# Implementing Program Protection and Cybersecurity


**Melinda Reed**
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

**Mark Godino**
Office of the Deputy Assistant Secretary of Defense for C3, Cyber, & Business Systems

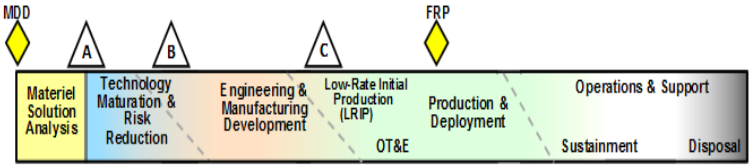

**Precision Strike Annual Review (PSAR-15)**

**Springfield, VA | March 17, 2015**

# Malicious Supply Chain Risk

- ***Threat:***
  - Nation-state, terrorist, criminal, or rogue developer who gains control of ***systems or information*** through supply chain opportunities; exploits vulnerabilities remotely, and/or degrades system behavior
- ***Vulnerabilities:***
  - All systems, networks, and applications
  - Intentionally implanted logic (HW/SW)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
  - Controlled unclassified information resident on, or transiting supply chain networks
- ***Consequences:***
  - Loss of data; system corruption
  - Loss of confidence in critical warfighting capability; mission impact

***Access points are throughout the acquisition lifecycle…***




***…and across numerous supply chain entry points***

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

# Many System Security Risks to Consider

## Quality Escape

Product defect/inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance

## Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

## Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

## Malicious Insertion

The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data

## Anti-Tamper

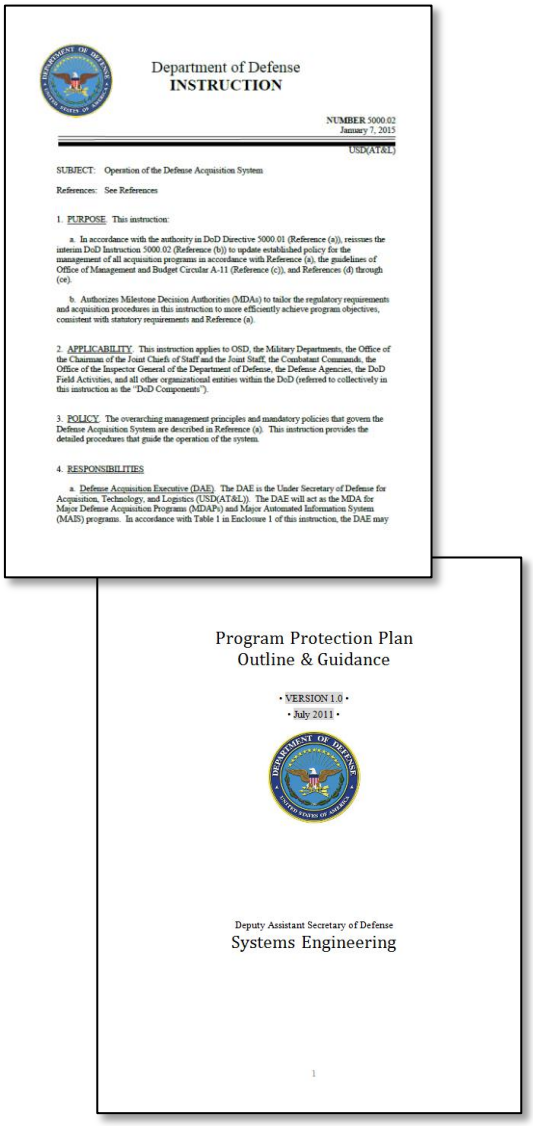
Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

## Information Losses

Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

***Systems Security Engineering is a critical discipline of SE, addressing a spectrum of security risks that are magnified by complex system attributes***

# DoDI 5000.02 and PPP Outline & Guidance


Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive 5000.01 (Reference (a)), reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through (ee).

