



DoD Trusted Systems and Networks (TSN) Update

Kristen Baldwin

Principal Deputy

**Office of the Deputy Assistant Secretary of Defense
for Systems Engineering, OUSD(AT&L)**

NDIA Cyber Division Breakfast Meeting

February 12, 2013

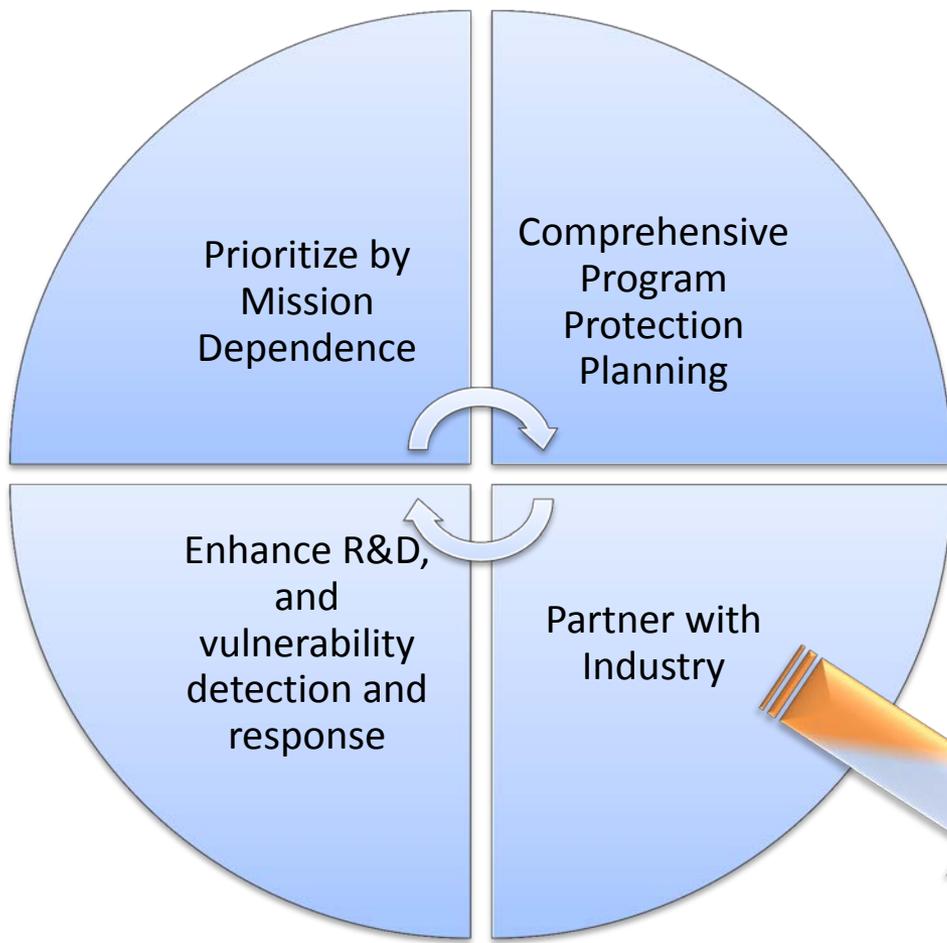


Trusted Defense Systems and Networks Strategy



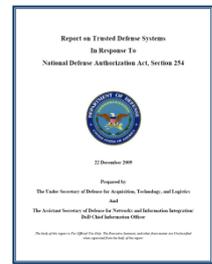
Drivers/Enablers

- National Cybersecurity Strategies
- Congressional Interest
- Globalization Challenges
- Increasing System Complexity
- Increased Threat



Delivering Trusted Systems

Report on Trusted Defense Systems



USD(AT&L)
ASD(NII)/DoD CIO

Executive Summary:

<http://www.acq.osd.mil/se/igp/spec-studies.html>



Ensuring Confidence in Defense Systems and Networks



- **Threat: Nation-state, terrorist, criminal, or rogue developer who:**
 - Gain control of systems through supply chain opportunities
 - Exploit vulnerabilities remotely
- **Vulnerabilities**
 - All systems, networks, and applications
 - Intentionally implanted logic
 - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- **Traditional Consequences: Loss of critical data and technology**
- **Emerging Consequences: Exploitation of manufacturing and supply chain**
- **Either can result in corruption; loss of confidence in critical warfighting capability**

Today's acquisition environment drives the increased emphasis:

Then

Stand-alone systems

Some software functions

Known supply base

CPI (technologies)

>>>

>>>

>>>

>>>

Now

Networked systems

Software-intensive

Prime Integrator, hundreds of suppliers

CPI and critical components



What Are We Protecting?



