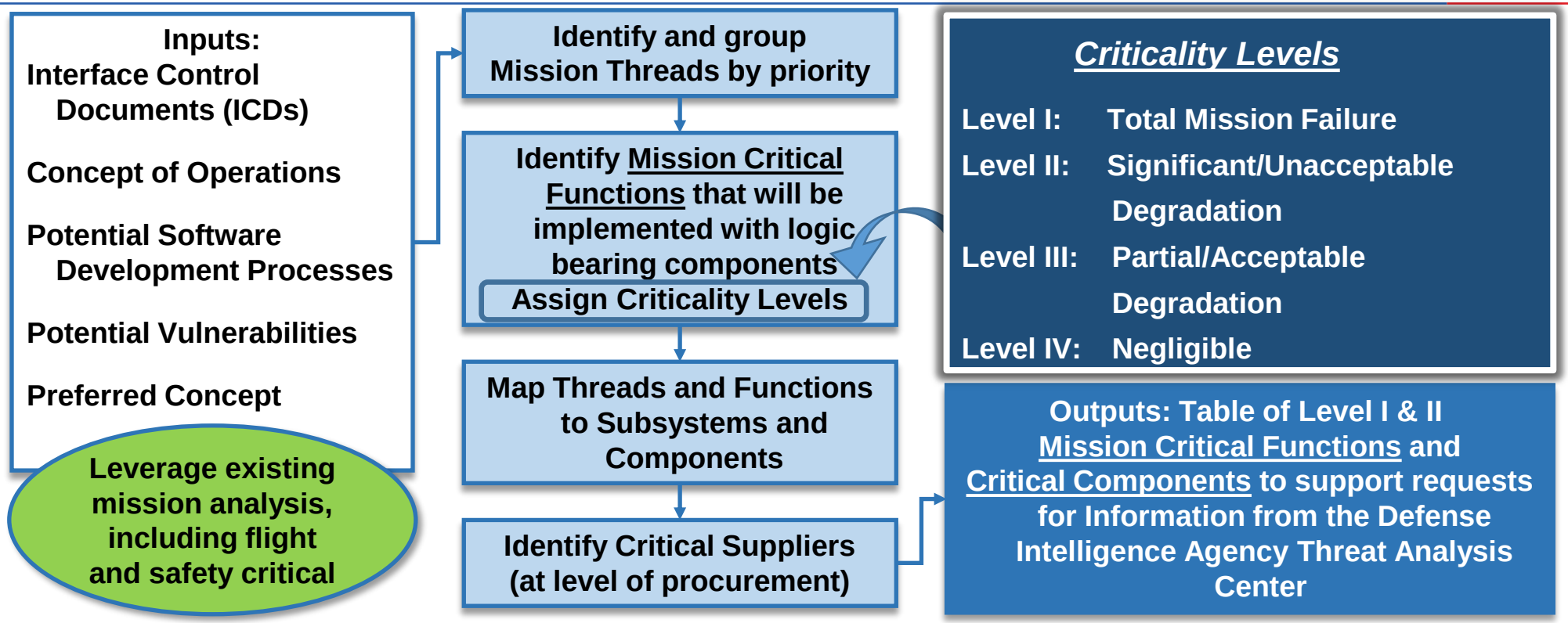
- **Mission Critical Functions (MCFs):**
  - Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed (Source: DoDI 5200.44)
- **Critical Components (CCs):**
  - **A component which is or contains information and communications 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)

