Identification and Protection of Critical Program Information (CPI)

Raymond Shanahan

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

18th Annual NDIA Systems Engineering Conference

Springfield, VA | October 27, 2015

DASD, Systems Engineering Mission

Systems Engineering focuses on engineering excellence − the creative application of scientific principles:

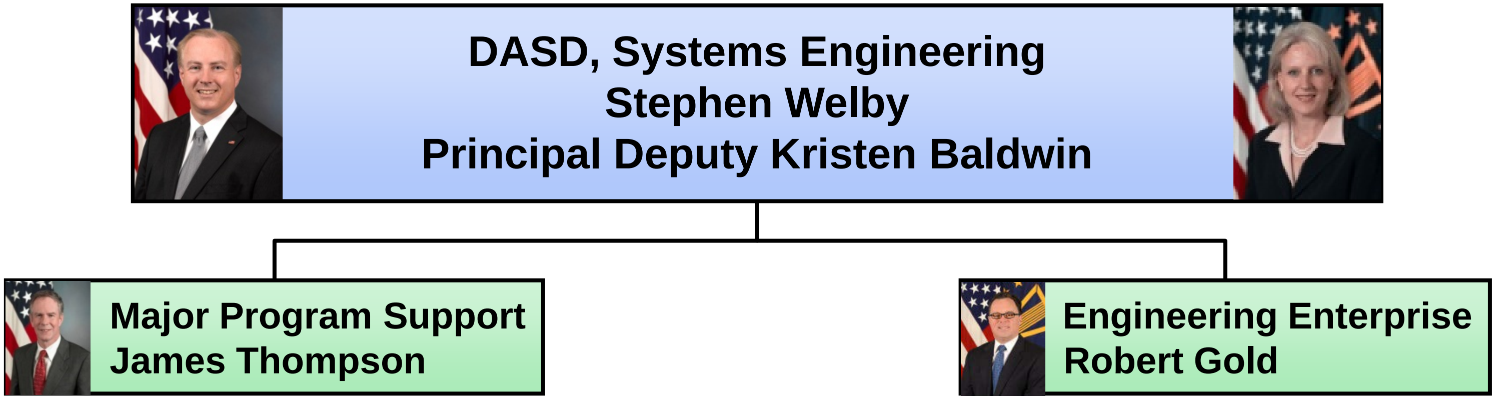
- To design, develop, construct and operate complex systems
- To forecast their behavior under specific operating conditions
- To deliver their intended function while addressing economic efficiency, environmental stewardship and safety of life and property

DASD(SE) Mission: Develop and grow the Systems Engineering capability of the Department of Defense – through engineering policy, continuous engagement with component Systems Engineering organizations and through substantive technical engagement throughout the acquisition life cycle with major and selected acquisition programs.

A Robust Systems Engineering Capability Across the Department Requires Attention to Policy, People and Practice

- ***US Department of Defense is the World's Largest Engineering Organization***
- ***Over 108,000 Uniformed and Civilian Engineers***
- ***Over 39,000 in the Engineering (ENG) Acquisition Workforce***

DASD, Systems Engineering



DASD, Systems Engineering
Stephen Welby
Principal Deputy Kristen Baldwin

Major Program Support
James Thompson

Engineering Enterprise
Robert Gold

Supporting USD(AT&L) Decisions with Independent Engineering Expertise

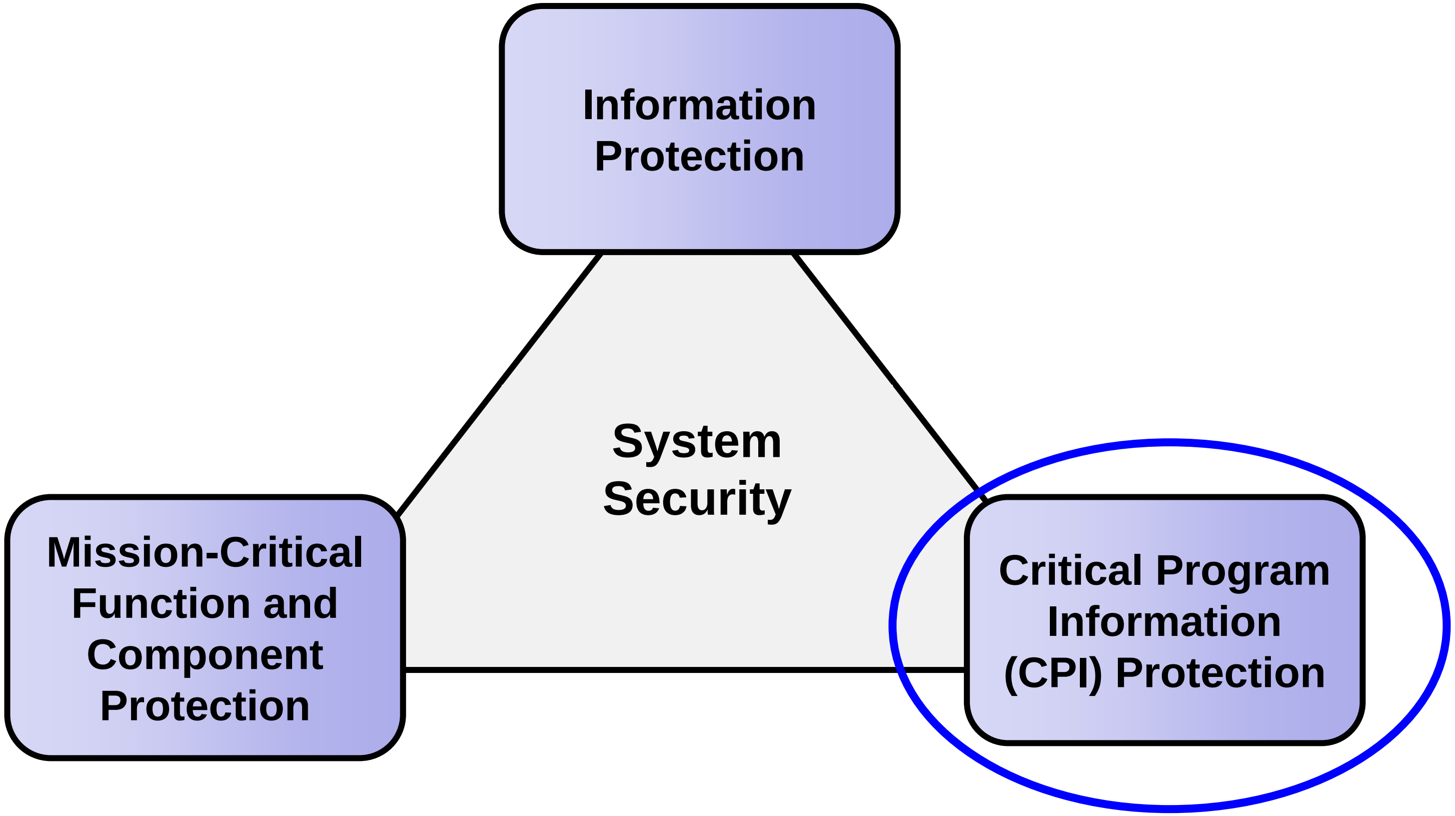
- **Engineering Assessment / Mentoring of Major Defense Programs**
- **Program Support Assessments**
- **Overarching Integrated Product Team and Defense Acquisition Board Support**
- **Systems Engineering Plans**
- **Systemic Root Cause Analysis**
- **Development Planning/Early SE**
- **Program Protection**

