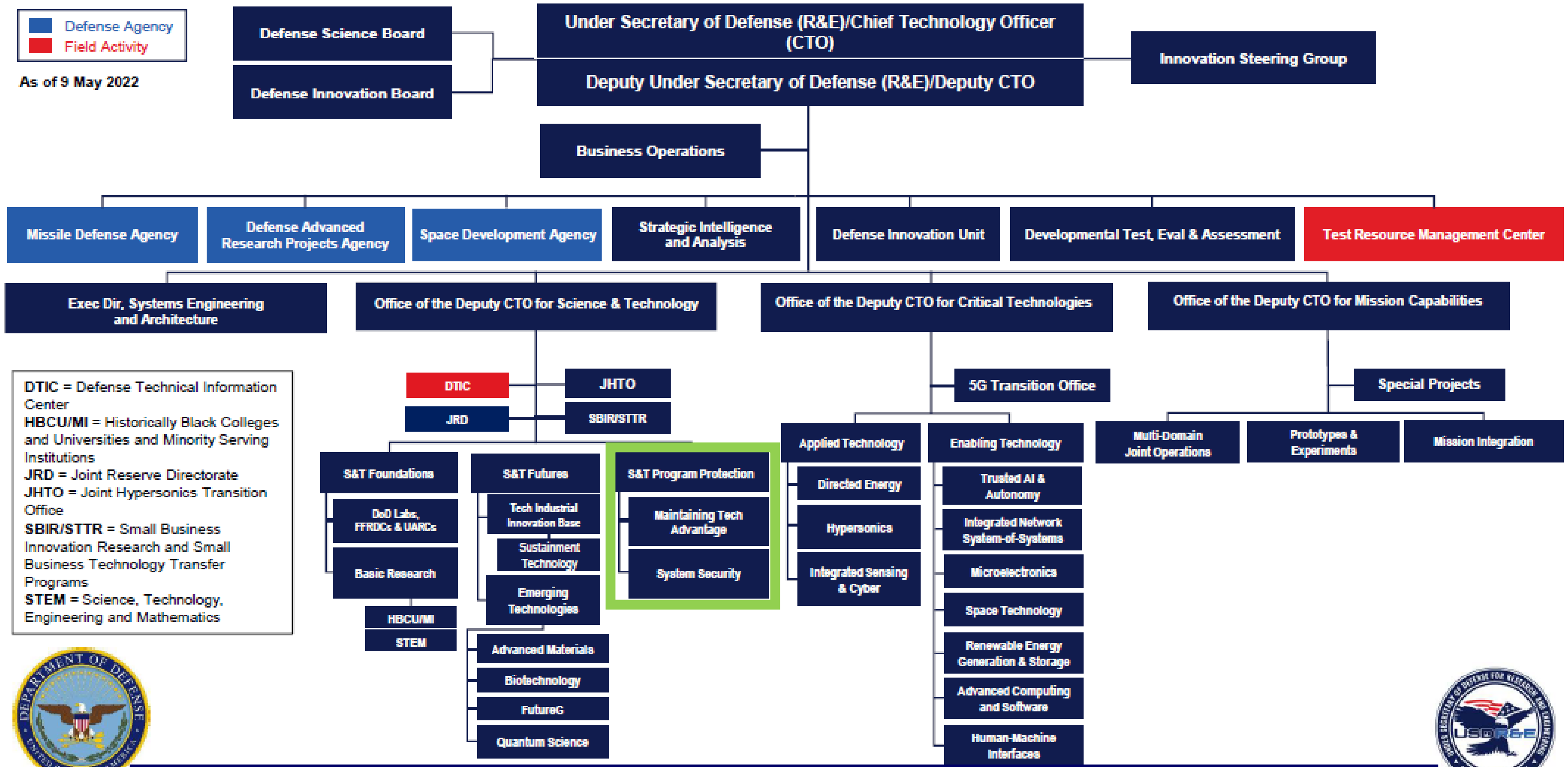
USD(R&E)

Critical Program Information (CPI) Identification Update

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
October 16 - 19, 2023

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Organization

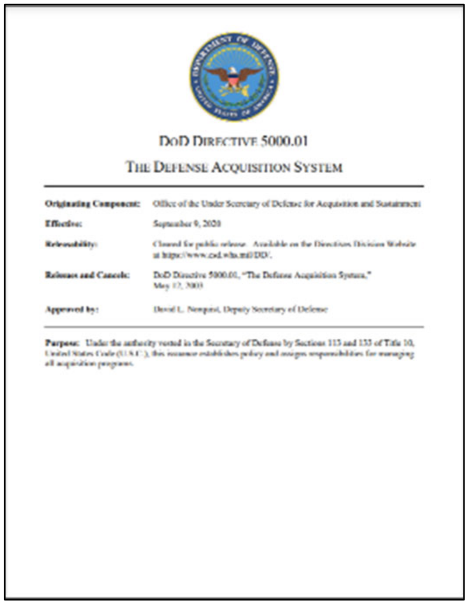

🟦 Defense Agency
🟥 Field Activity
As of 9 May 2022
Defense Science Board
Defense Innovation Board
Under Secretary of Defense (R&E)/Chief Technology Officer (CTO)
Deputy Under Secretary of Defense (R&E)/Deputy CTO
Innovation Steering Group
Business Operations
Missile Defense Agency
Defense Advanced Research Projects Agency
Space Development Agency
Strategic Intelligence and Analysis
Defense Innovation Unit
Developmental Test, Eval & Assessment
Test Resource Management Center
Exec Dir, Systems Engineering and Architecture
Office of the Deputy CTO for Science & Technology
Office of the Deputy CTO for Critical Technologies
Office of the Deputy CTO for Mission Capabilities
DTIC
JRD
JHTO
SBIR/STTR
S&T Foundations
DoD Labs, FFRDCs & UARCs
Basic Research
HBCU/MI
STEM
S&T Futures
Tech Industrial Innovation Base
Sustainment Technology
Emerging Technologies
Advanced Materials
Biotechnology
FutureG
Quantum Science
S&T Program Protection
Maintaining Tech Advantage
System Security
5G Transition Office
Applied Technology
Directed Energy
Hypersonics
Integrated Sensing & Cyber
Enabling Technology
Trusted AI & Autonomy
Integrated Network System-of-Systems
Microelectronics
Space Technology
Renewable Energy Generation & Storage
Advanced Computing and Software
Human-Machine Interfaces
Special Projects
Multi-Domain Joint Operations
Prototypes & Experiments
Mission Integration

DTIC = Defense Technical Information Center
HBCU/MI = Historically Black Colleges and Universities and Minority Serving Institutions
JRD = Joint Reserve Directorate
JHTO = Joint Hypersonics Transition Office
SBIR/STTR = Small Business Innovation Research and Small Business Technology Transfer Programs
STEM = Science, Technology, Engineering and Mathematics

STPP Mission: Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through <u>assured, secure and resilient</u> systems and a healthy viable national security innovation base

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

DoD Directive 5000.01 “The Defense Acquisition System” and Technology and Program Protection

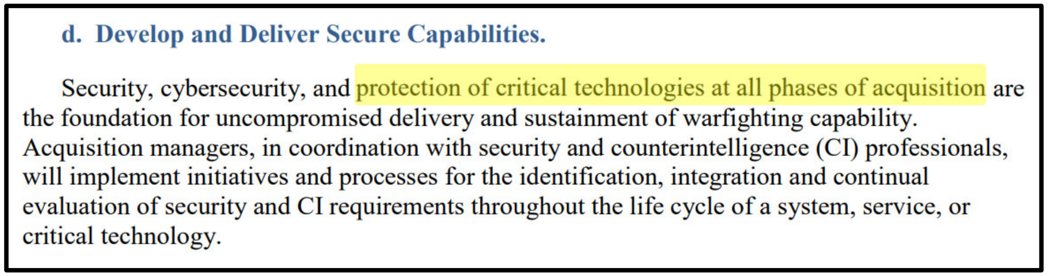


DoD Directive 5000.01

The Defense Acquisition System

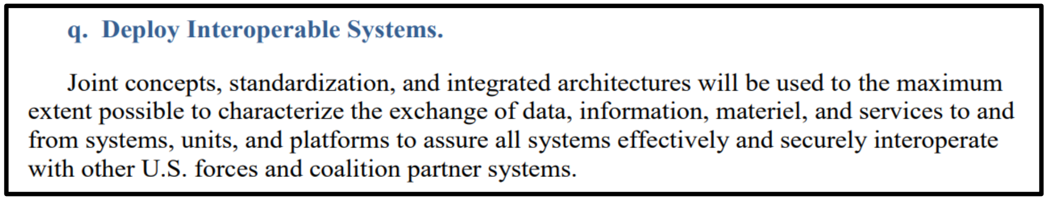
Originating Component:	Office of the Under Secretary of Defense for Acquisition and Sustainment
Effective:	September 9, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Releases and Cancels:	DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003
Approved by:	David L. Norquist, Deputy Secretary of Defense

Purpose: Under the authority vested in the Secretary of Defense by Sections 113 and 133 of Title 10, United States Code (U.S.C.), this issuance establishes policy and assigns responsibilities for managing all acquisition programs.



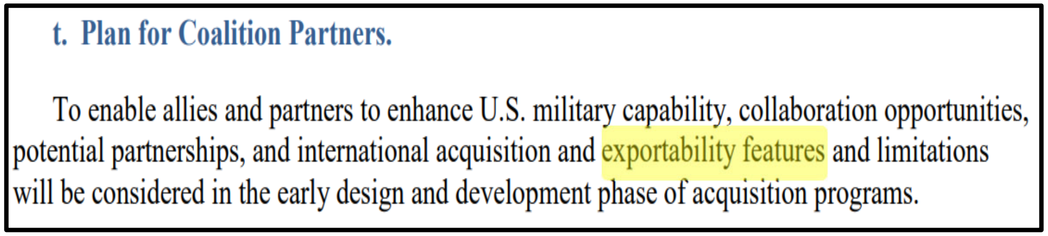
d. Develop and Deliver Secure Capabilities.

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.