Critical Components and CPI Identification



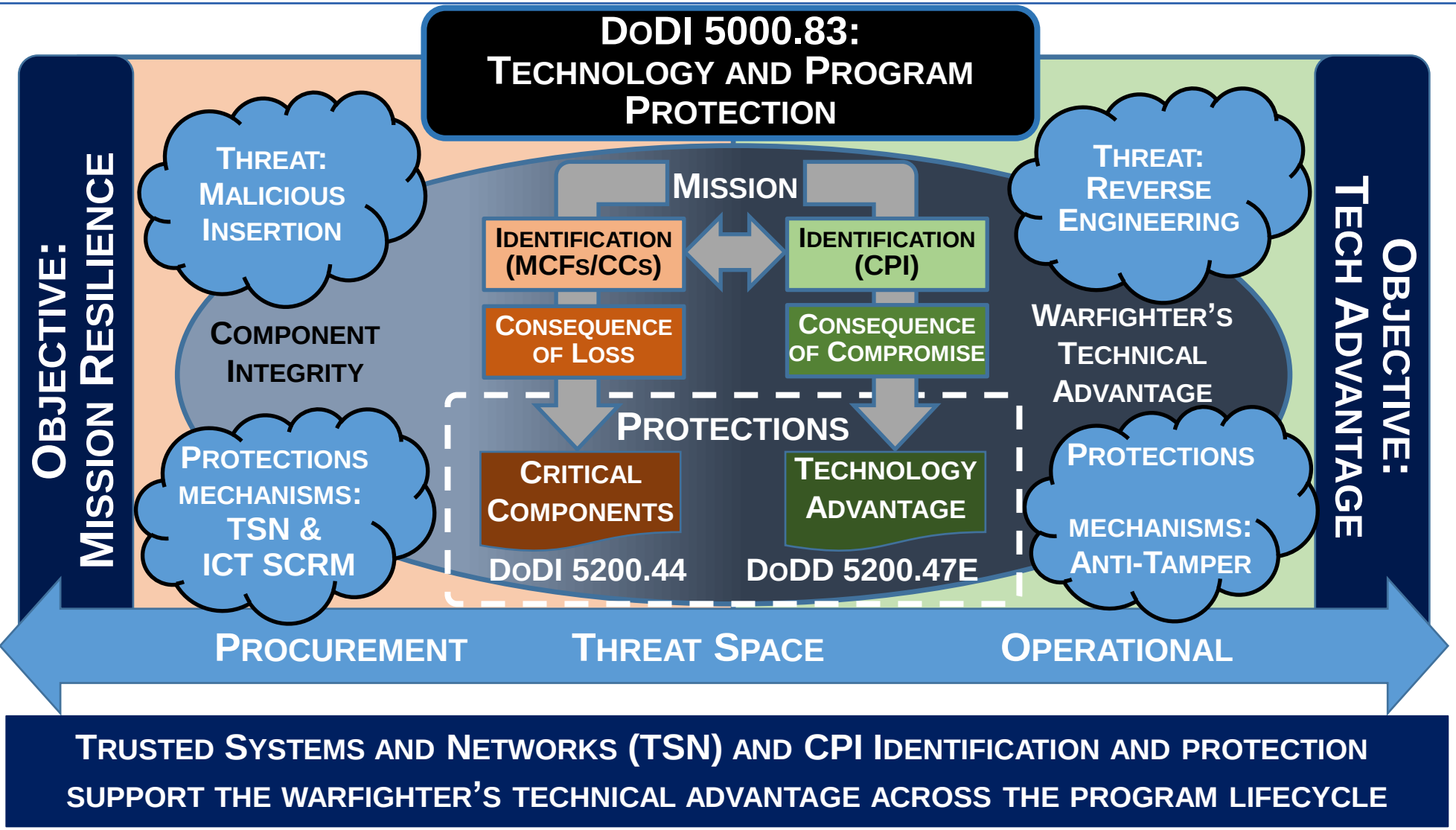
- **Identification of Critical Components (CCs) supports the system's ability to complete the assigned mission if that component is lost due to sabotage**
- **Identification of CPI supports the DoD's ability to protect the warfighter's technical advantage from loss**
  - Components that protect Mission Critical Functions become CCs too
- **While there is overlap in the components and technologies identified, there are enough unique properties to each process that they should be evaluated separately**
  - CPI Process may identify components and technologies that are not critical to the mission (training and maintenance)
  - Mission Critical Function Process may identify components that don't directly contribute to the warfighter's technical advantage