Leading Systems Engineering Practice in DoD and Industry

- **Systems Engineering Policy and Guidance**
- **Technical Workforce Development**
- **Specialty Engineering (System Safety, Reliability and Maintainability, Quality, Manufacturing, Producibility, Human Systems Integration)**
- **Security, Anti-Tamper, Counterfeit Prevention**
- **Standardization**
- **Engineering Tools and Environments**

Providing technical support and systems engineering leadership and oversight to USD(AT&L) in support of planned and ongoing acquisition programs

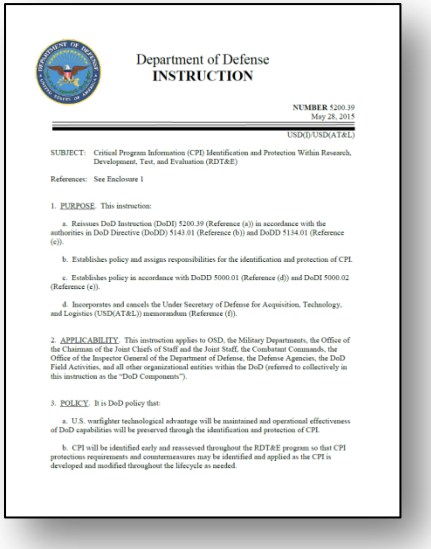
Program Protection Elements


Information Protection
System Security
Mission-Critical Function and Component Protection
Critical Program Information (CPI) Protection

Today's focus is on CPI identification and protection

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0133 applies. Distribution is unlimited.

Recent Updates to CPI and AT Policy



Department of Defense
INSTRUCTION

NUMBER 5200.39
May 28, 2015

USD(I)/USD(AT&L)

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)).

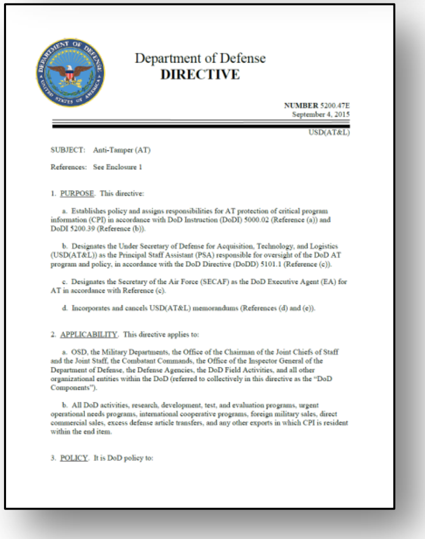
d. Incorporates and cancels the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) memorandum (Reference (f)).

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.

b. CPI will be identified early and reassessed throughout the RDT&E program so that CPI protections requirements and countermeasures may be identified and applied as the CPI is developed and modified throughout the lifecycle as needed.



Department of Defense
DIRECTIVE

NUMBER 5200.47E
September 4, 2015

USD(AT&L)

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").