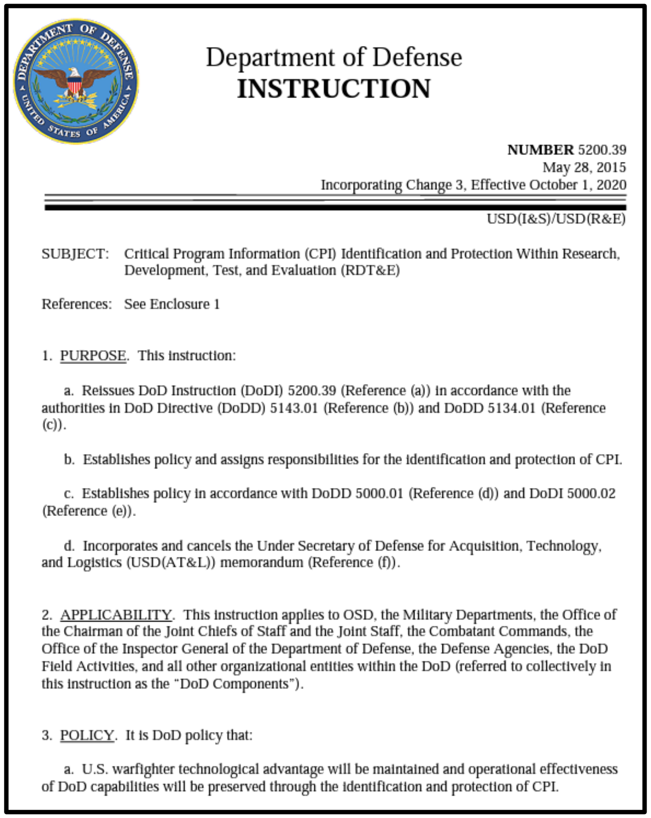
To enable allies and partners to enhance U.S. military capability, collaboration opportunities, potential partnerships, and international acquisition and exportability features and limitations will be considered in the early design and development phase of acquisition programs.

critical technology
(DoD Instruction 2040.02)

Technology or technologies essential to the design, development, production, operation, application, or maintenance of an article or service **that makes or could make a significant contribution to the military potential of any country**, including the United States. This includes, but is not limited to, design and manufacturing know-how, technical data, software, keystone equipment, and inspection and test equipment.

Three policy statements anchor program protection and anti-tamper into the Defense Acquisition System in support of the 2022 National Defense Strategy

What have we accomplished?
Identified Gaps within the DoDI 5200.39



Department of Defense
INSTRUCTION

NUMBER 5200.39
May 28, 2015
Incorporating Change 3, Effective October 1, 2020

USD(I&S)/USD(R&E)

SUBJECT: Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues DoD Instruction (DoDI) 5200.39 (Reference (a)) in accordance with the authorities in DoD Directive (DoDD) 5143.01 (Reference (b)) and DoDD 5134.01 (Reference (c)).

b. Establishes policy and assigns responsibilities for the identification and protection of CPI.

c. Establishes policy in accordance with DoDD 5000.01 (Reference (d)) and DoDI 5000.02 (Reference (e)).

d. Incorporates and cancels the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) memorandum (Reference (f)).

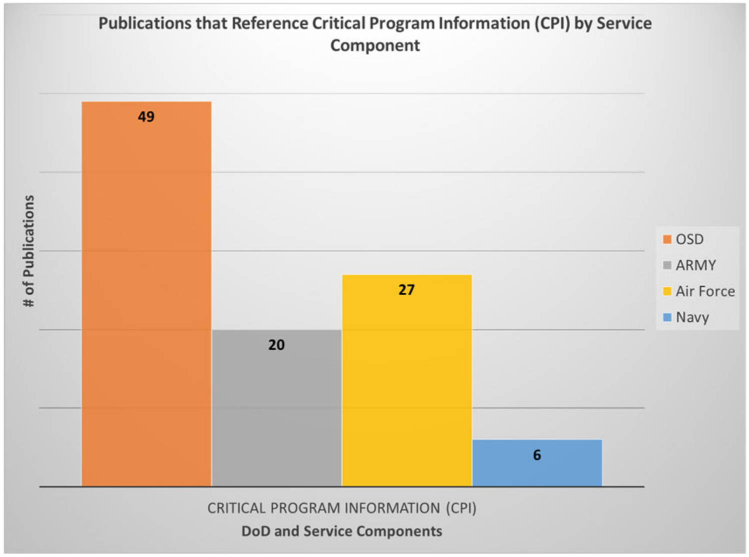
2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other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

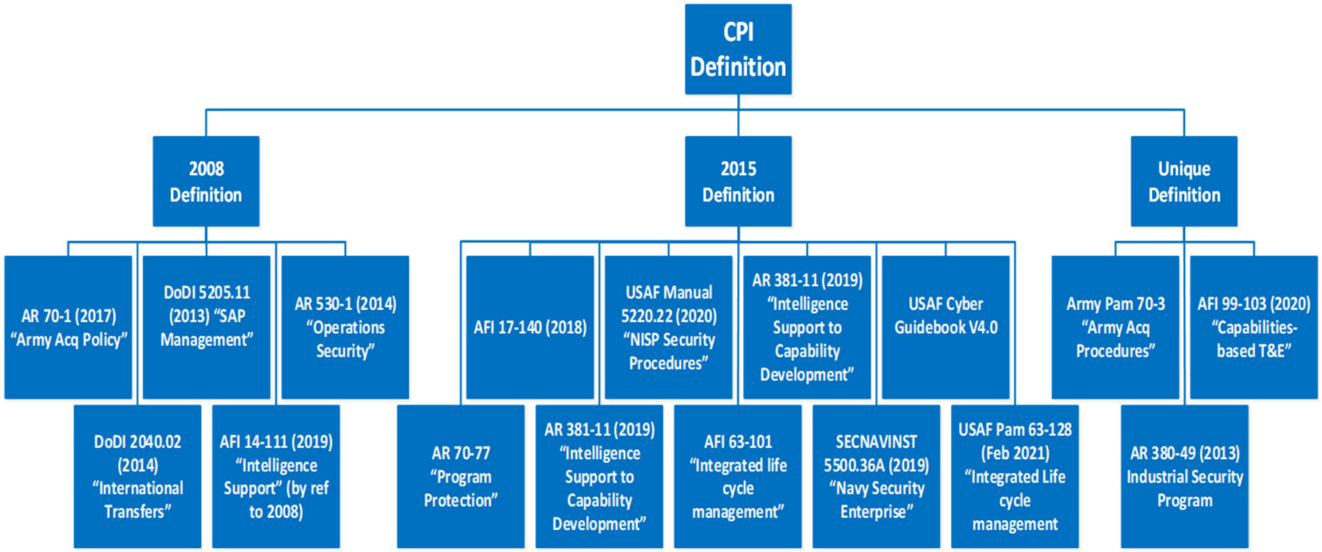
3. POLICY. It is DoD policy that:

a. U.S. warfighter technological advantage will be maintained and operational effectiveness of DoD capabilities will be preserved through the identification and protection of CPI.

- **Capability elements (defined as part of the CPI definition) includes "may include, but are not limited to" the illustrative examples which potentially contributes to the confusion.**
- **The subject of DoDI 5200.39 is CPI Identification and Protection Within Research, Development, Test and Evaluation (RDT&E), which includes design and development phases of the system lifecycle. Definition needs to reflect this scope clearly.**
- **5200.39 clearly states the DoD policy is:**
  - Identify CPI early and reassess throughout the RDT&E program so that CPI protections requirements and countermeasures may be identified and applied as CPI is developed and modified throughout the lifecycle as needed.
  - It is imperative to preserve CPI protections early and throughout the lifecycle.
- **DoDI 5200.39 contains "Horizontal Protection" responsibilities for the "Secretary of the Air Force" that are executed as the AT Executive Agent.**
  - "Conducts DoD-wide analysis of AT protections in support of horizontal protection"
- **DoDI 5200.39 is missing a responsibilities for:**
  - CPI Removal and Revalidation
  - CPI Identification in accordance with Technology Transfer

Challenge 1: DoD Has Multiple CPI Definitions
Critical Program Information (CPI) in Issuances





CPI Definition

2008 Definition
- AR 70-1 (2017) "Army Acq Policy"
- DoDI 5205.11 (2013) "SAP Management"
- AR 530-1 (2014) "Operations Security"
- DoDI 2040.02 (2014) "International Transfers"
- AFI 14-111 (2019) "Intelligence Support" (by ref to 2008)

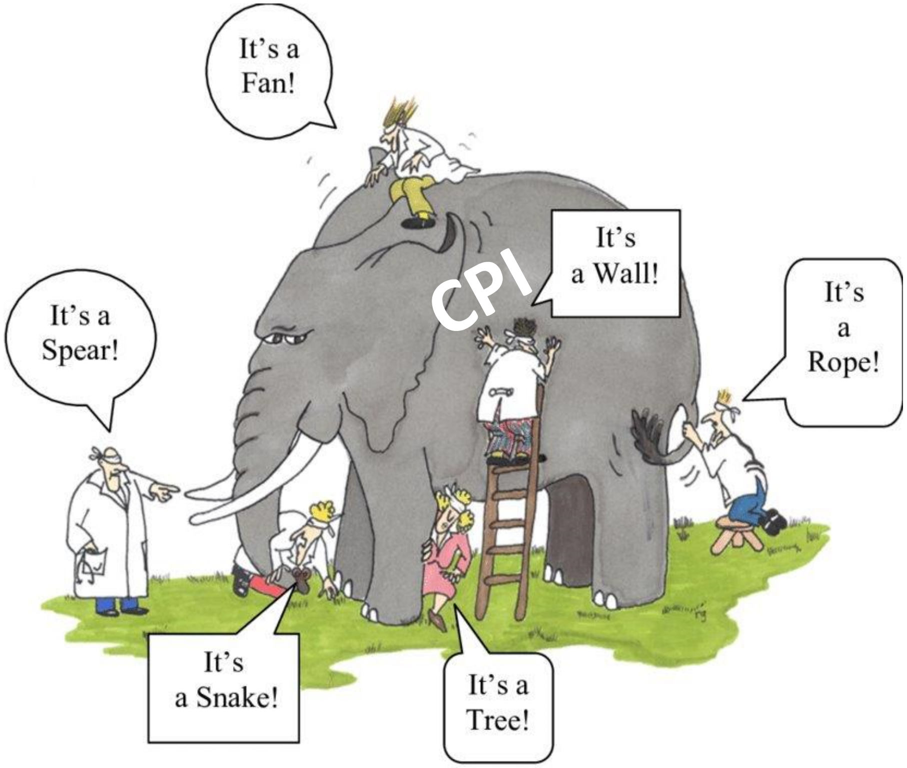
2015 Definition
- AFI 17-140 (2018)
- USAF Manual 5220.22 (2020) "NISP Security Procedures"
- AR 381-11 (2019) "Intelligence Support to Capability Development"
- USAF Cyber Guidebook V4.0
- AR 70-77 "Program Protection"
- AR 381-11 (2019) "Intelligence Support to Capability Development"
- AFI 63-101 "Integrated life cycle management"
- SECNAVINST 5500.36A (2019) "Navy Security Enterprise"
- USAF Pam 63-128 (Feb 2021) "Integrated Life cycle management

Unique Definition
- Army Pam 70-3 "Army Acq Procedures"
- AFI 99-103 (2020) "Capabilities-based T&E"
- AR 380-49 (2013) Industrial Security Program

- CPI is utilized in over 100 DoD and Component issuances
- There are multiple definitions (or references to the definition) in both DoD and Component policy
  - References to the 2008 and 2015 definition of CPI
  - References to the current definition of CPI
  - Unique references that do not trace to either definition

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Potential Solution 1: Create Overarching Definition for Critical Program Information (CPI) and Clarify Meaning with Adjectives



- We are all "looking at" and interested in the same thing.
  - ○ "warfighter's technical advantage" and,
  - ○ "if compromised undermines military preeminence"

○ Preliminary Definition:

