Comprehensive Program Protection Planning for the Materiel Solution Analysis (MSA) Phase

Melinda Reed

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

15th Annual NDIA Systems Engineering Conference
San Diego, CA | October 24, 2012

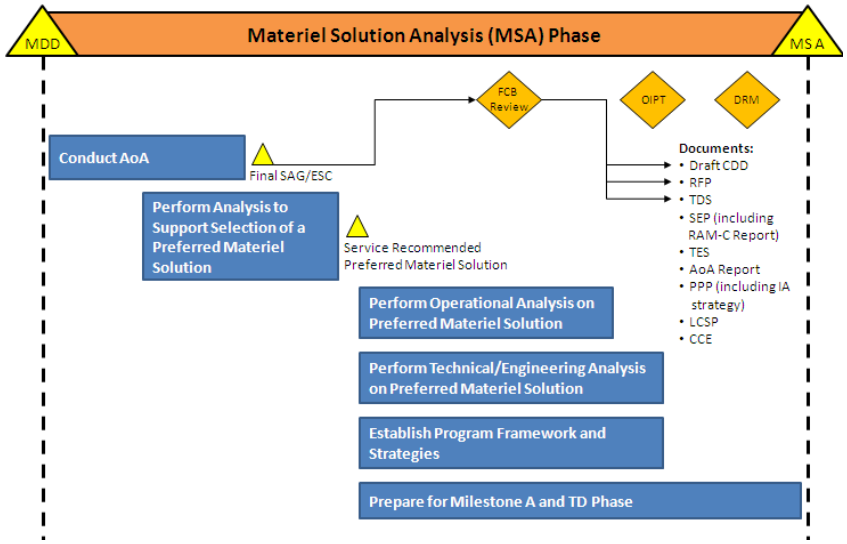
Presentation Objectives

- **Discuss the Materiel Solution Analysis (MSA) Phase Program Protection Plan (PPP) Analysis for Supply Chain and Malicious Insertion Threats**
- **Show the risk based cost-benefit trade to select the mitigations**
- **Describe basic protections to incorporate in the MSA Phase PPP and RFP**
- **Recognize that supply chain and malicious insertion program protections are a shared government-industry responsibility**

DoDI 5200.mm
Trusted Systems and Networks

- **Key Policy Objectives**
  - Manage risk of mission-critical function and component compromise throughout lifecycle of key systems
    - Criticality Analysis is the systems engineering process for focusing activities
    - Mitigations: Supply chain risk management, software assurance, secure design
  - Use all-source intelligence analysis to inform procurement decisions
  - Codify trusted foundry requirement for DoD-unique ASICs
  - Document planning and accomplishments in PPP and IA Strategy
- **Key OSD and Component Responsibilities**
  - Ensure and coordinate protection of mission critical functions and components across the program lifecycle
  - Advance state of the art in software assurance methodology and tools
  - Investigate “trust” implications for non-ASIC microelectronics
  - Analyze suspected and confirmed supply chain exploits across DoD
  - Tasks the Heads of the Components to establish TSN focal points,
  - Tasks DoD with developing a strategy for trust in FPGAs
- **Status**
  - Instruction is currently awaiting signature

MSA Phase Engineering/ Technical Analysis



Draft MSA model from OSD Development Planning Working Group, June 2012.

MSA Phase Engineering Analysis Objectives

- Confirm CONOPS and develop mission and functional threads
- Develop draft system requirements and notional system design
- Identify critical technology elements
- Determine external interfaces and interoperability requirements
- Identify critical functions and CPI

Feeds key Milestone A Requirements

- RFP, SEP (including RAM-C report), TDS, TES, PPP, LCSP, Component Cost Estimate

Influences Draft CDD development

- Balances capability, cost, schedule, risk and affordability

Requires an adequately resourced and experienced Technical Staff

- System and Domain Engineers
- Cost Analysts
- Mission and Operations Reps

Materiel Solution Analysis (MSA) Phase PPP Challenges

Ensuring that basic development, design and supply chain protections are established in the PPP and the RFP to prevent ,detect and respond to malicious attacks