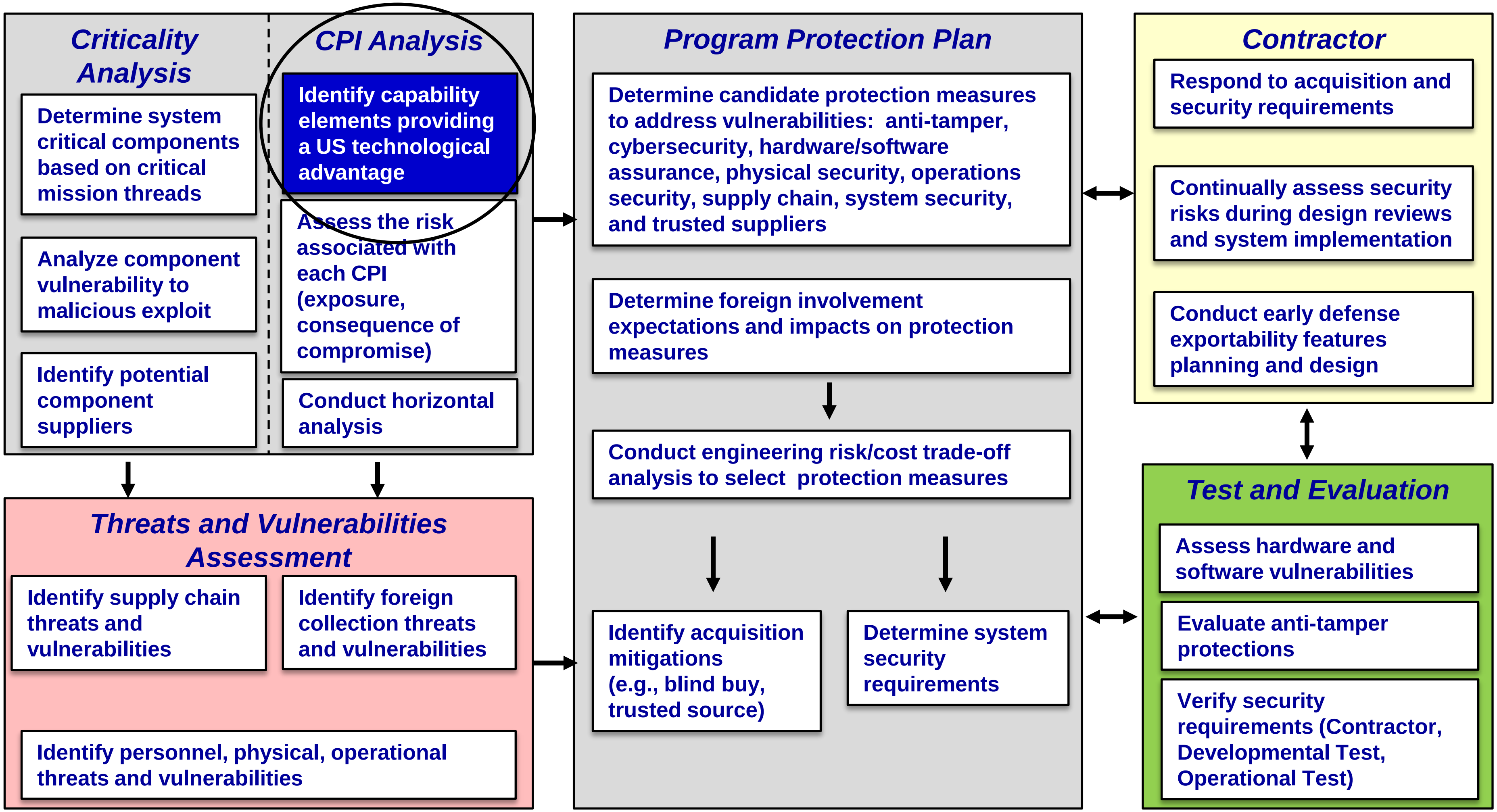
b. All DoD activities, research, development, test, and evaluation programs, urgent operational needs programs, international cooperative programs, foreign military sales, direct commercial sales, excess defense article transfers, and any other exports in which CPI is resident within the end item.

3. POLICY. It is DoD policy to:

- **DoD Instruction (DoDI) 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015**
  - – Focuses the definition of CPI on capability elements that provide a technological advantage
  - – Requires that CPI be identified early and reassessed throughout the program
  - – Emphasizes horizontal identification and protection
  - – Aligns with policies and responsibilities of DoDI 5000.02, DoDD 5200.47E, and DoDI 5200.44
- **DoD Directive (DoDD) 5200.47E, "Anti-Tamper," September 4, 2015**
  - – Establishes AT program governance, specifically designates SAF as the DoD Executive Agent for AT and requires that DoD Component heads establish Offices of Primary Responsibility for AT
  - – Requires that DoD Component heads conduct AT planning, implementation, and evaluations in alignment with guidance from the DoD Executive Agent for AT

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0133 applies. Distribution is unlimited.

System Security Engineering (SSE) Methodology



Criticality Analysis

Determine system critical components based on critical mission threads

Analyze component vulnerability to malicious exploit

Identify potential component suppliers

CPI Analysis

Identify capability elements providing a US technological advantage

Assess the risk associated with each CPI (exposure, consequence of compromise)

Conduct horizontal analysis

Threats and Vulnerabilities Assessment

Identify supply chain threats and vulnerabilities

Identify foreign collection threats and vulnerabilities

Identify personnel, physical, operational threats and vulnerabilities

Program Protection Plan

Determine candidate protection measures to address vulnerabilities: anti-tamper, cybersecurity, hardware/software assurance, physical security, operations security, supply chain, system security, and trusted suppliers

Determine foreign involvement expectations and impacts on protection measures

Conduct engineering risk/cost trade-off analysis to select protection measures

Identify acquisition mitigations (e.g., blind buy, trusted source)

Determine system security requirements

Contractor

Respond to acquisition and security requirements

Continually assess security risks during design reviews and system implementation

Conduct early defense exportability features planning and design

Test and Evaluation

Assess hardware and software vulnerabilities

Evaluate anti-tamper protections

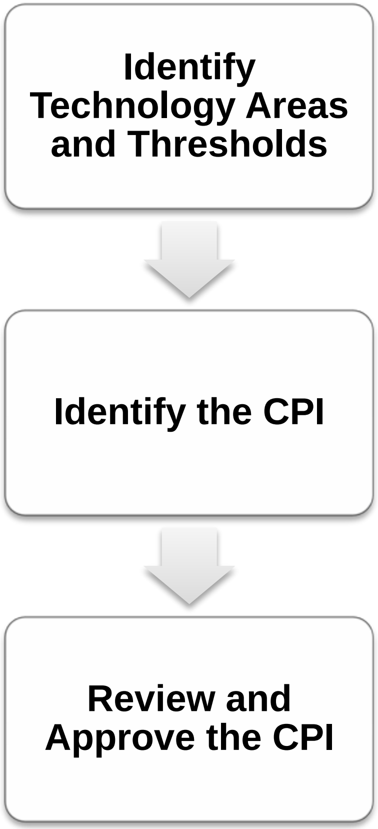
Verify security requirements (Contractor, Developmental Test, Operational Test)

CPI – Our Most Critical Capabilities

- **Per DoD Instruction 5200.39, CPI has been scoped to focus only on those elements that:**
  - Provide a capability advantage
  - Reside on the end-item (system or supporting systems)

- **Definition of CPI**
  - "U.S. capability elements that ***contribute 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, its training equipment, or maintenance support equipment."