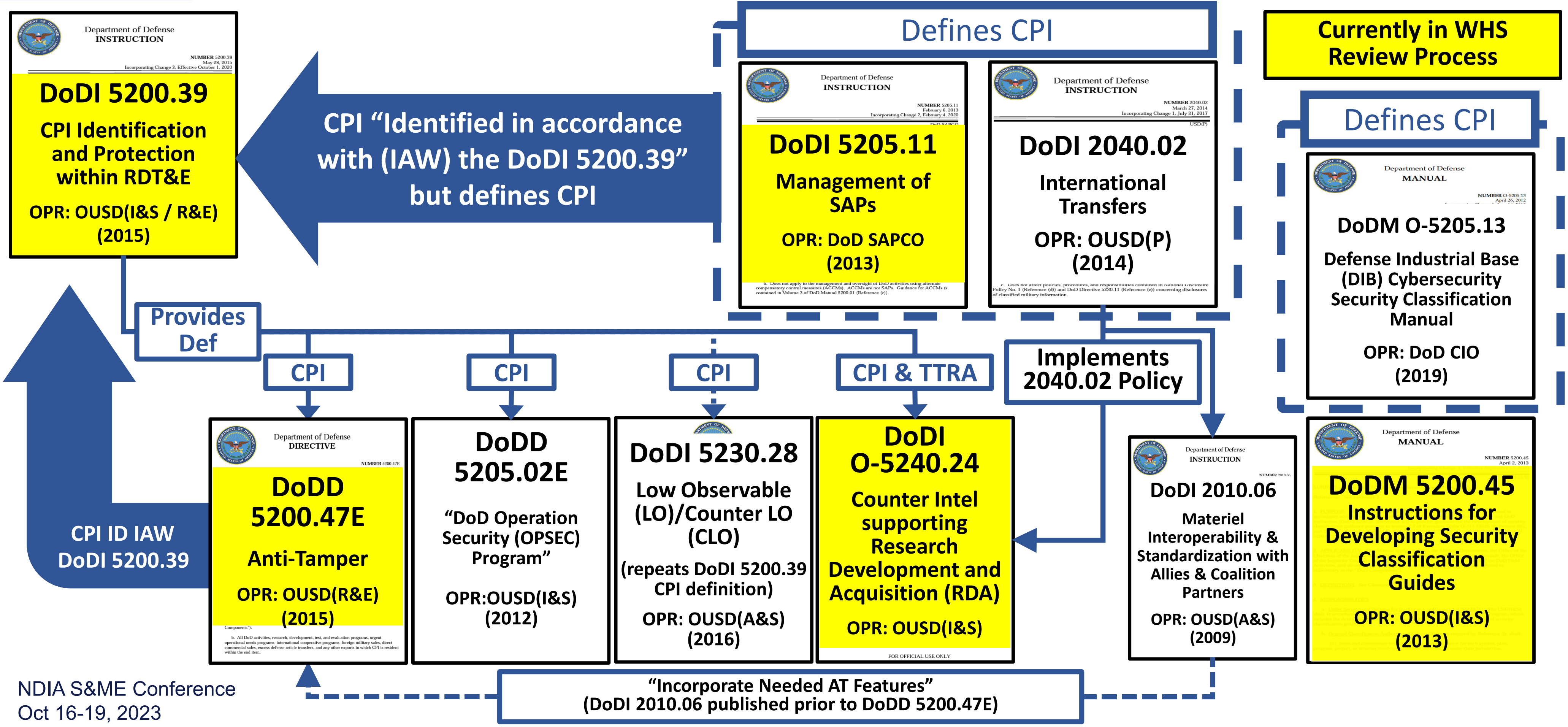
DoD ~~U.S.~~ capabilities ~~elements~~ that contribute to the **warfighter's technical advantage**, which **if compromised, undermines U.S. military preeminence**. ~~U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.~~

○ Used to identify:

- ○ Technology Transfer
- ○ Technology Protection (Anti-Tamper)
- ○ Security (SAP)

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Framework of Dependent Policies:
Policies that Define or Assign Responsibilities for CPI



Department of Defense
INSTRUCTION
NUMBER 5200.39
May 28, 2015
Incorporating Change 3, Effective October 1, 2020

DoDI 5200.39
CPI Identification and Protection within RDT&E
OPR: OUSD(I&S / R&E) (2015)

CPI "Identified in accordance with (IAW) the DoDI 5200.39" but defines CPI

Defines CPI

Department of Defense
INSTRUCTION
NUMBER 5205.11
February 6, 2013
Incorporating Change 2, February 4, 2020
DoD SAPCO

DoDI 5205.11
Management of SAPs
OPR: DoD SAPCO (2013)

b. Does not apply to the management and oversight of DoD activities using alternate compensatory control measures (ACCMs). ACCMs are not SAPs. Guidance for ACCMs is contained in Volume 3 of DoD Manual 5200.01 (Reference (c)).

Department of Defense
INSTRUCTION
NUMBER 2040.02
March 27, 2014
Incorporating Change 1, July 31, 2017
USD(P)

DoDI 2040.02
International Transfers
OPR: OUSD(P) (2014)

c. Does not affect policies, procedures, and responsibilities contained in National Disclosure Policy No. 1 (Reference (d)) and DoD Directive 5230.11 (Reference (e)) concerning disclosures of classified military information.

Currently in WHS Review Process

Defines CPI

Department of Defense
MANUAL
NUMBER O-5205.13
April 26, 2012

DoDM O-5205.13
Defense Industrial Base (DIB) Cybersecurity Security Classification Manual
OPR: DoD CIO (2019)

Provides Def

CPI

CPI

CPI

CPI & TTRA

Implements 2040.02 Policy

CPI ID IAW DoDI 5200.39

Department of Defense
DIRECTIVE
NUMBER 5200.47E

DoDD 5200.47E
Anti-Tamper
OPR: OUSD(R&E) (2015)

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.

DoDD 5205.02E
"DoD Operation Security (OPSEC) Program"
OPR:OUSD(I&S) (2012)

DoDI 5230.28
Low Observable (LO)/Counter LO (CLO)
(repeats DoDI 5200.39 CPI definition)
OPR: OUSD(A&S) (2016)

DoDI O-5240.24
Counter Intel supporting Research Development and Acquisition (RDA)
OPR: OUSD(I&S)

FOR OFFICIAL USE ONLY

Department of Defense
INSTRUCTION
NUMBER 2010.06

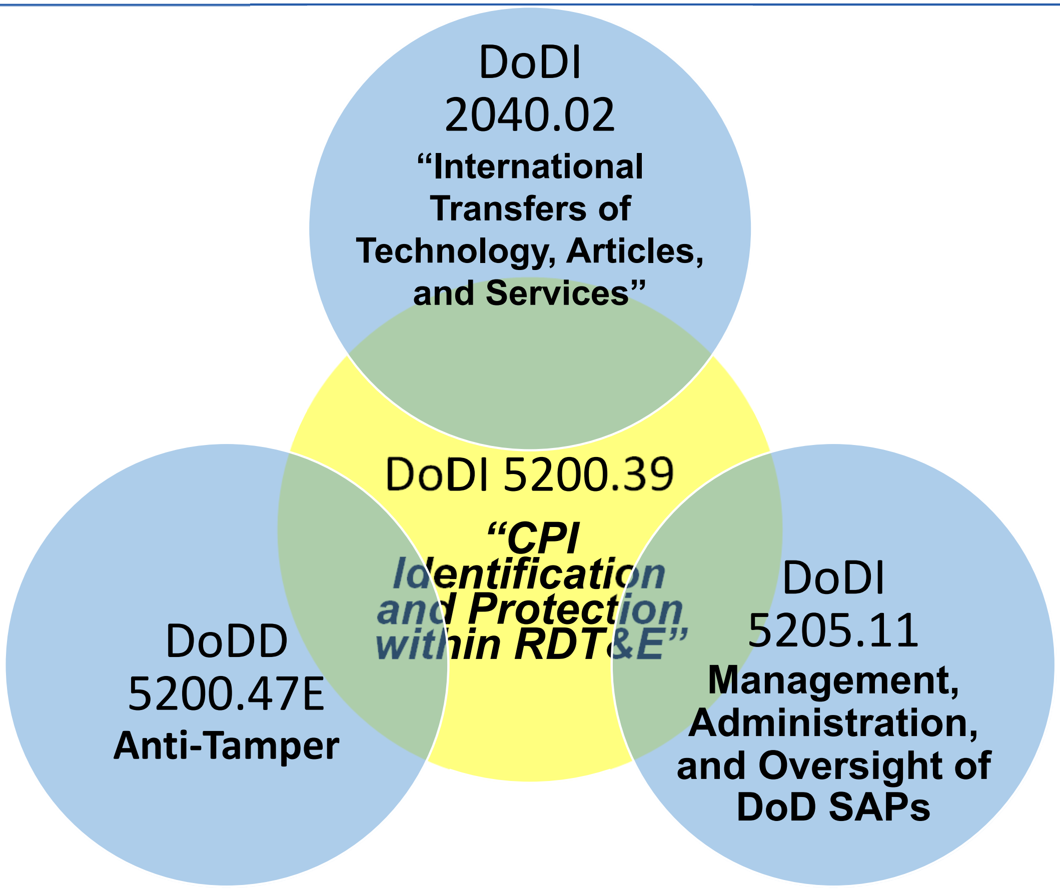
DoDI 2010.06
Materiel Interoperability & Standardization with Allies & Coalition Partners
OPR: OUSD(A&S) (2009)

Department of Defense
MANUAL
NUMBER 5200.45
April 2, 2013

DoDM 5200.45
Instructions for Developing Security Classification Guides
OPR: OUSD(I&S) (2013)

"Incorporate Needed AT Features"
(DoDI 2010.06 published prior to DoDD 5200.47E)

Proposed Alignment of Critical Program Information (CPI) with Communities of Interest



DoDI 2040.02
"International Transfers of Technology, Articles, and Services"