Program Protection Planning

DoDI 5000.02

DoDI 5200.39

DoDI 5200.44

DoDI 8500 Series
DoDI 8582.01

Technology

Components

Information

What: Leading-edge research and technology

Who Identifies: Technologists, System Engineers

ID Process: CPI Identification

Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments

Countermeasures: AT, Classification, Export Controls, Security, Foreign Disclosure, and CI activities

Focus: "Keep secret stuff in" by protecting any form of technology

What: Mission-critical elements and components

Who Identifies: System Engineers, Logisticians

ID Process: Criticality Analysis

Threat Assessment: DIA SCRM TAC

Countermeasures: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Foundry, etc.

Focus: "Keep malicious stuff out" by protecting key mission components

What: Information about applications, processes, capabilities and end-items

Who Identifies: All

ID Process: CPI identification, criticality analysis, and classification guidance

Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments

Countermeasures: Information Assurance, Classification, Export Controls, Security, etc.

Focus: "Keep critical information from getting out" by protecting data

Protecting Warfighting Capability Throughout the Life Cycle



Program Protection Integrated in Policy



DoDI 5000.02 Operation of the Defense Acquisition System

- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD
- References DoDI 5200.39



DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD

- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Expands definition of CPI to include degradation of mission effectiveness



DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components



DoDI 8500.01E Information Assurance

- Establishes policy and assigns responsibilities to achieve DoD information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

DoD Issuances Website: <http://www.dtic.mil/whs/directives/corres/ins1.html>



Program Protection Guidance



Program Protection Plan Outline & Guidance, dated 18 Jul 2011

- **Focal point for documenting Program security activities, including:**
 - Plans for identifying and managing risk to CPI and critical functions and components
 - Responsibilities for execution of comprehensive program protection
 - Tables of actionable data, not paragraphs of boilerplate
 - End-to-end system analysis and risk management
- **<http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf>**

Defense Acquisition Guidebook Chapter 13, “Program Protection”

- **Provides implementation guidance for TSN Analysis and CPI Protection**
- **Describes SSE activities throughout the Defense Acquisition Life Cycle**
- **<https://acc.dau.mil/dag13>**



DoDI 5200.44 Trusted Systems and Networks



Department of Defense INSTRUCTION

NUMBER 5200.44
November 5, 2012

DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. **PURPOSE.** This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

2. **APPLICABILITY.** This Instruction 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 (hereinafter referred to collectively as the "DoD Components").

- Implements the DoD's Trusted Systems and Networks (TSN) strategy
- Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing
 - Criticality Analysis as the systems engineering process for risk identification
 - Countermeasures: Supply chain risk management, software assurance, secure design patterns
 - Intelligence analysis to inform program management
- Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)
- Document planning and accomplishments in program protection and information assurance activities