Identifying CPI



Identify Technology Areas and Thresholds

Identify the CPI

Review and Approve the CPI

- What are the criteria/thresholds for determining if specific software or hardware on my system is CPI?
- What specific software or hardware on my system meets or exceeds these criteria/thresholds?
- Do the appropriate approval authorities agree with the CPI determination?

“CPI will be <u>identified early</u> and reassessed throughout the RDT&E program…” DoD Instruction 5200.39

CPI Identification Resources

- Government and contractor technologists / subject matter experts
- Open source intelligence analysis of the technology (literary reviews, on-line postings, technology conference topics/agenda, commercial databases)
- Security Classification Guides
- DoD Policy*
- DoD Component-specific CPI tools and decision aids
- Acquisition Security Database (ASDB)*
- Example list of CPI*

*Under development

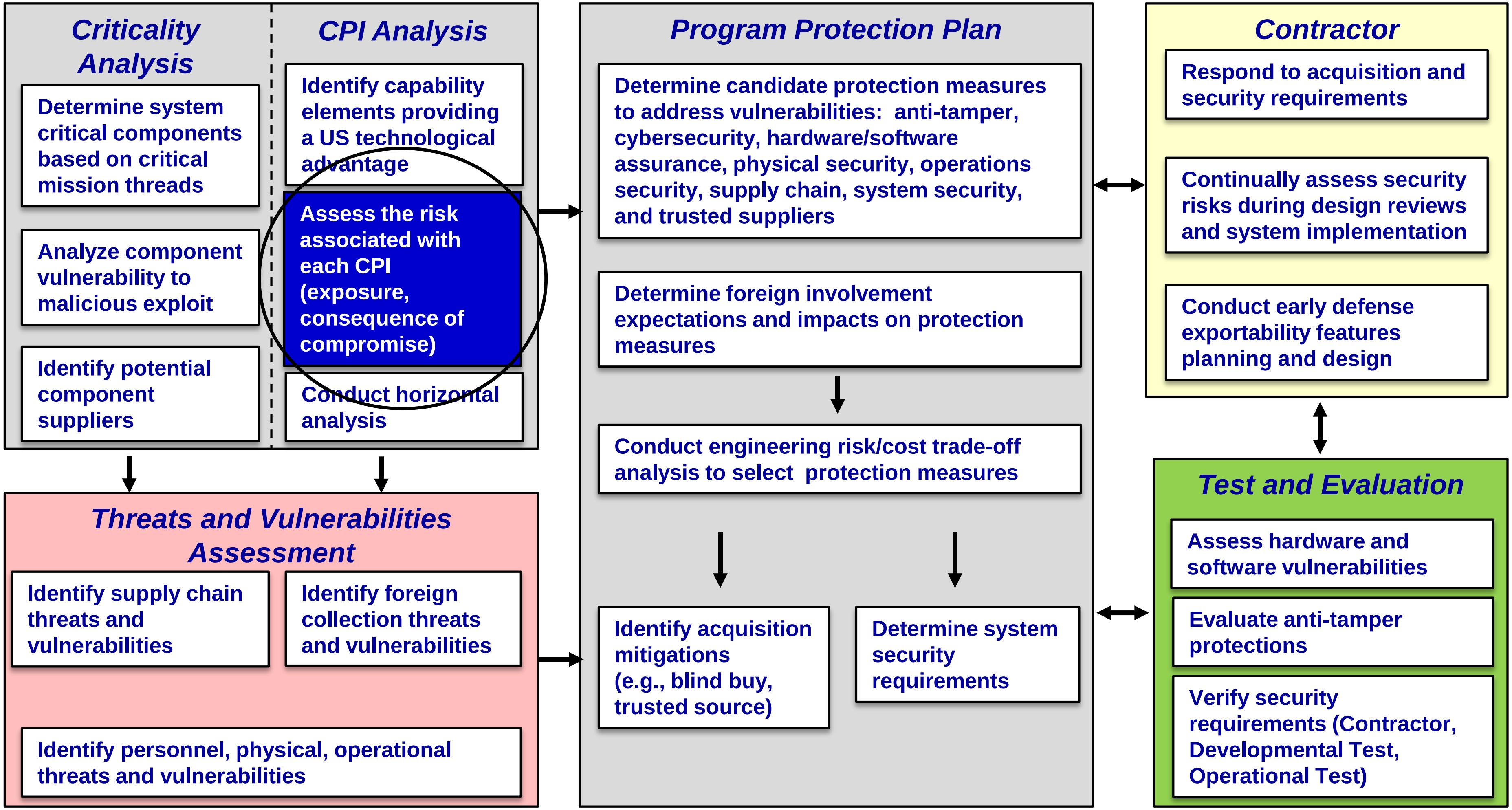
Monitoring CPI and CPI Protections

Event/Trigger	A change…	Potential Impact(s)
Operational Environment	In the physical location of the system with CPI other than that for which it was originally designed	Increased or decreased system exposure
Protection Effectiveness	In the ability of the CPI protections to deter, impede, detect, and/or respond to an attempt to exploit CPI	Compromised CPI Increased number of known residual vulnerabilities
Security Classification	To a relevant SCG, and thus the classification thresholds used for information that may reveal CPI	Information which revealed CPI may no longer be classified; conversely, information which may reveal CPI may now be classified
System Modification	To the system architecture and/or designs	CPI added, removed, or modified CPI protection measures modified
Technology Maturation	In the state-of-the-art for a particular CPI technology domain, and thus the thresholds used for CPI identification	Technologies previously identified as CPI may no longer qualify as CPI; Technologies not previously identified as CPI may qualify as CPI
Threat	In the adversary ability to obtain the CPI	Increased number of known residual vulnerabilities

“CPI will be identified early and reassessed throughout the RDT&E program…” DoD Instruction 5200.39

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0133 applies. Distribution is unlimited.