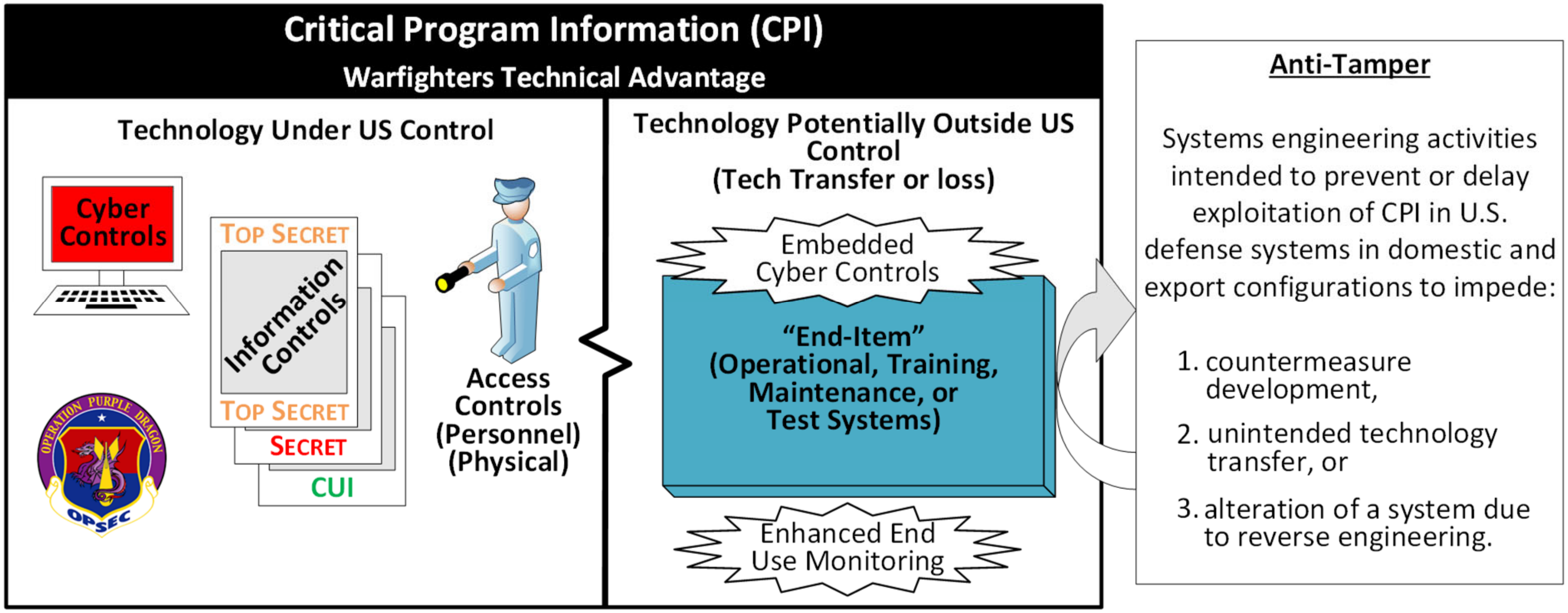
DoDI 5200.39
"CPI Identification and Protection within RDT&E"

DoDD 5200.47E
Anti-Tamper

DoDI 5205.11
Management, Administration, and Oversight of DoD SAPs

- Rational: CPI exists across the lifecycle of the program and needs to be protected from concept through fielding
- DoDI 5200.39 will contain:
  - Central definition for CPI (other issuances will align to this definition)
  - Responsibilities to identify CPI required by:
    - Special Access Programs (SAPs)
    - Anti-Tamper Community (AT)
    - Technology Transfer Community
  - Responsibilities to revalidate and remove CPI designation as appropriate.
- Each community utilizing CPI will align protections and other unique attributes under their specific issuance

Potential Solution 1: Create Overarching Definition for CPI, Scope of CPI and Unique Protection Characteristics



Critical Program Information (CPI)

Warfighters Technical Advantage

Technology Under US Control

Cyber Controls

Information Controls

TOP SECRET

TOP SECRET

SECRET

CUI

Access Controls (Personnel) (Physical)

OPERATION PURPLE DRAGON

OPSEC

Technology Potentially Outside US Control (Tech Transfer or loss)

Embedded Cyber Controls

"End-Item" (Operational, Training, Maintenance, or Test Systems)

Enhanced End Use Monitoring

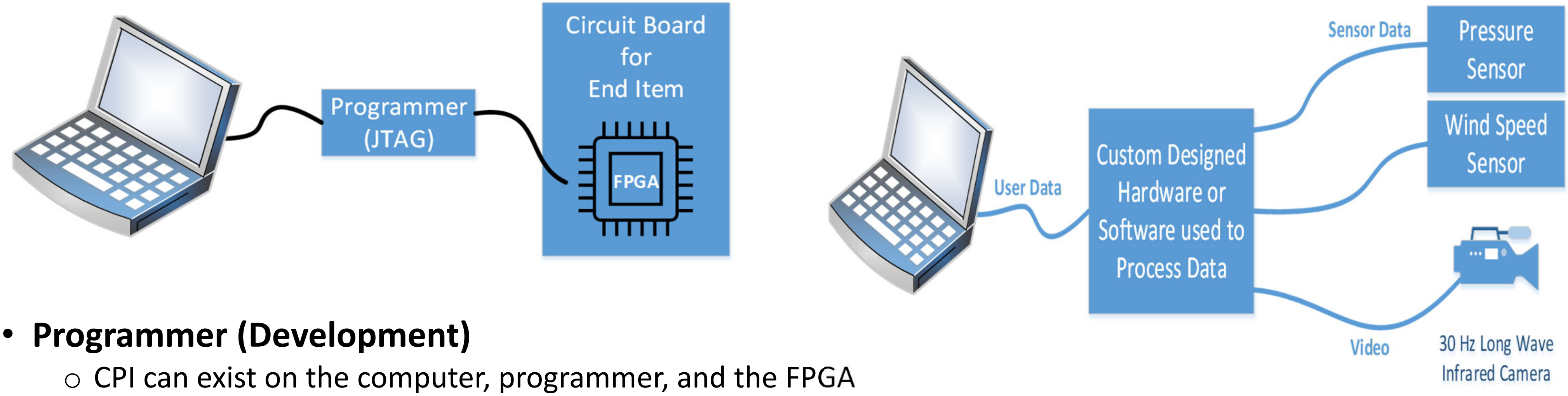
Anti-Tamper

Systems engineering activities intended to prevent or delay exploitation of CPI in U.S. defense systems in domestic and export configurations to impede:

1. countermeasure development,
2. unintended technology transfer, or
3. alteration of a system due to reverse engineering.

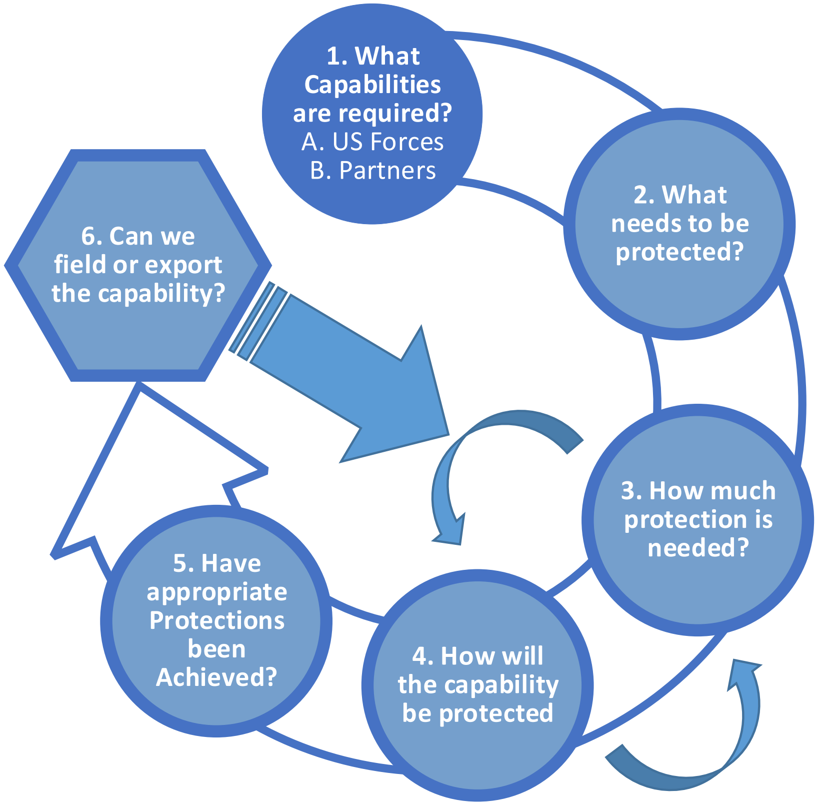
- CPI does not "appear" on the end-item. CPI exists from the start of a program and is developed.
  - During development: Cyber Controls, Information Controls, Operational Security (OPSEC), and Physical and Personnel Security all play a roll in protecting the capability.
  - Once the capability is outside of US Control in a system: Embedded cyber, Enhanced End Use Monitoring, and Anti-Tamper protect the capability.

Potential Solution 1: Create Overarching Definition for CPI
Where does CPI Exist in Systems?



- **Programmer (Development)**
  - CPI can exist on the computer, programmer, and the FPGA
  - Only the CPI on the FPGA would be considered for Anti-Tamper or “resident” CPI
- **System (Operation)**
  - CPI can only exist in the custom hardware and software (not COTS).
  - User and/or Sensor Data is not CPI (may be classified)
  - System components (30 Hz LWIR Camera) may have export restrictions (depending on country) but is not CPI by default

Challenge 2: Differing Chains of Command Use Different CPI Processes


1. What Capabilities are required?
A. US Forces
B. Partners
2. What needs to be protected?
3. How much protection is needed?
4. How will the capability be protected
5. Have appropriate Protections been Achieved?
6. Can we field or export the capability?

1. **What Capabilities are Required?**
   - **A. US Forces**
   - **B. Partners**
2. **What needs to be protected?**
3. **How much protection is needed?**
4. **How will the capability be protected?**
5. **Have the appropriate protections been achieved?**
6. **Can we field or export the capability?**

A. US Forces?

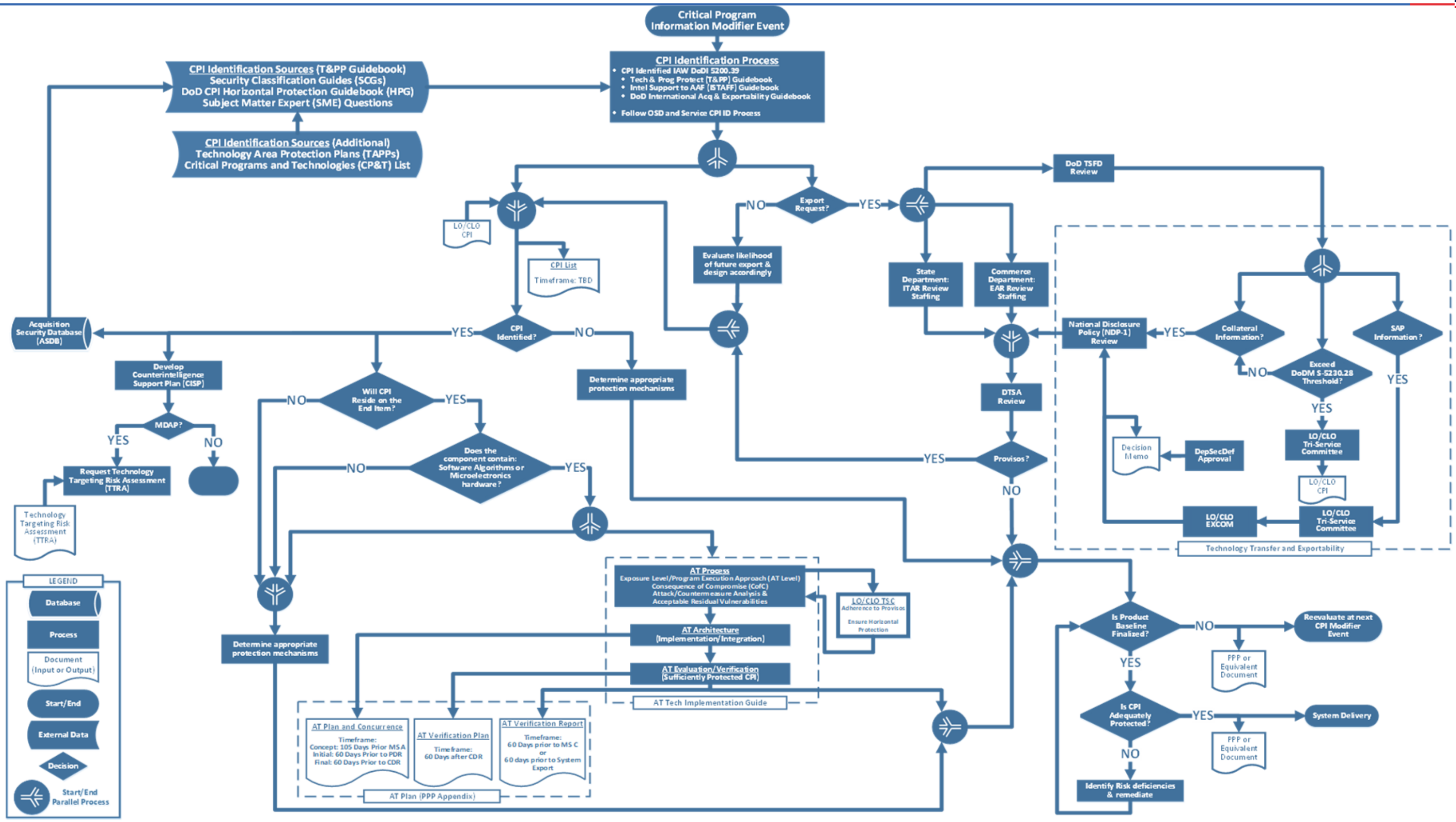
- Milestone Decision Authority (MDA) is responsible for assessing overall program risk and approve, as appropriate, the acquisition strategy at major decision points.
- Cost, Schedule, and Performance are driving factors for MDA