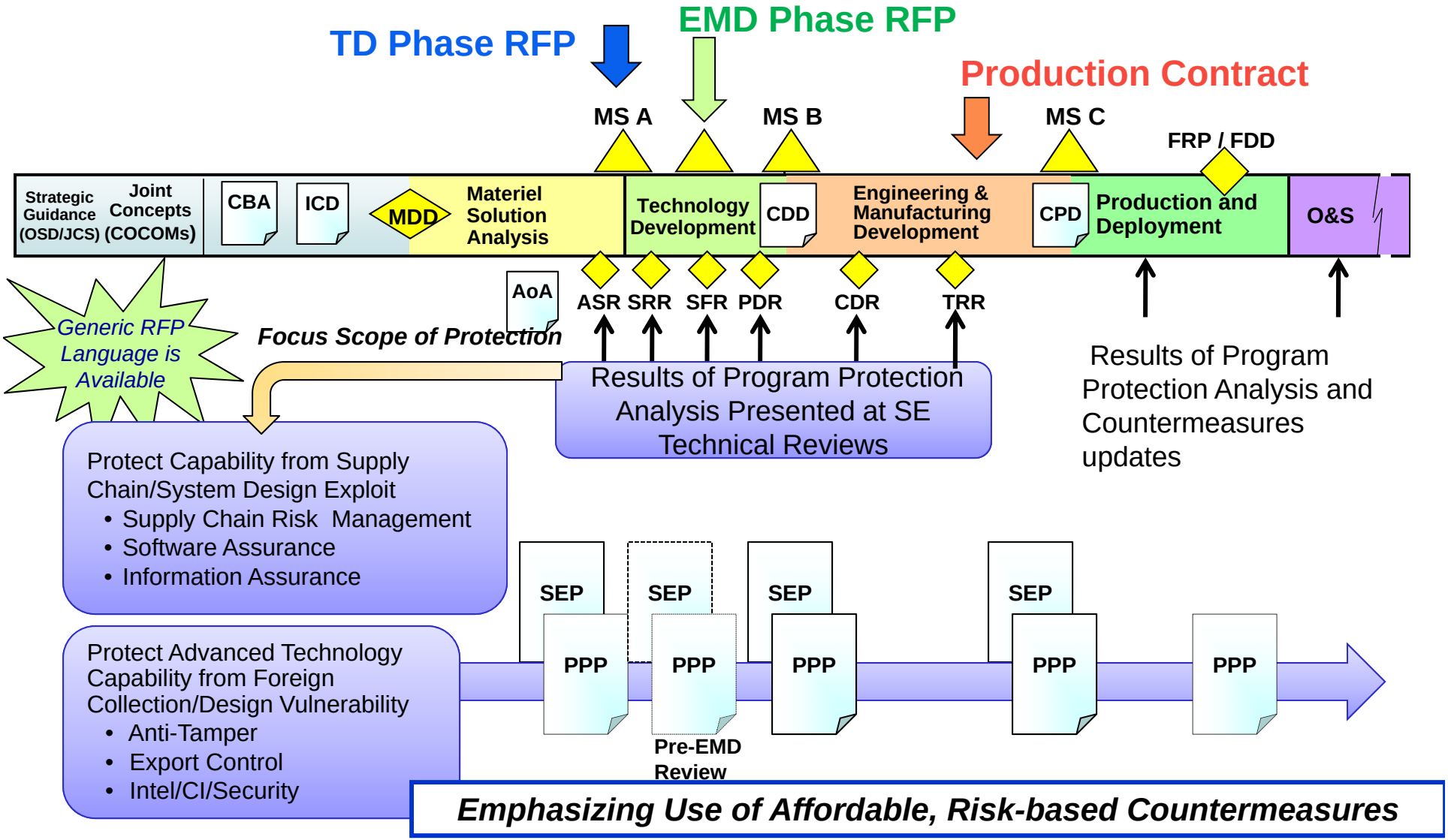
Prevent – Countermeasures that reduce the exploitation of development, design and supply chain vulnerabilities

Detect – Countermeasure that monitor, alert and capture data about the attack

Respond – Countermeasures that analyze attacks and alter system or processes to mitigate the attack

Milestone A Program Protection Plans should contain all three types of mitigations as well as plans for more detailed program protection analysis and updates to inform system security engineering early in the design