System Security Engineering (SSE) Methodology



Criticality Analysis

Determine system critical components based on critical mission threads

Analyze component vulnerability to malicious exploit

Identify potential component suppliers

CPI Analysis

Identify capability elements providing a US technological advantage

Assess the risk associated with each CPI (exposure, consequence of compromise)

Conduct horizontal analysis

Threats and Vulnerabilities Assessment

Identify supply chain threats and vulnerabilities

Identify foreign collection threats and vulnerabilities

Identify personnel, physical, operational threats and vulnerabilities

Program Protection Plan

Determine candidate protection measures to address vulnerabilities: anti-tamper, cybersecurity, hardware/software assurance, physical security, operations security, supply chain, system security, and trusted suppliers

Determine foreign involvement expectations and impacts on protection measures

Conduct engineering risk/cost trade-off analysis to select protection measures

Identify acquisition mitigations (e.g., blind buy, trusted source)

Determine system security requirements

Contractor

Respond to acquisition and security requirements

Continually assess security risks during design reviews and system implementation

Conduct early defense exportability features planning and design

Test and Evaluation

Assess hardware and software vulnerabilities

Evaluate anti-tamper protections

Verify security requirements (Contractor, Developmental Test, Operational Test)

Determining CPI Risk – Level of Protection Required

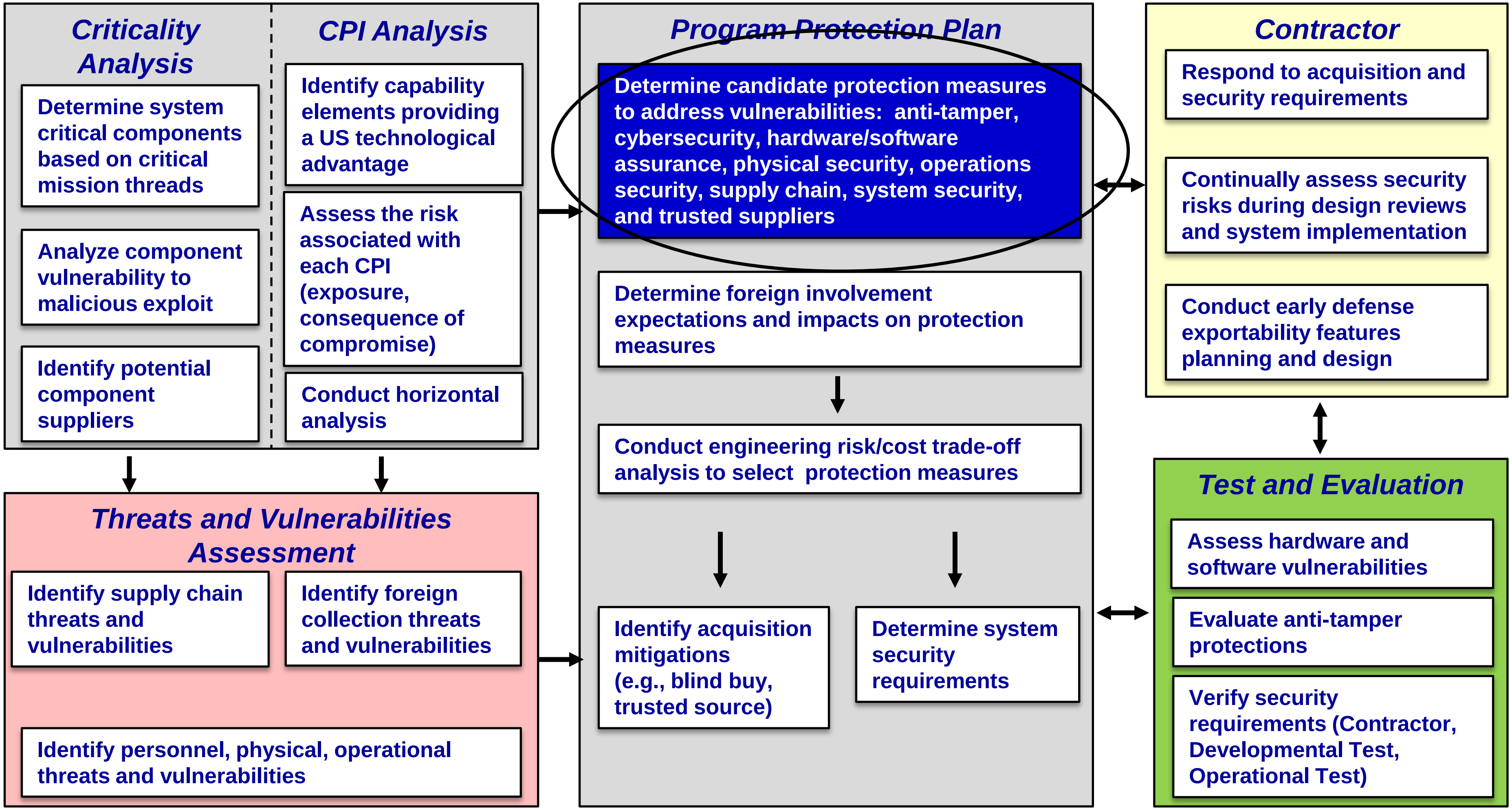
- **The level of protection is based on the risk associated with each CPI**
  - Risk = consequence of CPI compromise, system exposure, and assessed threat
- **Consequence of CPI Compromise***
  - The impact, if the CPI is compromised, on U.S. tactical or strategic military advantage, and the time and resources required for the U.S. to re-gain that tactical or strategic military advantage.
- **Exposure**
  - The likelihood that an adversary will be able to obtain the end-item: operational environment is a primary factor.
  - ***Per AT Guidelines v2.1, assume export level exposure.***
- **Threat**
  - An assessment of foreign adversary interest and skill in obtaining CPI.