TSN Analysis for Supply Chain and HW/SW Assurance

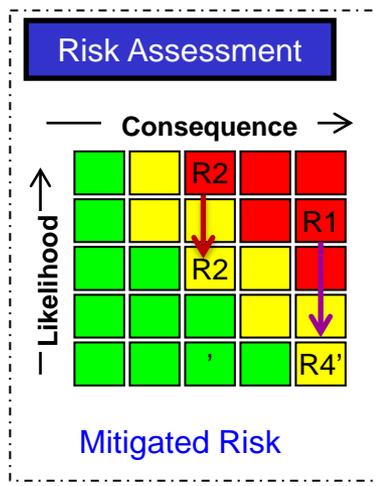
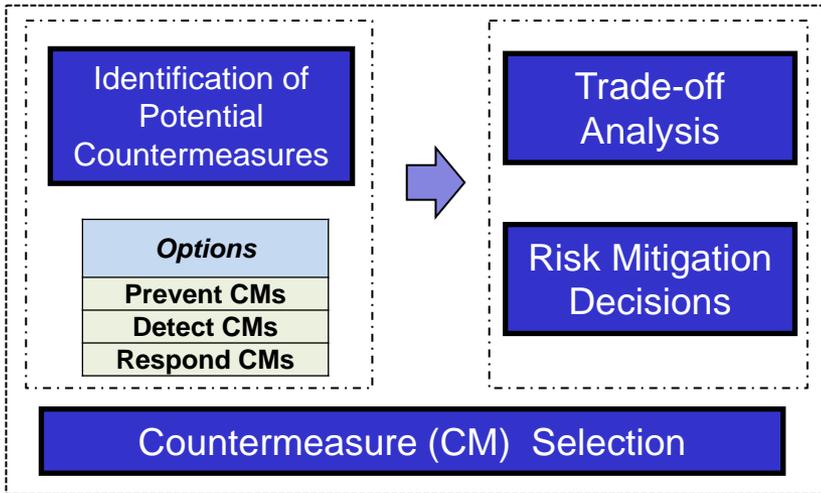
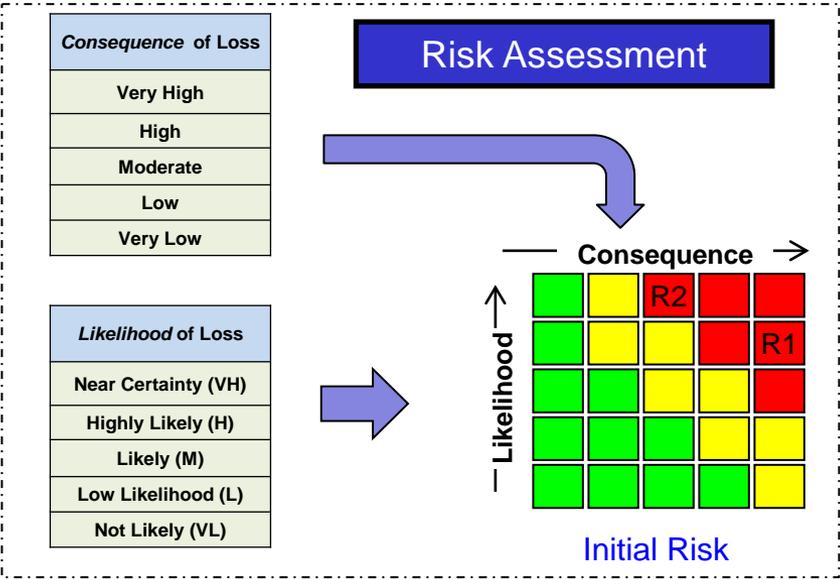


Criticality Analysis

Threat Assessment

Vulnerability Assessment

Information Assurance Assessment





Defense Industrial Base (DIB) Cyber Security



“The private sector, government, military, our allies - all share the same global infrastructure and we all share the responsibility to protect it.”

- Secretary of Defense Leon E. Panetta

Thursday, October 11, 2012

DoD efforts to advance cyber security in the DIB include:

- DIB Cyber Security/Information Assurance (CS/IA) Program, and its optional enhanced component the DIB Enhanced Cybersecurity Services (<http://dibnet.dod.mil>)
- Standards development in collaboration with Industry
- Reinforcing protection of technical information in acquisition activities



FY13 NDAA Sections 941 and 933



SEC. 941. REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS.

(a) PROCEDURES FOR REPORTING PENETRATIONS.—The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

(b) NETWORKS AND INFORMATION SYSTEMS SUBJECT TO REPORTING.—

(1) CRITERIA.—The Secretary of Defense shall designate a senior official to, in consultation with the officials specified in paragraph (2), establish criteria for covered networks to be subject to the procedures for reporting system penetrations under subsection (a).

(2) OFFICIALS.—The officials specified in this subsection are the following:

(A) The Under Secretary of Defense for Policy.

(B) The Under Secretary of Defense for Acquisition, Technology, and Logistics.

(C) The Under Secretary of Defense for Intelligence.

(D) The Chief Information Officer of the Department of Defense.

(E) The Commander of the United States Cyber Command.

(c) PROCEDURE REQUIREMENTS.—

(1) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each cleared defense contractor to rapidly report to a component of the Department of Defense designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection (b).

(b) Each such report shall include the following: (A) A description of the technique or method used in such penetration.

(B) A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration. (C) A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration.

SEC. 941. REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS.

(a) PROCEDURES FOR REPORTING PENETRATIONS.—The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

(b) NETWORKS AND INFORMATION SYSTEMS SUBJECT TO REPORTING.—

(1) CRITERIA.—The Secretary of Defense shall designate a senior official to, in consultation with the officials specified in paragraph (2), establish criteria for covered networks to be subject to the procedures for reporting system penetrations under subsection (a).

(2) OFFICIALS.—The officials specified in this subsection are the following:

(A) The Under Secretary of Defense for Policy.

(B) The Under Secretary of Defense for Acquisition, Technology, and Logistics.

(C) The Under Secretary of Defense for Intelligence.

(D) The Chief Information Officer of the Department of Defense.

(E) The Commander of the United States Cyber Command.