PPP Development and Updates



Program Protection Analysis for Supply Chain and Software Assurance

Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

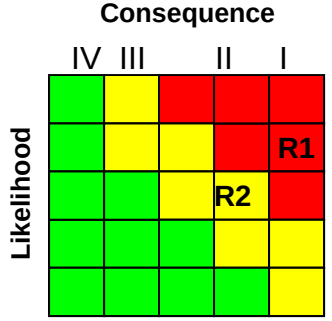
Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

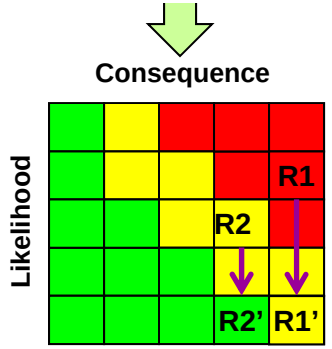
Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture



Risk Mitigation Decisions



Risk Mitigation and Countermeasure Options

Criticality Analysis Methodology

Criticality Analysis

MS A Phase Inputs:
ICD
Concept of Operations
Potential Software development processes
Potential Vulnerabilities
Preferred concept

- Identify and group Mission Threads by priority
- Identify Critical Functions that will be implemented with logic bearing components
- Assign Criticality Levels
- Map Threads and Functions to Subsystems and Components
- Identify Critical Suppliers

Integral Part of SE Process

Leverage existing mission assurance analysis, including flight & safety critical

Criticality Levels

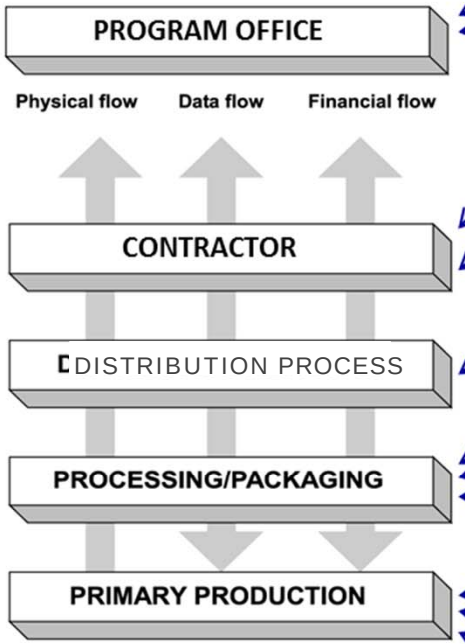
Level I: **Total Mission Failure**
Level II: **Significant/Unacceptable Degradation**
Level III: **Partial/Acceptable Degradation**
Level IV: **Negligible**

Outputs:
- Table of Level I & II Critical Functions and Components
- TAC Requests for Information

Generic Threats – Supply Chain Attacks

Coverage is for what part of the chain is infiltrated and what the malicious insertion accomplishes

Supply Chain



Attack Vectors

Clandestine changes to mission data

Infiltration of sites to insert back doors and malicious logic into some micro electronics (FPGAs and other devices)

Infiltration of company receiving department to add / substitute components with backdoors to allow remote penetration during operations, denial of service, etc.

Infiltration of transportation companies to intercept DoD component shipments (developmental or COTS) and substitute components that have malicious code inserted

Insertion of malicious software in the open source used for math libraries

Infiltration allowing malicious software implantation through 3rd party bundling

Establishment of shell company to insert counterfeit parts

Infiltration to manipulate the hardware or software baselines

Infiltration of company software development to insert software which exfiltrates data

Infiltration to compromise the design/fabrication of hardware

Can have multiple levels: OEMs → subassembly suppliers → assembly suppliers → integrators

Generic Threats – Malicious System Exploitation Attacks

Attack Vectors for Malicious exploitation of fielded systems

Exploitation of system design vulnerabilities

Configuration, Operational Practices

Supply Chain (penetration, corruption)

Malware (downloaded, embedded)

External Mission Load Compromise

DNS Based Threats (cache poisoning)

Applications (built-in malware)

E-mail Based Threats (attachments)

Data Leakage (via social media)

Password Misuse (sharing)

Denial of Service (embedded malware)

Kill Switch Activation (embedded malware)

Mission Critical Function Alteration (embedded malware)