***Enhancements underway by DoD Executive Agent for Anti-Tamper**

> **"CPI will be horizontally identified and protected…based on the exposure of the system, consequence of CPI compromise, and assessed threats."**
> **DoD Instruction 5200.39**

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0133 applies. Distribution is unlimited.

System Security Engineering (SSE) Methodology



Criticality Analysis

- Determine system critical components based on critical mission threads
- Analyze component vulnerability to malicious exploit
- Identify potential component suppliers

CPI Analysis

- Identify capability elements providing a US technological advantage
- Assess the risk associated with each CPI (exposure, consequence of compromise)
- Conduct horizontal analysis

Threats and Vulnerabilities Assessment

- Identify supply chain threats and vulnerabilities
- Identify foreign collection threats and vulnerabilities
- Identify personnel, physical, operational threats and vulnerabilities

Program Protection Plan

- Determine candidate protection measures to address vulnerabilities: anti-tamper, cybersecurity, hardware/software assurance, physical security, operations security, supply chain, system security, and trusted suppliers
- Determine foreign involvement expectations and impacts on protection measures
- Conduct engineering risk/cost trade-off analysis to select protection measures
- Identify acquisition mitigations (e.g., blind buy, trusted source)
- Determine system security requirements

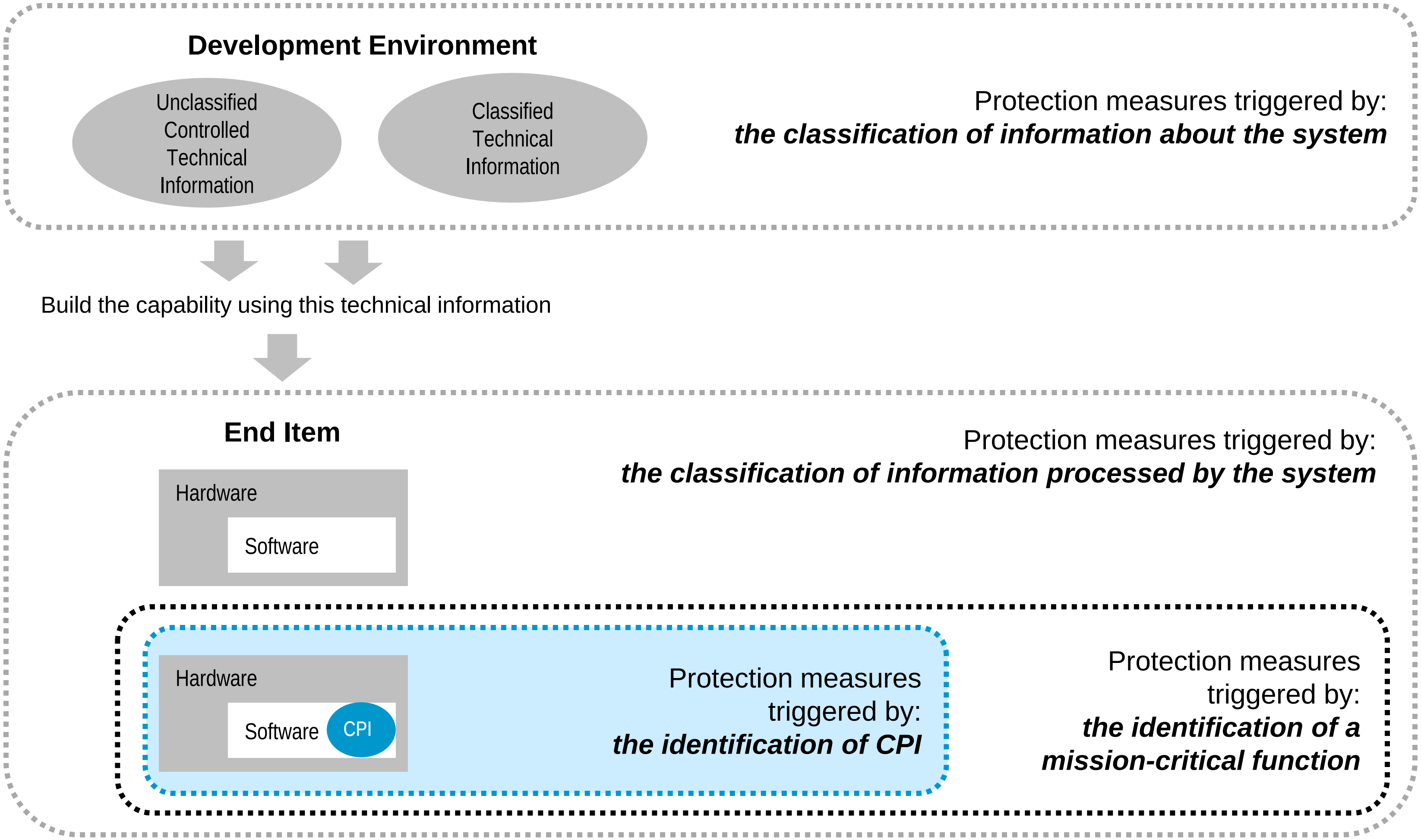
Contractor

- Respond to acquisition and security requirements
- Continually assess security risks during design reviews and system implementation
- Conduct early defense exportability features planning and design