(c) PROCEDURE REQUIREMENTS.—

(1) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each cleared defense contractor to rapidly report to a component of the Department of Defense designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection (b).

(b) Each such report shall include the following: (A) A description of the technique or method used in such penetration.

(B) A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration. (C) A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration.

- **FY13 NDAA SEC. 941: REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS**
 - “The Secretary of Defense shall establish procedures that require each cleared defense contractor to report ... when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.”
- **FY13 NDAA SEC. 933: IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED BY THE DEPARTMENT OF DEFENSE**
 - USD(AT&L), in coordination with the DoD CIO... “shall develop and implement a baseline software assurance policy for the entire lifecycle of covered systems. Such policy shall be included as part of the strategy for trusted defense systems of the Department of Defense.”
 - ...“(2) require covered systems to identify and prioritize security vulnerabilities and, based on risk, determine appropriate remediation strategies for such security vulnerabilities;”

NDAA: National Defense Authorization Act <http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf>



Software Assurance



- **FY 12 Activities**

- Established DoD Software Assurance (SwA) enterprise-level Community of Practice (CoP) in coordination with DCIO(CS)/TMSN and NSA(CAS)
- Initiated three DoD SwA stakeholder initiatives:
 - SwA-related contract language
 - Enterprise coordination and information sharing
 - Workforce education and training
- Updated SwA elements of the Defense Acquisition Guidebook to assist acquisition programs in tailoring and refining software security requirements
- Initiated a study of SwA tools for development and operational testing
- Agreed upon a standard definition of SwA across the Department

- **FY 13 Goals**

- Expand the DoD SwA Community of Practice to increase coordination, collaboration, and promulgation of best practices
- Update policy, guidance, and PPP activities to address software assurance in software development and system operation



System Security Community Activities



- **NDIA “Guidebook for System Assurance”, Version 1.0, 2008**
 - Process/technology guidance to increase the level of system assurance through a planned, systematic set of multi-disciplinary activities
 - <http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf>
- **ISO/IEC 15026 – System and Software Engineering – Systems and Software Assurance**
 - Establishes common assurance concepts, vocabulary, integrity levels and life cycle activities
- **ISO/IEC 27036 – IT Security Techniques – Supplier Relationships**
 - Establishes techniques between acquirer and supplier for supply chain risk management
- **International Council on Systems Engineering (INCOSE) Handbook**
 - Working group to develop security engineering updates to INCOSE SE Handbook
- **NIST - System Security Engineering (SSE) 800-160 Special Pub (In Development)**
 - Aligns SSE with ISO/IEC15288 terminology, incorporates DoD best practices
 - DoD Appendix targets DoD community, includes Systems Engineering Technical Review (SETR) criteria
- **The Open Group (TOG)**
 - The Open Trusted Technology Provider Framework (O-TTPF) - open standard that codifies best practices across the entire lifecycle (targeted against counterfeit HW & malicious SW)
 - <http://www.opengroup.org/ogttf/>



System Security Engineering (SSE) Research Activities



Security Engineering Research at Systems Engineering Research Center (SERC) <http://www.sercuarc.org>

- **Published the SSE Research Roadmap in August 2010**



- Outlines approach for advancing SSE definitions, metrics, frameworks, and human capital through coordinated research plans
- Captures input from 50+ industry, academia, and government experts

- **Conducting follow-on research in “System Aware” Security**



- Defining secure design patterns for cyber-physical systems
 - e.g., physical and virtual configuration hopping, diverse redundancy of components
- Applying scoring methodology to evaluate alternatives
 - Identifying critical functions to protect, asymmetric attack vectors, performance tradeoffs in secure design patterns, cost and collateral impacts
- Pilot application in DoD system



NDIA SE Division May 2012 PPP Workshop



- **NDIA SE Division System Assurance Committee, led workshop in May 2012**
 - Reviewed threat and policy related to trusted defense systems
 - Three focus groups identified issues for specific areas of Program Protection
 - Workshop participants voted to identify the Top 5 issues regarding Program Protection
- **NDIA SE Division System Assurance Committee**
 - For more information about the committee and its events, visit http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Pages/Systems_Assurance_Committee.aspx



NDIA SE Division May 2012 PPP Workshop Top 5 Issues



Rank	Group	Issue
1	3	Taxonomy Integration of the DoD security disciplines is hampered by terms of reference that have different meanings depending on the discipline or the context.
2	2	Limited Security Performance Metrics are available Lack of performance metrics to ensure program protection requirements.
3	1	Satisfying PPP Objectives through Improved Contract / Acquisition Strategy
4	2	Lack of well defined threat and attack vectors for SE community in Acquisition and Industry
5	2, 3	Lack of education across the acquisition and industry communities with regards to SSE