B. Partner Nations?

- Arms transfer decisions are **foreign policy and national security decisions** that support broader United States policy objectives. (NATIONAL SECURITY MEMORANDUM/NSM-18)

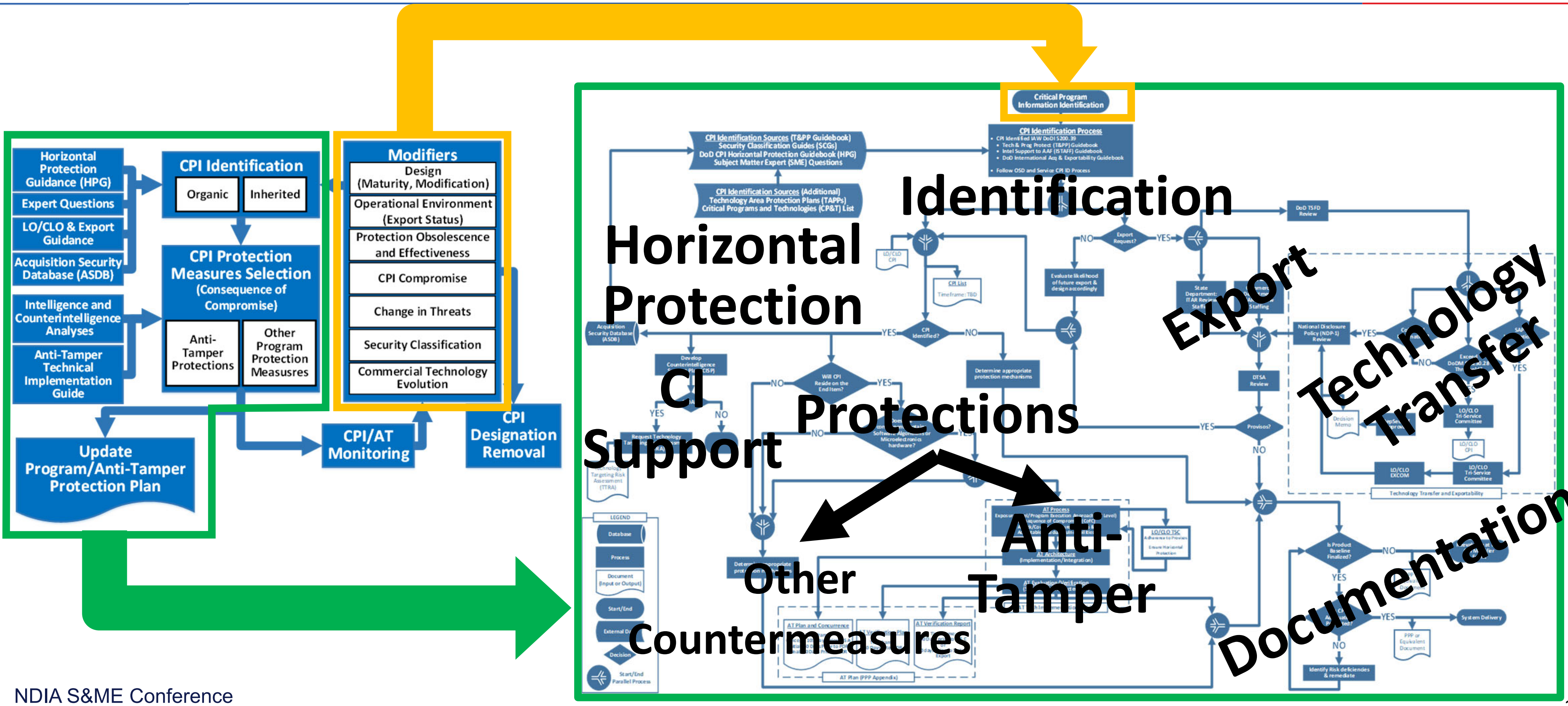
Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Challenge 2: Differing Chains of Command Use Different CPI Processes Flowchart Developed for CPI Identification


Critical Program Information Modifier Event
CPI Identification Process
• CPI Identified IAW DoDI 5200.39
• Tech & Prog Protect (T&PP) Guidebook
• Intel Support to AAF (ISTAFF) Guidebook
• DoD International Acq & Exportability Guidebook
• Follow OSD and Service CPI ID Process
CPI Identification Sources (T&PP Guidebook)
Security Classification Guides (SCGs)
DoD CPI Horizontal Protection Guidebook (HPG)
Subject Matter Expert (SME) Questions
CPI Identification Sources (Additional)
Technology Area Protection Plans (TAPPs)
Critical Programs and Technologies (CP&T) List
LO/CLO CPI
CPI List
Timeframe: TBD
Acquisition Security Database (ASDB)
CPI Identified?
YES
NO
Develop Counterintelligence Support Plan (CISP)
MDAP?
YES
NO
Request Technology Targeting Risk Assessment (TTRA)
Technology Targeting Risk Assessment (TTRA)
Will CPI Reside on the End Item?
NO
YES
Does the component contain: Software Algorithms or Microelectronics hardware?
NO
YES
Determine appropriate protection mechanisms
Determine appropriate protection mechanisms
Export Request?
NO
YES
Evaluate likelihood of future export & design accordingly
DoD TSFD Review
State Department: ITAR Review Staffing
Commerce Department: EAR Review Staffing
DTSA Review
Provisos?
YES
NO
National Disclosure Policy (NDP-1) Review
YES
Collateral Information?
Exceed DoDM S-5230.28 Threshold?
NO
YES
SAP Information?
YES
Decision Memo
DepSecDef Approval
LO/CLO Tri-Service Committee
LO/CLO CPI
LO/CLO Tri-Service Committee
LO/CLO EXCOM
Technology Transfer and Exportability
AT Process
Exposure Level/Program Execution Approach (AT Level)
Consequence of Compromise (CofC)
Attack/Countermeasure Analysis &
Acceptable Residual Vulnerabilities
LO/CLO TSC
Adherence to Provisos
Ensure Horizontal Protection
AT Architecture
(Implementation/Integration)
AT Evaluation/Verification
(Sufficiently Protected CPI)
AT Tech Implementation Guide
AT Plan and Concurrence
Timeframe:
Concept: 105 Days Prior MS A
Initial: 60 Days Prior to PDR
Final: 60 Days Prior to CDR
AT Verification Plan
Timeframe:
60 Days after CDR
AT Verification Report
Timeframe:
60 Days prior to MS C
or
60 days prior to System Export
AT Plan (PPP Appendix)
Is Product Baseline Finalized?
NO
YES
Reevaluate at next CPI Modifier Event
PPP or Equivalent Document
Is CPI Adequately Protected?
YES
NO
System Delivery
PPP or Equivalent Document
Identify Risk deficiencies & remediate
LEGEND
Database
Process
Document (Input or Output)
Start/End
External Data
Decision
Start/End Parallel Process

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Challenge 2: Differing Chains of Command Use Different CPI Processes
Developed Flowchart for CPI Identification