Test and Evaluation

- Assess hardware and software vulnerabilities
- Evaluate anti-tamper protections
- Verify security requirements (Contractor, Developmental Test, Operational Test)

Protecting CPI - System Context



Development Environment

Unclassified Controlled Technical Information

Classified Technical Information

Protection measures triggered by:
the classification of information about the system

Build the capability using this technical information

End Item

Hardware

Software

Protection measures triggered by:
the classification of information processed by the system

Hardware

Software

CPI

Protection measures triggered by:
the identification of CPI

Protection measures triggered by:
the identification of a mission-critical function

*Note that there are also protection measures triggered by the identification of a mission-critical function that impact acquisition and testing processes

CPI-Specific Protections

- **Based on the assessed level of risk identify the appropriate CPI protections**

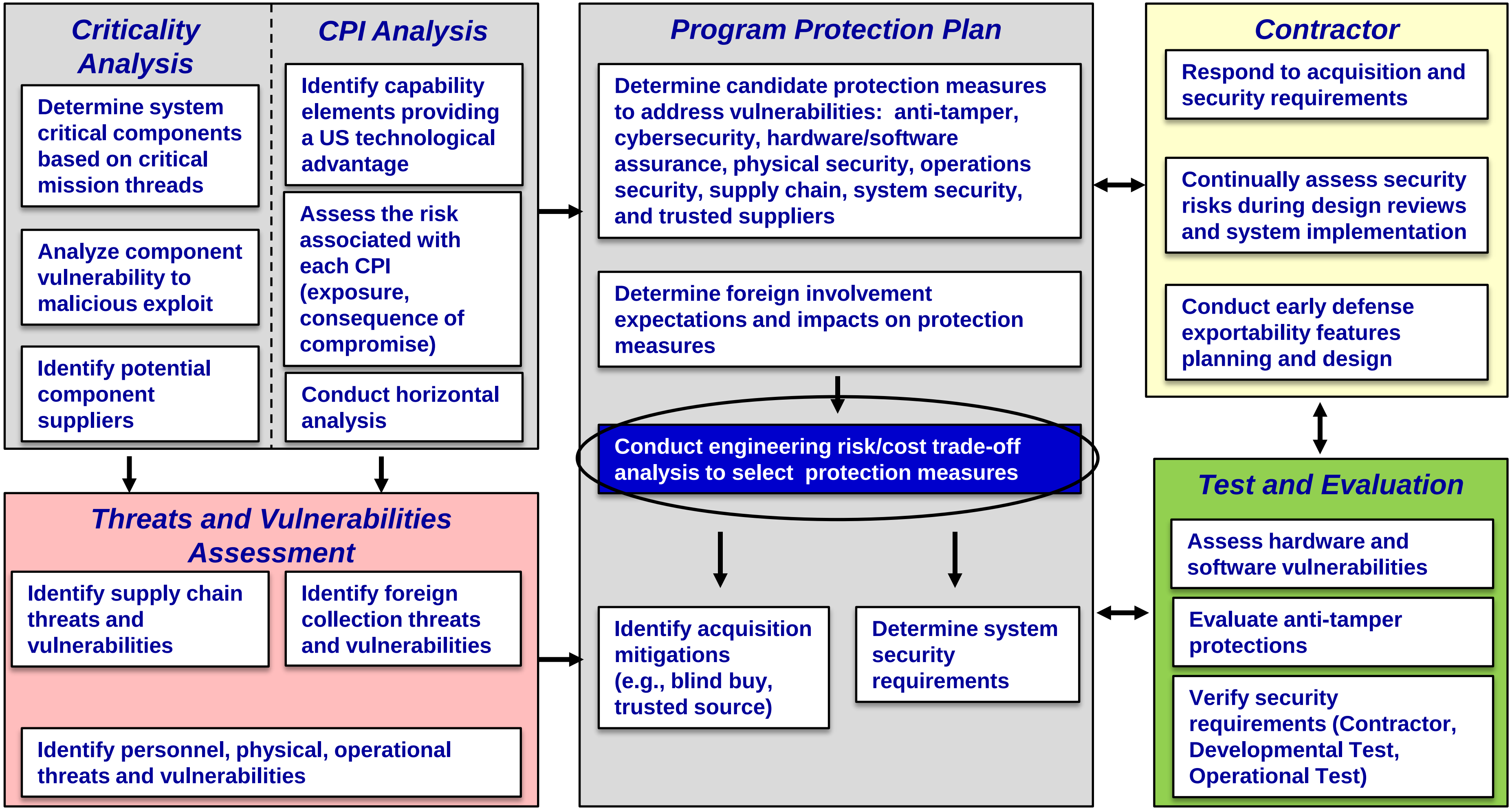
- **Anti-Tamper**
  - Systems engineering activities intended to prevent or delay exploitation of CPI in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering.

- **Differential Capability (subset of Exportability Features)**
  - Modifications to DoD systems which result in exportable versions. These modifications include incorporating capabilities that are unique to the foreign partner and removing capabilities that are for the U.S. only.

"Support the sale or transfer of certain defense articles to foreign governments and their participating contractors while preserving U.S. and foreign investments in CPI…" DoD Directive 5200.47E

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0133 applies. Distribution is unlimited.