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

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. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

4. RESPONSIBILITIES

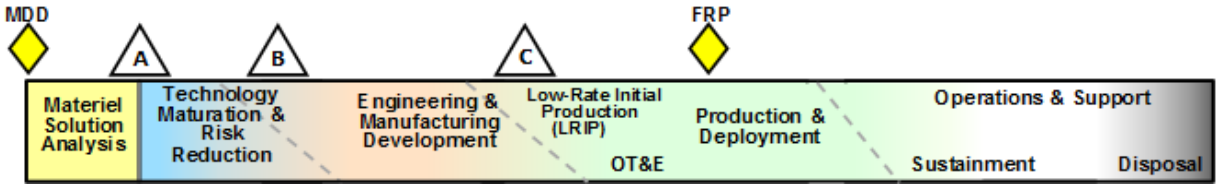
a. Defense Acquisition Executive (DAE). The DAE is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DAE will act as the MDA for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. In accordance with Table 1 in Enclosure 1 of this instruction, the DAE may


Program Protection Plan
Outline & Guidance

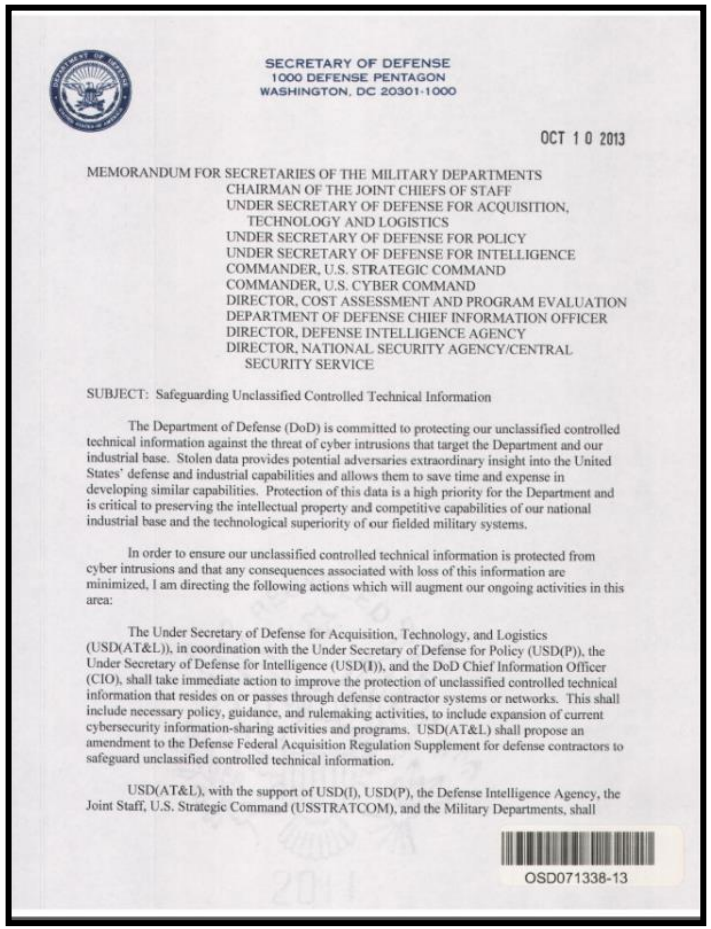
• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

- **Program managers will employ system security engineering practices and prepare a PPP to guide their efforts and the actions of others to manage the risks to critical program information and mission-critical functions and components associated with the program**
  - The PPP will be submitted for MDA approval at each Milestone review, beginning with Milestone A
- **Program managers will describe in their PPP:**
  - Critical Program Information, mission-critical functions, and critical components
  - Threats to and vulnerabilities of these items
  - Plans to apply countermeasures to mitigate associated risks
  - Plans for exportability and potential foreign involvement
  - The Cybersecurity Strategy and Anti-Tamper plan are included as appendices
- **PPP Outline and Guidance provides a template**