Criticality Analysis DoDI 5200.44 Definition and Methodology



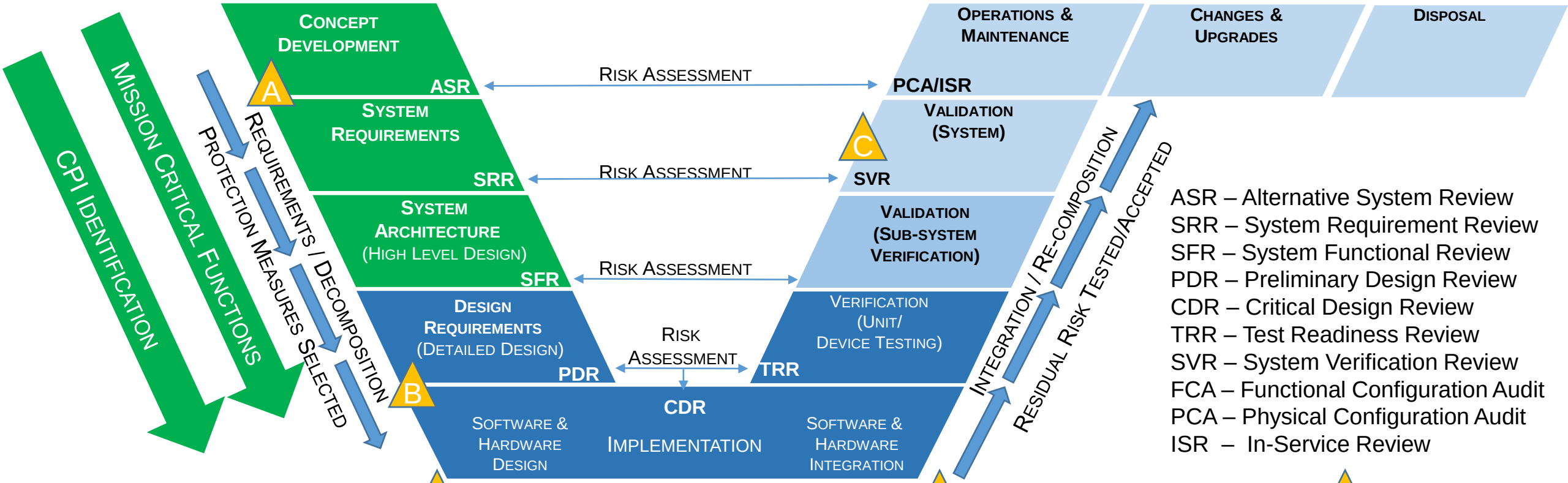
An end-to-end **functional decomposition** performed by systems engineers to **identify mission critical functions (MCFs) and components**. Includes identification of system missions, decomposition into the functions to perform those missions, and **traceability to the hardware, software, and firmware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

Technology and Program Protection in the Adaptive Acquisition Framework



- **DoDI 5000.83 provides S&T managers and lead engineers responsibilities for all technology and program protection activities**
- **DoDI 5200.44 and DoDD 5200.47E provide additional responsibilities for protections from specific vulnerabilities prioritized based on operational mission**
- **Each Component implements the policies in the manner that works best for them**

Systems Engineering "V": CPI Identification and Trusted Systems and Networks Criticality Analysis



ASR – Alternative System Review
SRR – System Requirement Review
SFR – System Functional Review
PDR – Preliminary Design Review
CDR – Critical Design Review
TRR – Test Readiness Review
SVR – System Verification Review
FCA – Functional Configuration Audit
PCA – Physical Configuration Audit
ISR – In-Service Review

	ASR	A	SRR	SFR	PDR	B	CDR	SVR	C	PCA/ISR
Criticality Analysis (CA)	Mission-based functions		System requirements	Sub-system/ sub-function level	Assembly/ component		Component (updated)	Component (updated)		Component (updated)
CPI Identification and Protection	AT Plan (concept) (105 Days before MS A)			AT Plan (initial)	AT Plan (final) AT Eval Plan (draft)		AT Eval Plan (final) AT Eval Report	CPI Validated		CPI Validated

Next Steps

- **Next steps**
  - Conduct use-case analysis with:
    - Anti-Tamper Program Office (ATPO)
    - Special Access Program Central Office (SAPCO)
    - International cooperation
  - Identify efficiencies to be gained in the process
  - Work to develop a DoD tool for CPI identification
  - Out-brief Industry on output