Exfiltration (by adversary)

Network Threat Activity (host discovery)

Compromised Server Attacks (on clients)

Malicious Activity (disruption, destruction)

Auditing Circumvention (evading detection)

Web Based Threats (disclosing sensitive info)

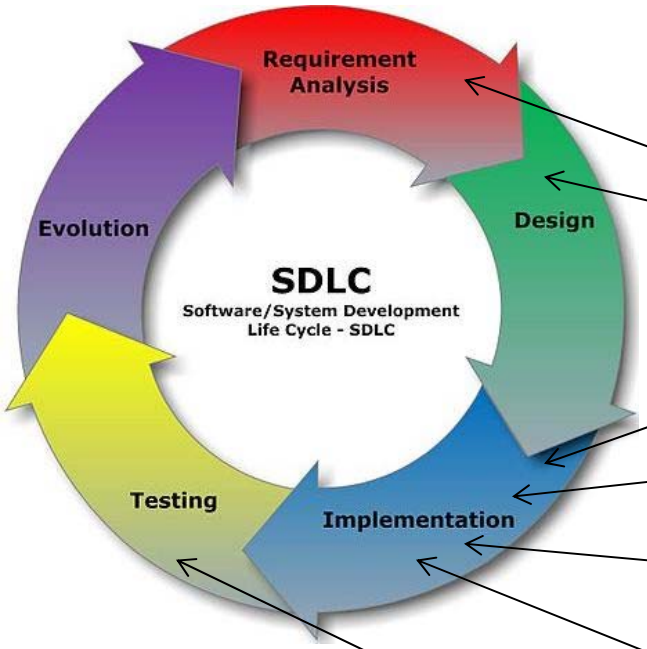
Zero Day Vectors (vulnerabilities without fixes)

Improper File/Folder Access (misconfiguration)

- **Supply Chain**
- **Embedded Malware**

Generic Threats – Malicious Insertion in Software Development Life Cycle

Coverage is for what part of SDLC is targeted and how malicious insertion is accomplished



Attack Vectors for Malicious Code Insertion

- Hidden in software's design (or even requirements)
- Appended to legitimate software code
- Added to linked library functions
- Added to installation programs, plug-ins, device drivers, or other support programs
- Integrated into development tools (e.g., compiler generates malicious code)
- Inserted via tools during system test

Vulnerability Assessment Methodology

Vulnerability Assessment

MS A Phase Inputs:
Concept of Operations
Notional System Architecture
Critical Functions
Some Potential Critical Components
Threat Analysis Results
Descriptions of Potential Processes:

- Determine Access Path Opportunities
- Determine Attack Scenarios
- Determine Exploitable Vulnerabilities
- Inform the TA/VA-Based Risk Likelihood Determination

Fidelity increases as the system is elaborated in later phases

Outputs:
- Supply Chain Vulnerabilities
- HW/SW development process vulnerabilities
- System design vulnerabilities
- Input to likelihood assessment of risks
- Possible Countermeasure / mitigation

Cost-Benefit-Risk Trade Study Methodology

- **For each critical function / critical component identified for risk reduction**
  - Determine at least two countermeasures to evaluate
  - Estimate the risk reduction achieved by each countermeasure
  - Estimate the implementation cost impacts

Component	Risk Rating	Counter / Mitigation	Cost impact	Risk reduction	Residual Risk Rating
Critical Component 1 (supplier X)	H	Counter 1	H	L	M to H
		Counter 2	M	M	M
Critical Function A and all components (suppliers W, Y, Z)	M	Counter 3	L	L	M
		Counter 2	M	M	L
Critical Function A Band all components (suppliers L,M, N, Q)	H	Counter 4	L	M	M
		Counter 5	M	L	M to H

Table - Cost Benefit Trade Summary

- **Select countermeasures for Implementation**
- **Document selected countermeasures in PPP with rationale and incorporate into the RFP: SOW and SRD**

Potential basic development, design and supply chain protections (1 of 4)