# Safeguarding Unclassified Controlled Technical Information



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

OCT 10 2013

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS
UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
COMMANDER, U.S. STRATEGIC COMMAND
COMMANDER, U.S. CYBER COMMAND
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

SUBJECT: Safeguarding Unclassified Controlled Technical Information

The Department of Defense (DoD) is committed to protecting our unclassified controlled technical information against the threat of cyber intrusions that target the Department and our industrial base. Stolen data provides potential adversaries extraordinary insight into the United States' defense and industrial capabilities and allows them to save time and expense in developing similar capabilities. Protection of this data is a high priority for the Department and is critical to preserving the intellectual property and competitive capabilities of our national industrial base and the technological superiority of our fielded military systems.

In order to ensure our unclassified controlled technical information is protected from cyber intrusions and that any consequences associated with loss of this information are minimized, I am directing the following actions which will augment our ongoing activities in this area:

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), in coordination with the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Intelligence (USD(I)), and the DoD Chief Information Officer (CIO), shall take immediate action to improve the protection of unclassified controlled technical information that resides on or passes through defense contractor systems or networks. This shall include necessary policy, guidance, and rulemaking activities, to include expansion of current cybersecurity information-sharing activities and programs. USD(AT&L) shall propose an amendment to the Defense Federal Acquisition Regulation Supplement for defense contractors to safeguard unclassified controlled technical information.

USD(AT&L), with the support of USD(I), USD(P), the Defense Intelligence Agency, the Joint Staff, U.S. Strategic Command (USSTRATCOM), and the Military Departments, shall

OSD071338-13

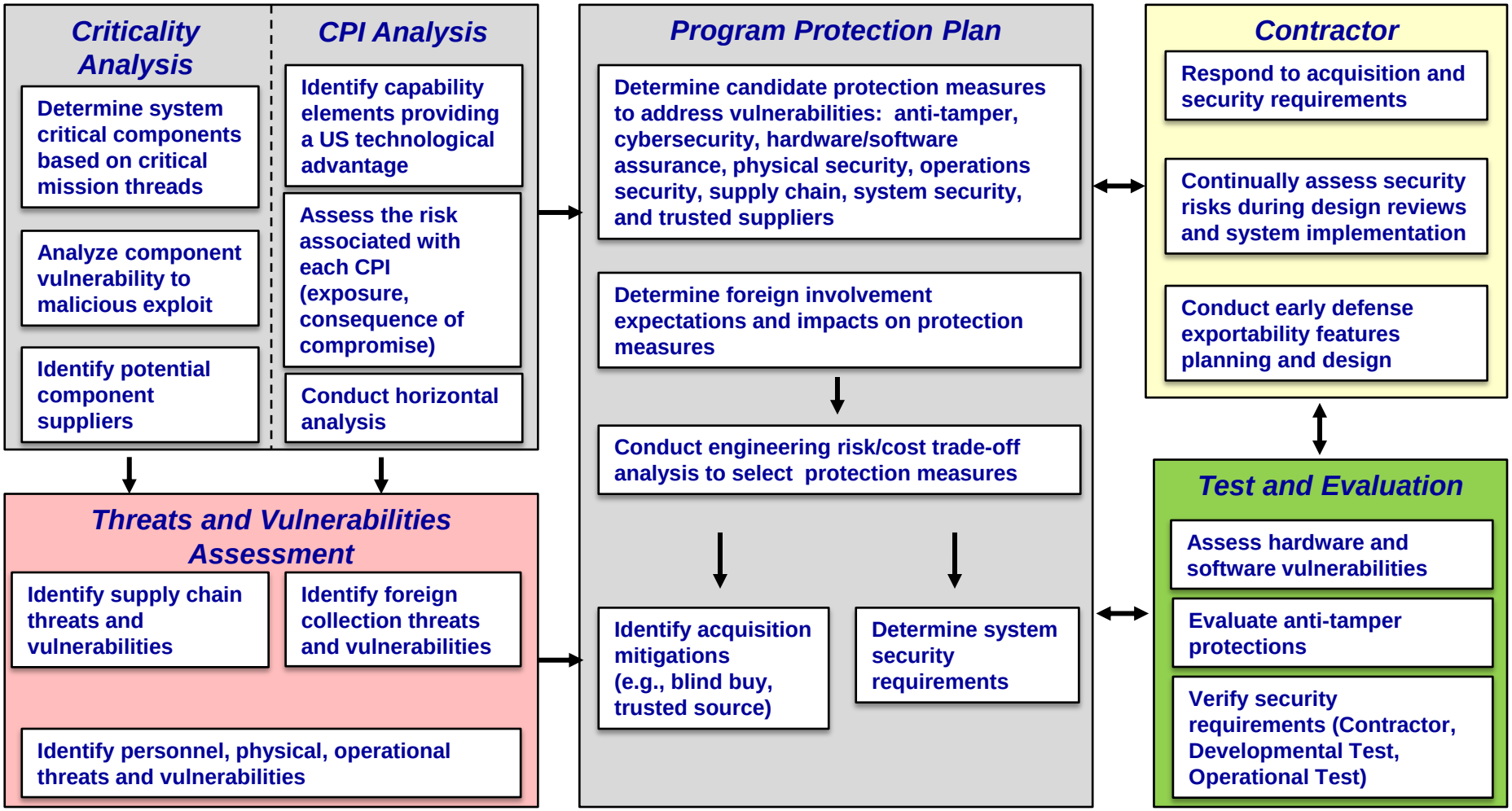
- **Secretary of Defense Memorandum, October 10, 2013**
  - Recognizes the threat to the competitive capabilities of the Defense Industrial Base (DIB) and the technological superiority of our fielded military systems.
  - Directs a series of actions to:
    - Protect DoD unclassified controlled technical information from cyber intrusions
    - Minimize the consequences associated with loss of this information
  - Augments and re-emphasizes current activities, such as the DIB Cyber Security/ Information Assurance (CS/IA) Program