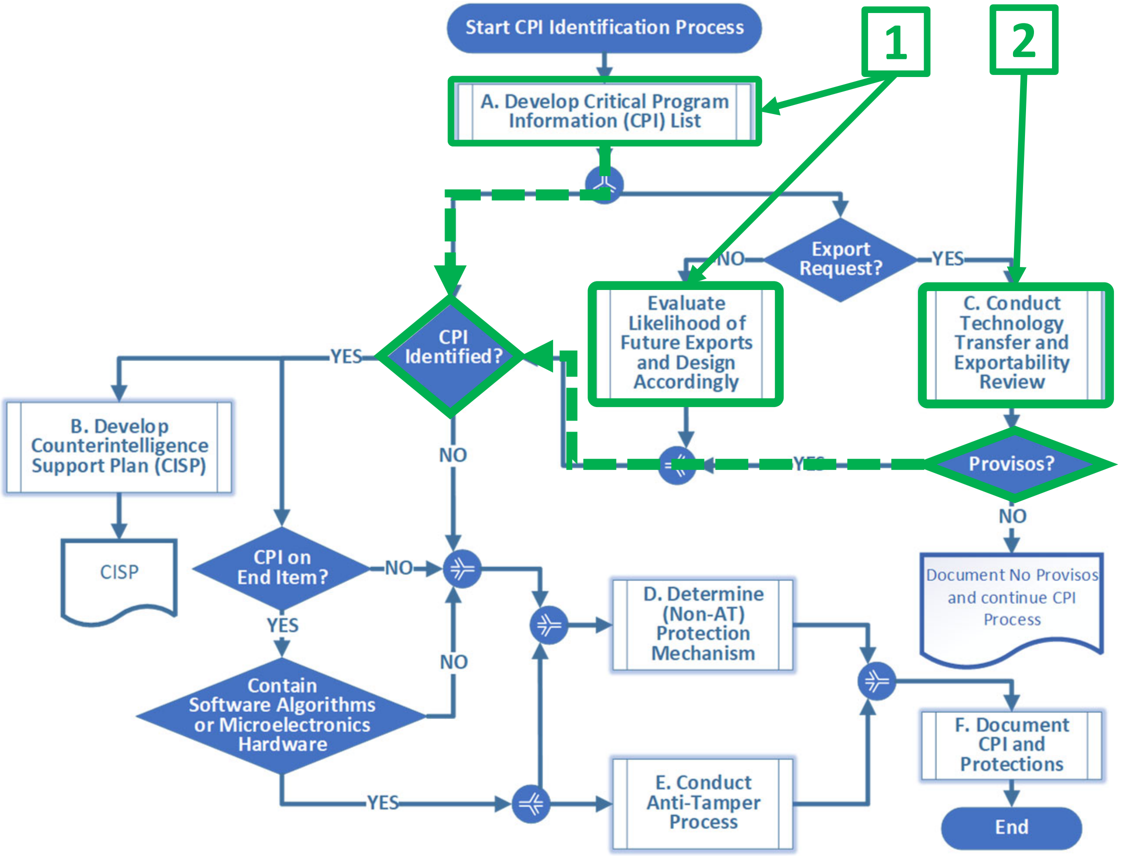


Horizontal Protection Guidance (HPG)
Expert Questions
LO/CLO & Export Guidance
Acquisition Security Database (ASDB)
Intelligence and Counterintelligence Analyses
Anti-Tamper Technical Implementation Guide
CPI Identification
Organic
Inherited
CPI Protection Measures Selection (Consequence of Compromise)
Anti-Tamper Protections
Other Program Protection Measusres
Modifiers
Design (Maturity, Modification)
Operational Environment (Export Status)
Protection Obsolescence and Effectiveness
CPI Compromise
Change in Threats
Security Classification
Commercial Technology Evolution
Update Program/Anti-Tamper Protection Plan
CPI/AT Monitoring
CPI Designation Removal
Critical Program Information Identification
CPI Identification Sources (T&PP Guidebook)
Security Classification Guides (SCGs)
DoD CPI Horizontal Protection Guidebook (HPG)
Subject Matter Expert (SME) Questions
CPI Identification Sources (Additional)
Technology Area Protection Plans (TAPPs)
Critical Programs and Technologies (CP&T) List
CPI Identification Process
CPI Identified IAW DoDI 5200.39
Tech & Prog Protect (T&PP) Guidebook
Intel Support to AAF (ISTAFF) Guidebook
DoD International Acq & Exportability Guidebook
Follow OSD and Service CPI ID Process
LO/CLO CPI
Export Request?
NO
YES
Evaluate likelihood of future export & design accordingly
CPI List
CPI Identified?
Will CPI Reside on the End Item?
Determine appropriate protection mechanisms
DoD TSFD Review
National Disclosure Policy (NDP-1) Review
DTSA Review
Provisos?
LO/CLO Tri-Service Committee
LO/CLO EXCOM
Technology Transfer and Exportability
Is Product Baseline Finalized?
System Delivery
PPP or Equivalent Document
Identify Risk deficiencies & remediate
AT Process
AT Architecture
AT Plan and Concurrence
AT Verification Report
AT Plan (PPP Appendix)
LO/CLO TSC
LEGEND
Database
Process
Document (Input or Output)
Start/End
External Data
Decision
Start/End Parallel Process
Identification
Horizontal Protection
Export
Technology Transfer
CI Support
Protections
Other Countermeasures
Anti-Tamper
Documentation

NDIA S&ME Conference
Oct 16-19, 2023

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

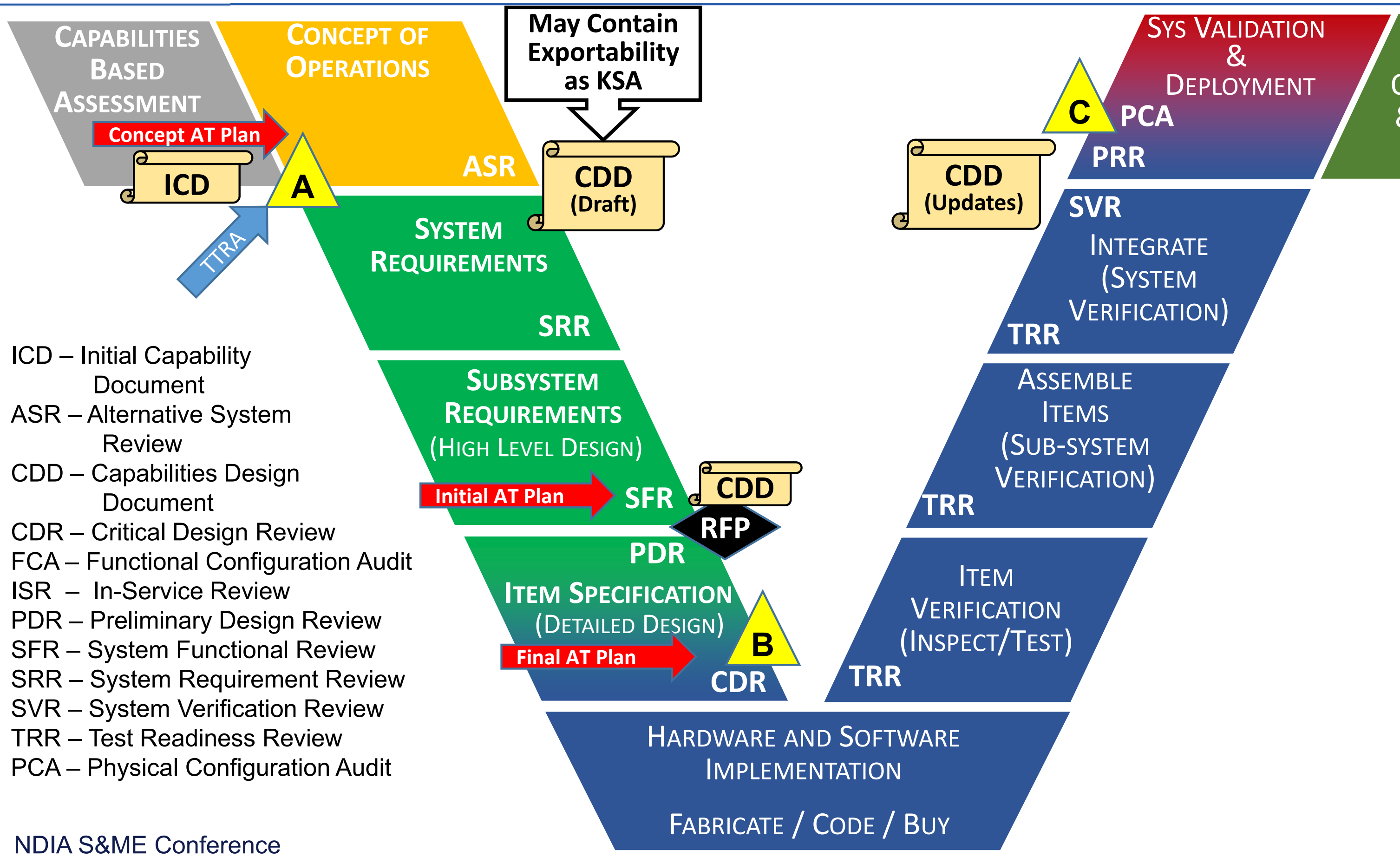
Flowchart for Critical Program Information (CPI) Identification
What needs to be protected?


Start CPI Identification Process
1
2
A. Develop Critical Program Information (CPI) List
Export Request?
NO
YES
Evaluate Likelihood of Future Exports and Design Accordingly
C. Conduct Technology Transfer and Exportability Review
CPI Identified?
YES
NO
B. Develop Counterintelligence Support Plan (CISP)
YES
Provisos?
NO
CISP
CPI on End Item?
NO
Document No Provisos and continue CPI Process
YES
NO
D. Determine (Non-AT) Protection Mechanism
Contain Software Algorithms or Microelectronics Hardware
F. Document CPI and Protections
YES
E. Conduct Anti-Tamper Process
End

- CPI is identified in twice within the diagram but is summed at a single point in the overall process:
  1. **Program's CPI Review during development**
     - All Programs are expected to review system for CPI.
     - May include an exportability Threshold or Objective requirement based on the Capabilities Development Document (CDD) Key system attribute (KSA) requirement.
  2. **(After Letter of Request) Proviso from:**
     - A. Technology Security and Foreign Disclosure (TSFD) Process,
       - ❑ DoDD 5230.28 - Low Observable (LO) and Counter LO (LO/CLO) International Transfer Guidance review.
     - B. Department of State (DoS), or
     - C. Department of Commerce (DoC) Reviews
- Any of these reviews can produce:
  - o Materials
  - o Processes
  - o Capabilities
  - o Information

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

2. What Needs to be Protected (and When)



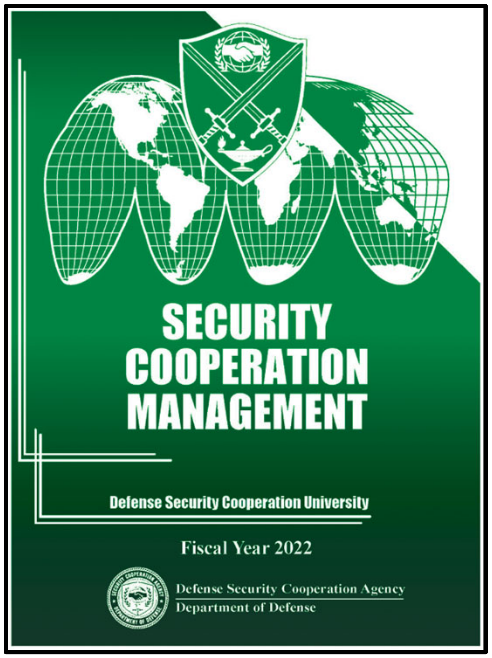
Capabilities Based Assessment
Concept AT Plan
ICD
TTRA
A
Concept of Operations
ASR
May Contain Exportability as KSA
CDD (Draft)
System Requirements
SRR
Subsystem Requirements (High Level Design)
Initial AT Plan
SFR
CDD
RFP
PDR
Item Specification (Detailed Design)
Final AT Plan
B
CDR
Hardware and Software Implementation
Fabricate / Code / Buy
Item Verification (Inspect/Test)
TRR
Assemble Items (Sub-system Verification)
TRR
Integrate (System Verification)
TRR
SVR
CDD (Updates)
PRR
PCA
C
Sys Validation & Deployment
System Operations & Support
Changes & Upgrades
Disposal

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

- Pre - MSA
- MSA - Materiel Solution Analysis
- TMRR - Technology Maturity & Risk Reduction
- EMD - Engineering and Manufacturing Development
- P&D - Production and Deployment
- O&S- Operations and Support

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Letter of Request
Security Cooperation Management (Greenbook)