- **The contractor shall:**
  - Create and update the program protection analysis at each of the SETRs to:
    - Identify mission critical functions and associated components
    - Identify technology exploitation, fielded system compromise, development and supply chain malicious insertion vulnerabilities
    - Utilize threat assessments
    - Develop program protection risks
    - Identify risk reduction countermeasures (mitigations) based upon a cost-benefit trade study
  - Maintain multi-level visibility into the supply chain of the critical function components .
  - Extend these responsibilities to sub-tier suppliers of critical function components
  - Incorporate government provided intelligence
  - Establish secure design and coding standards

Potential basic development, design and supply chain protections (2 of 4)

- **For Level I Mission Critical Functions/Critical Components the system shall establish basic protection requirements unless justified by a cost benefit analysis. Supply Chain and Development basic protections shall include:**
  - Supplier Management Plan that
    - Includes supplier selection criteria to reduce supply chain risks
    - Identifies functionally equivalent alternate components and sources
    - Evaluates and maintains a list of suppliers and alternates suppliers with respect to the criteria established
  - An anonymity plan that
    - Protects the baseline design, test and supply chain data
    - Use blinds buys for component procurement
  - Additional access controls that
    - Further limits access beyond normal program control
    - Logs access
    - Establishes data collection for post attack forensic analysis
    - Require inspection and approval of changes
  - Black hat attack testing of system, development environment and supply chain
  - Red team testing
  - Material and non material attack / compromise response process development

Potential basic development, design and supply chain protections (3 of 4)

- **For Level I Mission Critical Functions/Critical Components the system shall establish basic protection requirements unless justified by a cost benefit analysis. Design requirements basic protections shall include:**
  - Establish least privilege using distrustful decomposition (privilege reduction) or similar approach to move level I critical functions into separate mutually untrusting programs*
  - Physical and logical diversification of components for critical functions which require redundancy to meet reliability or safety requirements
  - Physical and logical diversification with voting to establish trustworthiness of selected level I critical function components
  - Wrappers for COTS, legacy and developmental software to enforce strong typing, context checking and other interface validation methods for interfaces with critical functions.
  - Wrappers for COTS, legacy and developmental software to identify and log invalid interface data using secure logging approaches

- **Basic protection security requirements and designs shall be discussed in each of the Systems Engineering Technical Reviews**

*See SEI -2009-TR-010

Potential basic development, design and supply chain protections (4 of 4)

To evaluate each contractor's implementation of the basic program protections

- **Section L of the RFP should include:**
  - The contractor shall describe for level I mission critical functions / components the approach to :
    - Supplier management and the use of an anonymity plans
    - Maintenance of multi-level visibility into the supply chain of the critical function components
    - PPP analysis to determine and mitigate program protection risks
    - Establish and update secure design and coding standards
    - Use of secure design patterns and least privilege for critical functions
    - Use of physical and logical diversification for critical function components

- **Section M of the RFM should include**
  - The above section L statement in the evaluation criteria

RFP Sections

RFP Package

- Section A: Solicitation Contract Form
- Section B: Supplies or services and prices/costs
- **Section C: Description/specifications/work statement**
  - **System Requirements Document (SRD - SPEC)**
  - **Statement of Work (SOW)**
  - **Contract Deliverable Requirements List (CDRLs)**
- Section D: Packaging and marking
- Section E: Inspection and Acceptance
- Section F: Deliveries or performance
- Section G: Contract administration data
- Section H: Special contract requirements
- Section I: Contract Clauses
- Section J: List of Documents, Exhibits, and other Attachments
- Section K: Representations, Certification, and Other Statements of Offerors
- **Section L: Instructions, conditions, and notice to offerors**
- **Section M: Evaluation factors for award**

- **Incorporate Process Protections**
  Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or equivalent
- **Incorporate Design Protections**
  System Requirements Document (SRD), Specification, or equivalent
- **Contract Deliverable Requirements List (CDRL) and Data Item Description (DID)**

- **Description of program protection processes for Level I/II critical components**
  - Sections L and M