System Security Engineering (SSE) Methodology



Criticality Analysis

- Determine system critical components based on critical mission threads
- Analyze component vulnerability to malicious exploit
- Identify potential component suppliers

CPI Analysis

- Identify capability elements providing a US technological advantage
- Assess the risk associated with each CPI (exposure, consequence of compromise)
- Conduct horizontal analysis

Threats and Vulnerabilities Assessment

- Identify supply chain threats and vulnerabilities
- Identify foreign collection threats and vulnerabilities
- Identify personnel, physical, operational threats and vulnerabilities

Program Protection Plan

- Determine candidate protection measures to address vulnerabilities: anti-tamper, cybersecurity, hardware/software assurance, physical security, operations security, supply chain, system security, and trusted suppliers
- Determine foreign involvement expectations and impacts on protection measures
- Conduct engineering risk/cost trade-off analysis to select protection measures
- Identify acquisition mitigations (e.g., blind buy, trusted source)
- Determine system security requirements

Contractor

- Respond to acquisition and security requirements
- Continually assess security risks during design reviews and system implementation
- Conduct early defense exportability features planning and design

Test and Evaluation

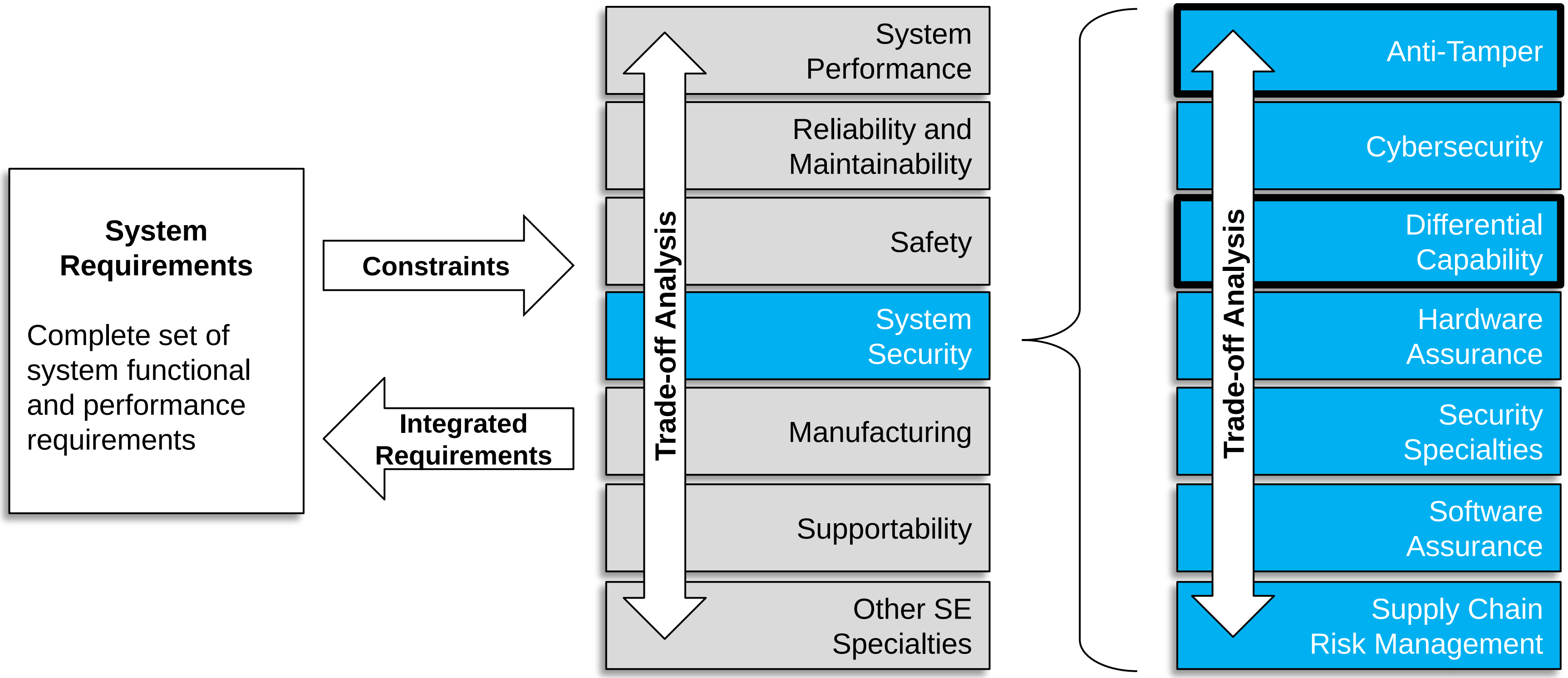
- Assess hardware and software vulnerabilities
- Evaluate anti-tamper protections
- Verify security requirements (Contractor, Developmental Test, Operational Test)

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0133 applies. Distribution is unlimited.

Protecting CPI -
SE and SSE Trade-off Analyses

Systems Engineering Specialties

System Security Engineering Specialties



System Requirements

Complete set of system functional and performance requirements

Constraints

Integrated Requirements

Trade-off Analysis

System Performance

Reliability and Maintainability

Safety

System Security

Manufacturing

Supportability

Other SE Specialties

Trade-off Analysis

Anti-Tamper

Cybersecurity

Differential Capability

Hardware Assurance

Security Specialties

Software Assurance

Supply Chain Risk Management

Areas for Continued Focus

- **Reduce the subjectivity inherent in the current CPI identification and protection process by:**
  - Developing procedures that define a DoD standard set of activities to identify and protect CPI
  - Enhancing the ASDB to better support horizontal identification and protection
  - Developing an Example List of CPI that provides a list of capabilities that are typical CPI by system type
  - Enhancing Anti-Tamper guidance, specifically criteria associated with consequence of CPI compromise determinations
- **Mature and integrate system security engineering practices, to include CPI identification and protection, into systems engineering practices**

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0133 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition

Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Raymond Shanahan

ODASD, Systems Engineering

571.372.6558

raymond.c.shanahan.civ@mail.mil

Matthew Perticone

Engility Corporation

571.372.6555

matthew.perticone.ctr@mail.mil

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0133 applies. Distribution is unlimited.