SECURITY COOPERATION MANAGEMENT

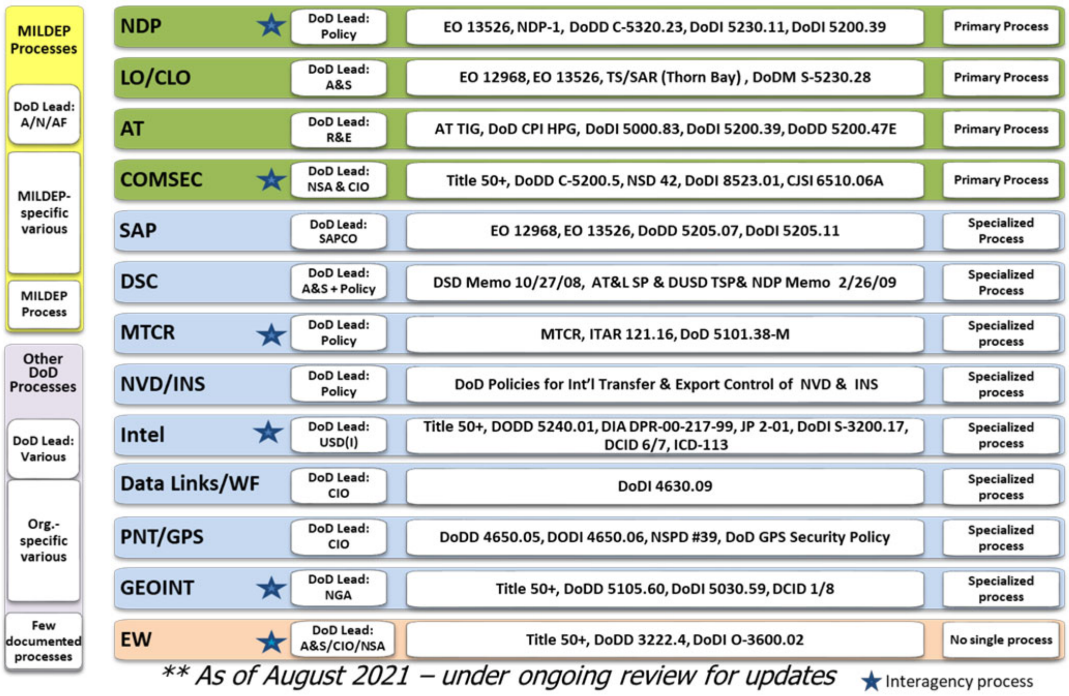
Defense Security Cooperation University

Fiscal Year 2022

Defense Security Cooperation Agency
Department of Defense

- When the Security Cooperation Organization (SCO) becomes aware of credible demand signals indicating the probable submission of :
  - Letter of Request (LoR) for Price and Availability (P&A),
  - Letter of Offer and Acceptance (LoA),
  - Commercial Request for Information (RFI) or
  - Request for Proposal (RFP) for sensitive or classified defense articles or services.
- The SCO should develop a Pre-LoR Assessment Request (PAR), as directed in Security Assistant Management Manual (SAMM) C3.1.2.
  - The intent of the PAR is to inform the interagency community and the cognizant implementing agency to initiate the **Technology Security and Foreign Disclosure (TSFD) process** for timely release of determinations.

Technology Security and Foreign Disclosure (TSFD) Processes



MILDEP Processes DoD Lead: A/N/AF MILDEP-specific various MILDEP Process	NDP	★	DoD Lead: Policy	EO 13526, NDP-1, DoDD C-5320.23, DoDI 5230.11, DoDI 5200.39	Primary Process
	LO/CLO		DoD Lead: A&S	EO 12968, EO 13526, TS/SAR (Thorn Bay) , DoDM S-5230.28	Primary Process
	AT		DoD Lead: R&E	AT TIG, DoD CPI HPG, DoDI 5000.83, DoDI 5200.39, DoDD 5200.47E	Primary Process
	COMSEC	★	DoD Lead: NSA & CIO	Title 50+, DoDD C-5200.5, NSD 42, DoDI 8523.01, CJSI 6510.06A	Primary Process
	SAP		DoD Lead: SAPCO	EO 12968, EO 13526, DoDD 5205.07, DoDI 5205.11	Specialized Process
	DSC		DoD Lead: A&S + Policy	DSD Memo 10/27/08, AT&L SP & DUSD TSP& NDP Memo 2/26/09	Specialized Process
	MTCR	★	DoD Lead: Policy	MTCR, ITAR 121.16, DoD 5101.38-M	Specialized process
Other DoD Processes DoD Lead: Various Org.-specific various	NVD/INS		DoD Lead: Policy	DoD Policies for Int'l Transfer & Export Control of NVD & INS	Specialized process
	Intel	★	DoD Lead: USD(I)	Title 50+, DODD 5240.01, DIA DPR-00-217-99, JP 2-01, DoDI S-3200.17, DCID 6/7, ICD-113	Specialized process
	Data Links/WF		DoD Lead: CIO	DoDI 4630.09	Specialized process
	PNT/GPS		DoD Lead: CIO	DoDD 4650.05, DODI 4650.06, NSPD #39, DoD GPS Security Policy	Specialized process
	GEOINT	★	DoD Lead: NGA	Title 50+, DoDD 5105.60, DoDI 5030.59, DCID 1/8	Specialized process
Few documented processes	EW	★	DoD Lead: A&S/CIO/NSA	Title 50+, DoDD 3222.4, DoDI O-3600.02	No single process

*** As of August 2021 – under ongoing review for updates*

★ Interagency process

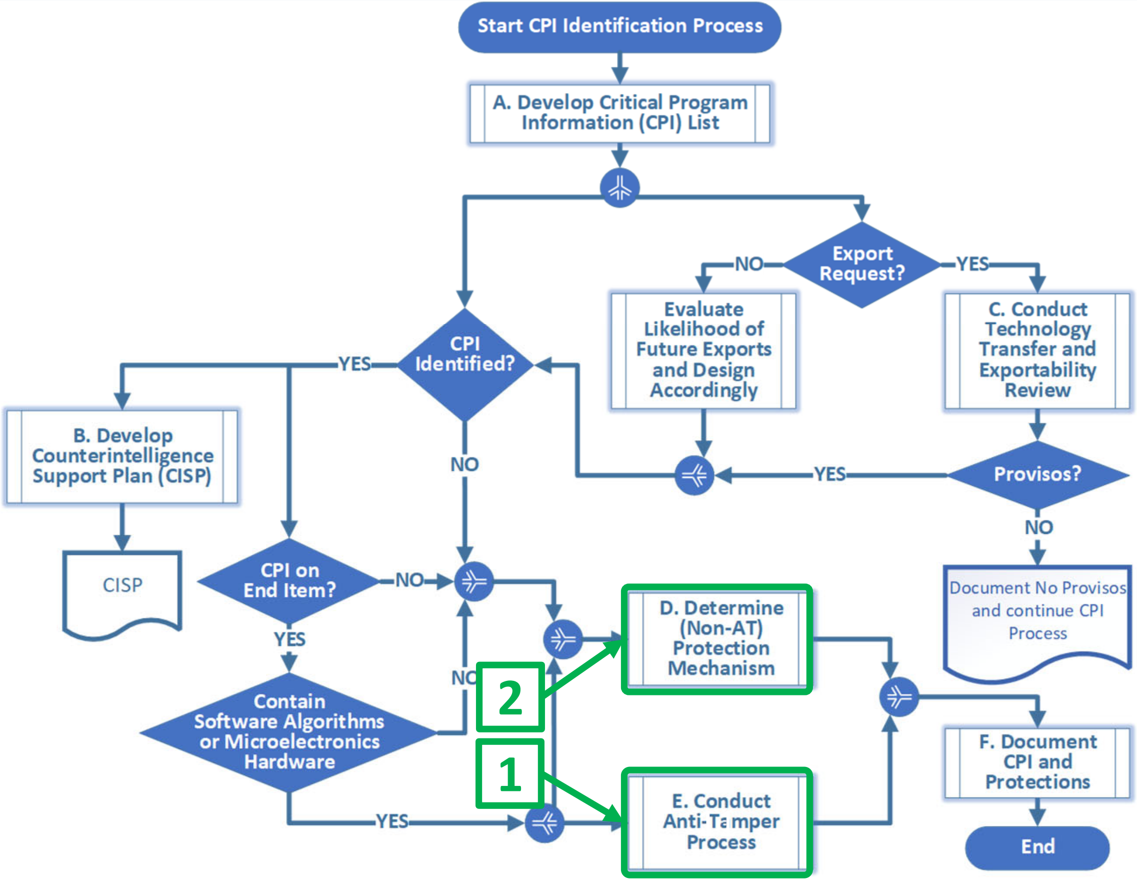
- NDP – National Disclosure Policy
- LO/CLO – Low Observable/ Counter Low Observable
- AT – Anti-Tamper
- COMSEC – Communications Security
- SAP – Special Access Program
- DSC – Defensive Systems Committee
- MTCR – Missile Technology Control Regime
- NVD – Night Vision Devices
- Intel – Intelligence
- Data Links & WF – Waveforms
- PNT/GPS – Geospatial Intelligence
- EW – Electronic Warfare

NOTES:
"Primary Process" refers to the processes for which there is documentation and multiple participants.

"Specialized Process" refers to the processes for which there is little or no documentation and a limited number of organizational participants

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Flowchart for Critical Program Information (CPI) Identification: 3. Level of Protection


Start CPI Identification Process
A. Develop Critical Program Information (CPI) List
Export Request?
NO
YES
Evaluate Likelihood of Future Exports and Design Accordingly
C. Conduct Technology Transfer and Exportability Review
CPI Identified?
YES
NO
B. Develop Counterintelligence Support Plan (CISP)
YES
Provisos?
NO
CISP
CPI on End Item?
NO
Document No Provisos and continue CPI Process
YES
D. Determine (Non-AT) Protection Mechanism
2
NO
Contain Software Algorithms or Microelectronics Hardware
1
F. Document CPI and Protections
YES
E. Conduct Anti-Tamper Process
End

- CPI “Level of Protection” is being determined at 2 points in the process with a 3rd point for horizontal discrepancies:

  1. End-Item (Anti-Tamper eligible systems)
     - Anti-Tamper uses the “Consequence-of-Compromise” criteria to assign variable protection levels to identified CPI.