MSA Phase Key Points

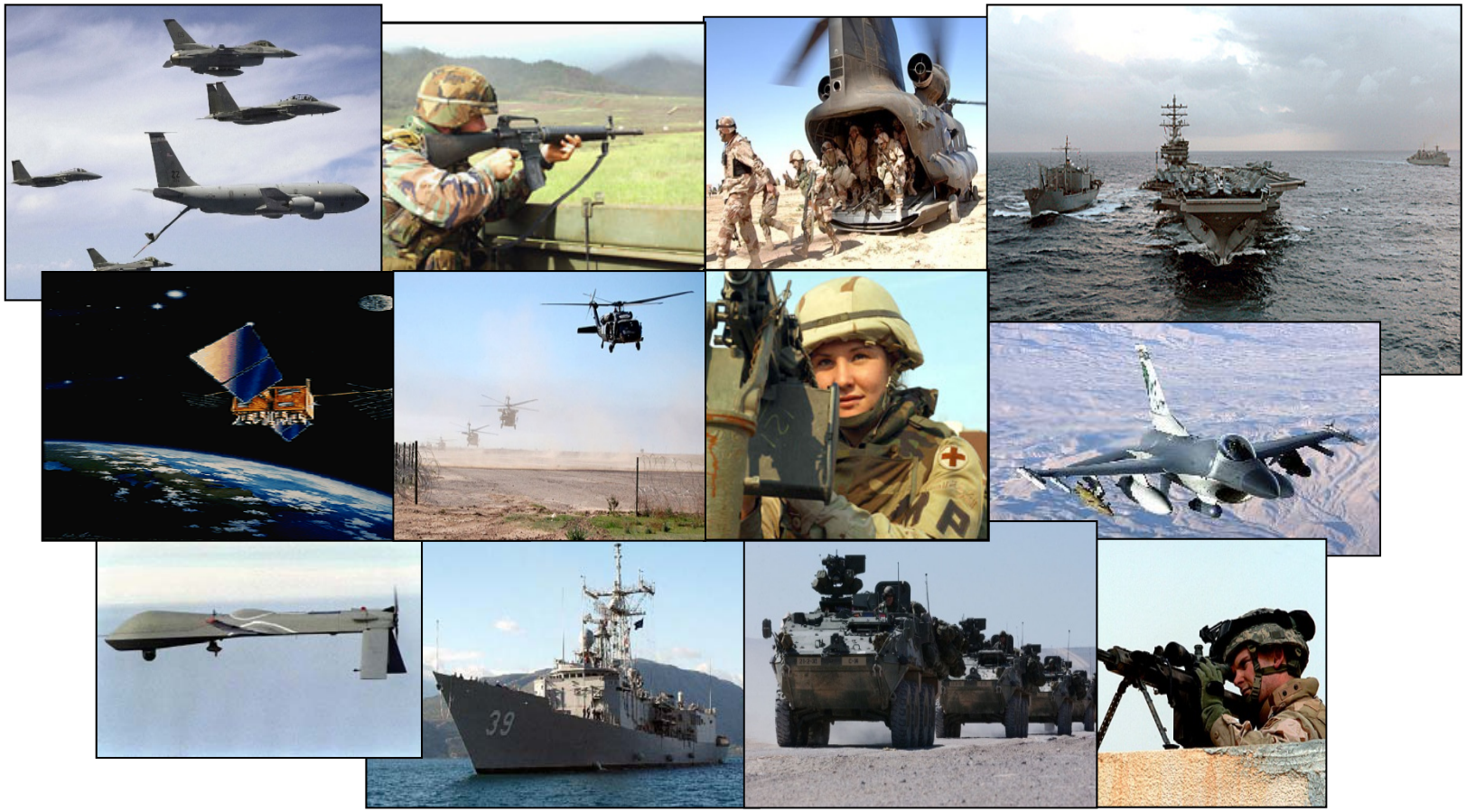
- **It is both possible and necessary to perform meaningful system security engineering prior to Milestone A**
  - Mission critical system functions and some potential implementing components can be identified
  - Known generic attack vectors mapped against the system CONOPS and notional architecture can be used to inform a vulnerability assessment that uncovers potential exploitable vulnerabilities

- **A risk based cost benefit trade-off is a mechanism to select the protection requirements to incorporate into the TD Phase RFP SOW and SRD**

- **The SOW should indicate that further program protection analysis is a Government-Industry shared responsibility throughout the remainder of the lifecycle as the system is refined and details are determined**

Questions?

Systems Engineering: Critical to Program Success



Innovation, Speed, and Agility

http://www.acq.osd.mil/se