# DFARS Clause 252.204-7012: Safeguarding Unclassified Controlled Technical Information*

- **Published November 18, 2013**
  - Clause affects all new contracts that contain, or will contain unclassified controlled technical information
  - Includes flow down to all subcontracts
- **Purpose: Establish minimum requirements for DoD unclassified controlled technical information on contractor information systems**
  - Requires contractors implement minimum set of information security controls
    - 51 information security controls from NIST SP 800-53, Revision 4
    - Combination of Technical, Process, Awareness, and Training measures
  - Requires contractors report cyber incident and compromises
  - Requires contractor actions to support DoD damage assessment as needed
- **Incident Reporting**
  - Reporting includes:
    - DoD contracts and subcontractor information affected by a cyber incident or compromise
    - DoD programs, platforms, or systems involved
    - Description of DoD technical information compromised
  - Reported information does not include signatures or other threat actor indicators

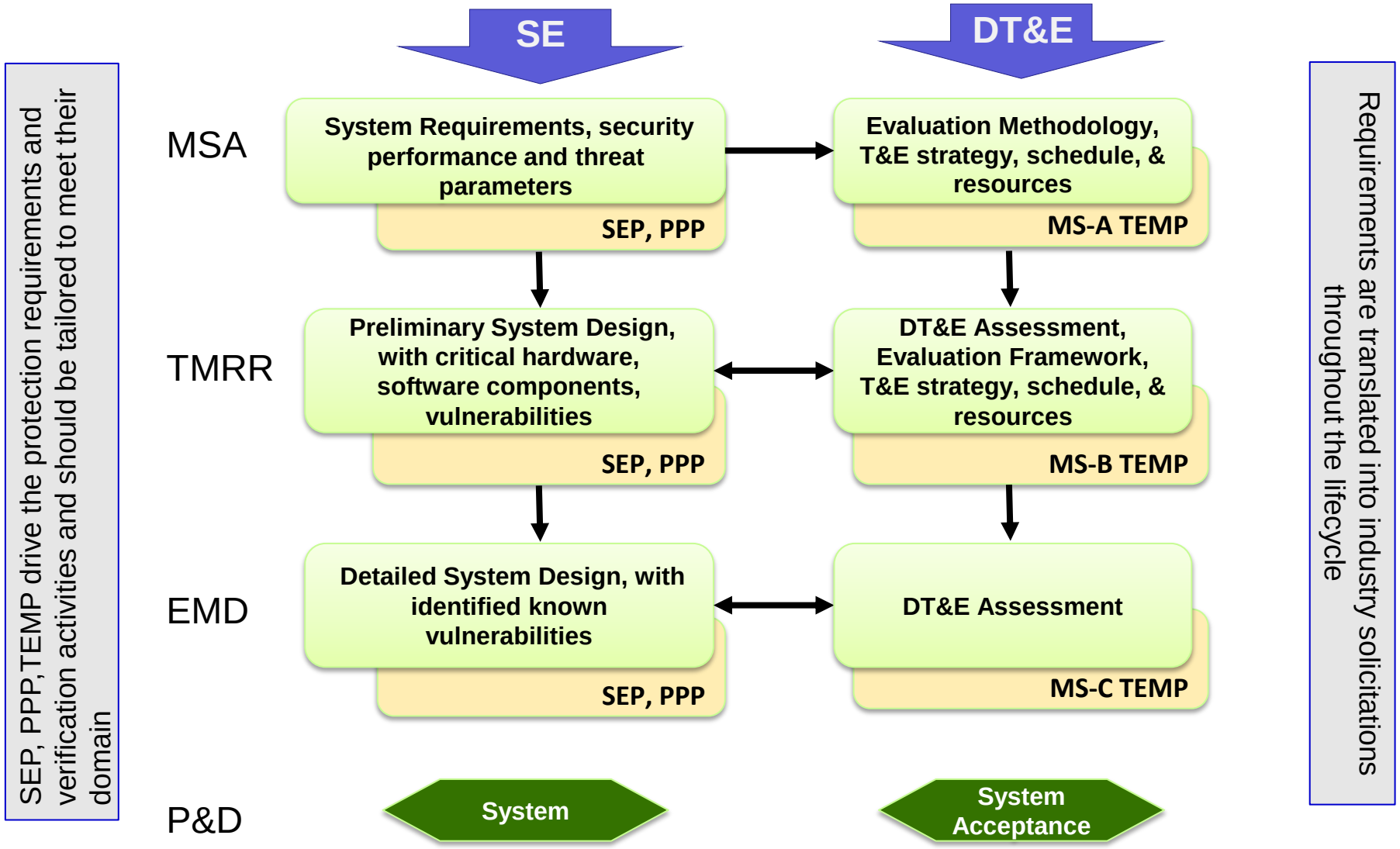
*http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

# PPP Methodology




**Program Protection – an Integral Part of Systems Engineering**

# SE, SSE and DT&E are Mutually Supportive



# Our Focus on SSE and SE

- **DoD is putting policy in place for a risk-based cost benefit trade-off process to protect systems, their supply chain, and their software development**
- **DoD is emphasizing the importance of SSE within systems engineering and its contribution to the design of systems by:**
  - Ensuring that program protection is addressed during the SE technical reviews
  - Incorporating program protection and system security engineering requirements and processes into engineering development contracts
  - Working with industry and standards groups revitalize system security engineering
- **Industry is playing an important role in the DoD SSE initiative by:**
  - Investing in research and processes to protect systems, the supply chain and the software development
  - Developing their SE and SSE processes and skills

**DoD efforts are targeting integration of system security engineering considerations throughout the system life cycle**


# Questions?