       CofC: (DoD Instruction 5200.39) - The impact, if the CPI is compromised, on

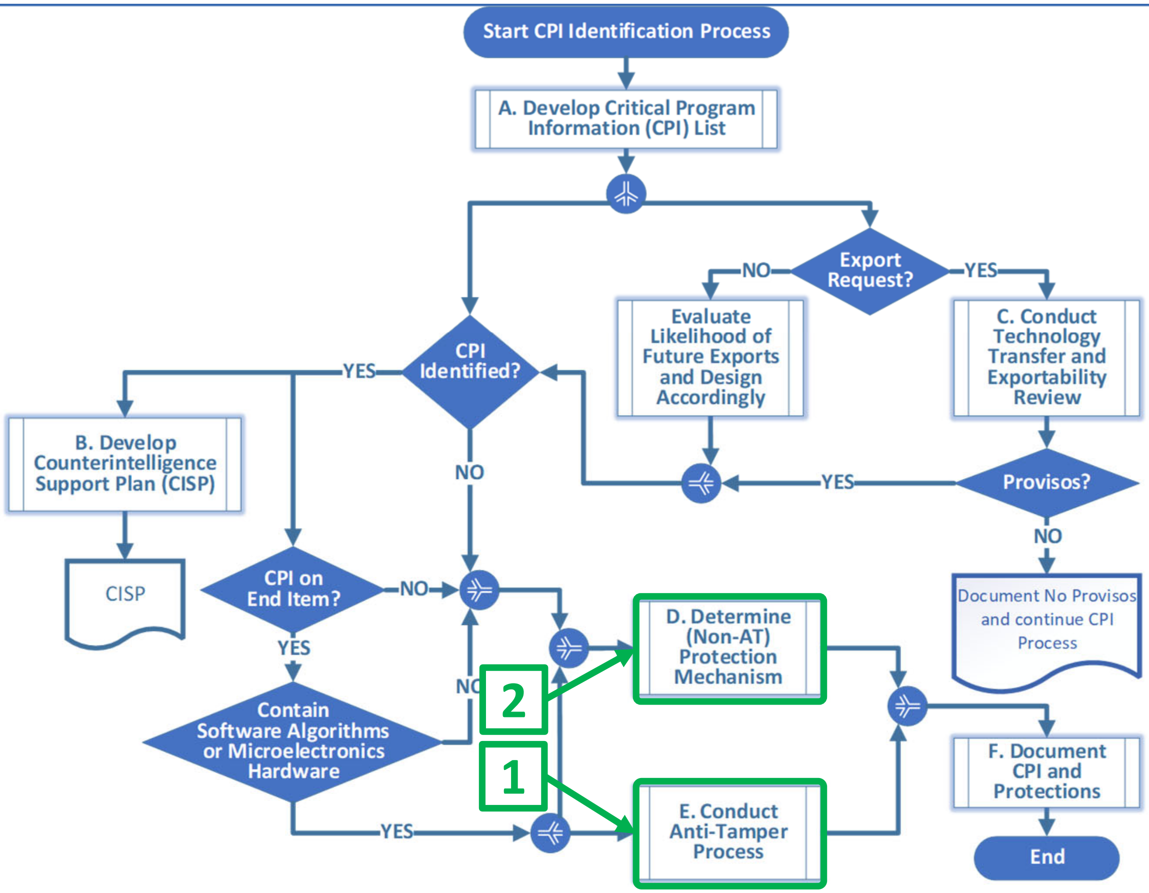
       - U.S. tactical or strategic military advantage, and
       - time and resources required for the U.S. to re-gain that tactical or strategic military advantage.

       NOTE: Items identified as CPI, and on the end-item, are eligible for both AT and other protection methods.

  2. Other protection measures
     - How are additional protections determined for Research Development Test & Evaluation (RDT&E) protections?

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Flowchart for Critical Program Information (CPI) Identification: 4. How will the capability be Protected?


Start CPI Identification Process
A. Develop Critical Program Information (CPI) List
Export Request?
NO
YES
Evaluate Likelihood of Future Exports and Design Accordingly
C. Conduct Technology Transfer and Exportability Review
CPI Identified?
YES
NO
B. Develop Counterintelligence Support Plan (CISP)
YES
Provisos?
NO
CISP
CPI on End Item?
NO
YES
Document No Provisos and continue CPI Process
D. Determine (Non-AT) Protection Mechanism
NO
2
Contain Software Algorithms or Microelectronics Hardware
1
F. Document CPI and Protections
YES
E. Conduct Anti-Tamper Process
End

- CPI Protections available will depend on system parameters.

1. **Anti-Tamper**
   - Will the technology/capability be on the "end-item" and potentially outside of US control?
   - Does the end-item contain software algorithms or microelectronics hardware that will benefit from Anti-Tamper efforts?
     - Systems engineering activities intended to prevent or delay exploitation of CPI in U.S. defense systems in domestic and export configurations to:

       A. impede countermeasure development,

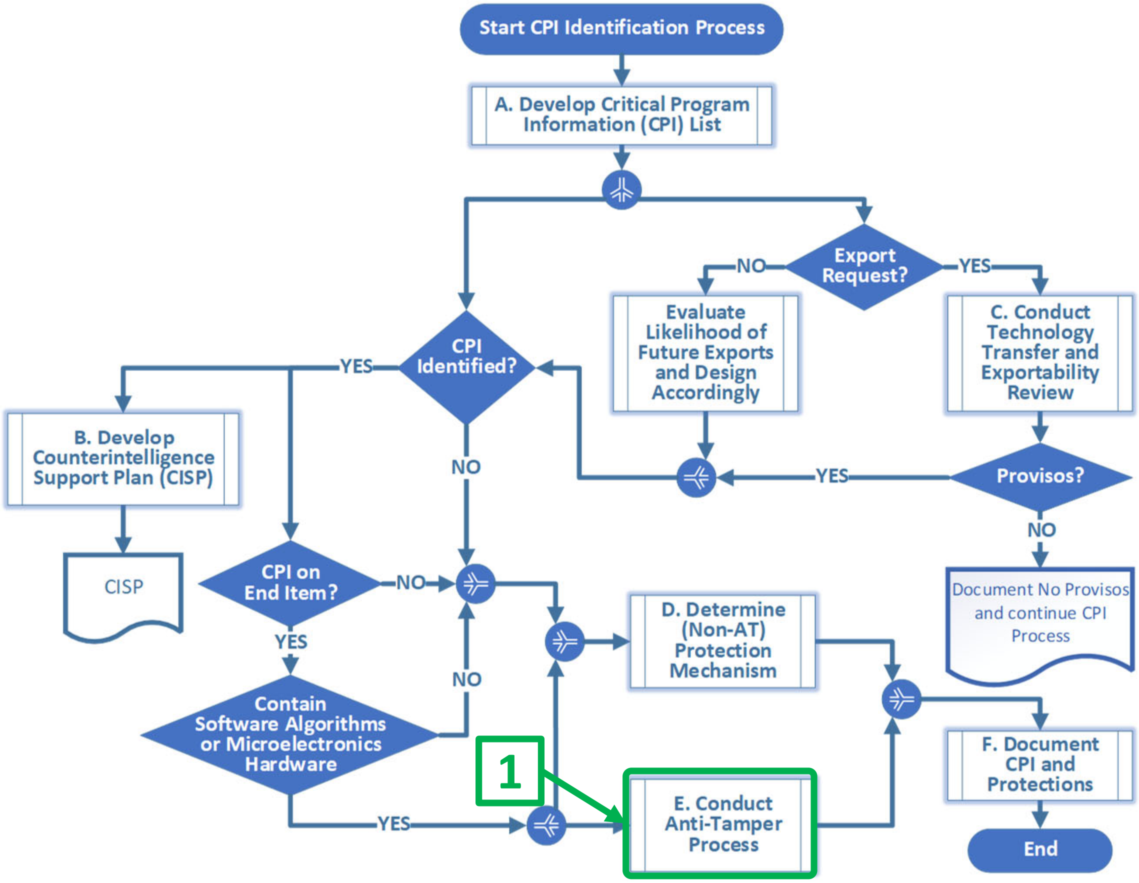
       B. unintended technology transfer, or alteration of a system due to reverse engineering.

       C. Prevention of "hands-on" countermeasure development.

2. **Other Protection Mechanisms**
   - Determined by other communities in the DoD

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Flowchart for Critical Program Information (CPI) Identification: 5. Have appropriate protections been achieved?



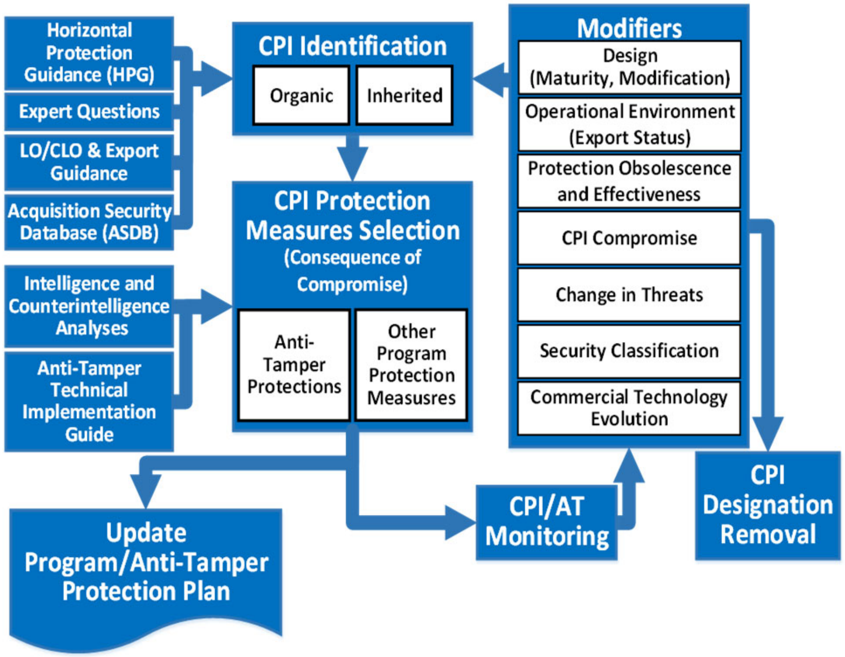
Start CPI Identification Process
A. Develop Critical Program Information (CPI) List
Export Request?
NO
YES
Evaluate Likelihood of Future Exports and Design Accordingly
C. Conduct Technology Transfer and Exportability Review
CPI Identified?
YES
NO
B. Develop Counterintelligence Support Plan (CISP)
Provisos?
YES
NO
CISP
CPI on End Item?
NO
YES
Document No Provisos and continue CPI Process
D. Determine (Non-AT) Protection Mechanism
Contain Software Algorithms or Microelectronics Hardware
NO
YES
1
E. Conduct Anti-Tamper Process
F. Document CPI and Protections
End

- Once protections are determined and instantiated in the system there is a final check to determine effectiveness and residual risk of the final system.

1. The Anti-Tamper Program was developed to include an expert review of the final instantiated design.
    - This report and a summary memo is provided to the program to support risk acceptance.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Technology and Program Protection (T&PP) Guidebook – Critical Program Information (CPI)



Horizontal Protection Guidance (HPG)

Expert Questions

LO/CLO & Export Guidance

Acquisition Security Database (ASDB)

Intelligence and Counterintelligence Analyses

Anti-Tamper Technical Implementation Guide

CPI Identification

Organic

Inherited

CPI Protection Measures Selection (Consequence of Compromise)

Anti-Tamper Protections

Other Program Protection Measusres

Modifiers

Design (Maturity, Modification)

Operational Environment (Export Status)

Protection Obsolescence and Effectiveness

CPI Compromise

Change in Threats

Security Classification

Commercial Technology Evolution

Update Program/Anti-Tamper Protection Plan

CPI/AT Monitoring

CPI Designation Removal

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

- **To identify CPI, S&T managers and engineers should consider the following activities:**
  - Use DoD, DoD Component, and program resources 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.

- Update will include removal/revalidation section

Note that CPI is not:

- Personally Identifiable or Protected Health Information (PII/ PHI)
- Financial/ Logistic information
- Operational information (waypoints and target location data)
- Designs, System performance, vulnerabilities, or weaknesses
- Manufacturing details (update will include processes)
- Unmodified commercial-off-the-shelf (COTS) technology
- Multi-Level Security, Cross Domain, or Cryptographic Solutions