*** Led by NDIA SE Division System Assurance Committee**



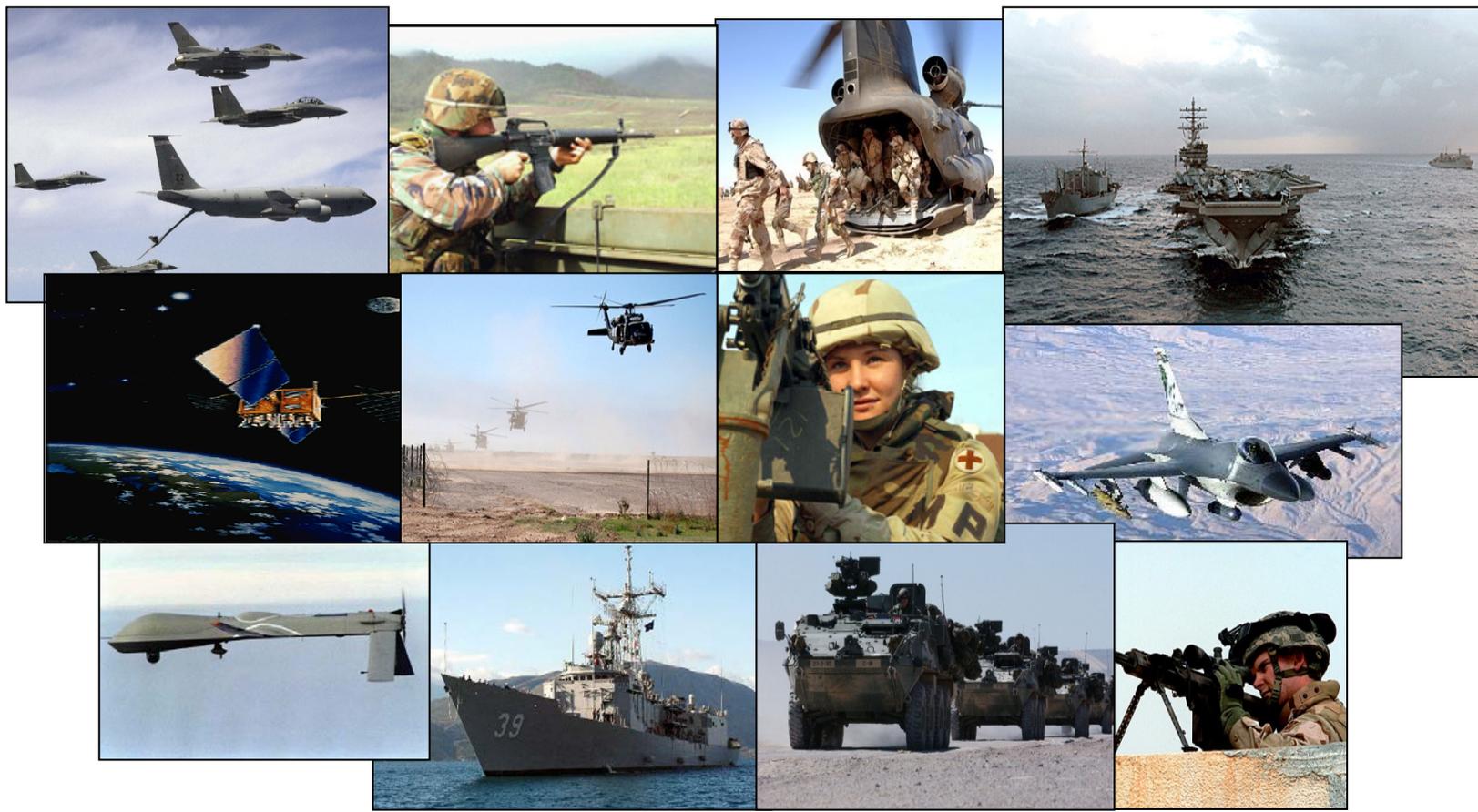
In Summary



- **Holistic approach to security is critical**
 - To focus attention on the threat
 - To avoid risk exposure from gaps and seams
- **Program protection policy provides overarching framework for trusted systems**
 - Common implementation processes are beneficial
- **Stakeholder integration is key to success**
 - Acquisition, CIO, Intelligence, Engineering, Industry, Academic communities are all stakeholders
- **Systems engineering brings these stakeholders, risk trades, policy, and design decisions together**
 - Informing leadership early; providing programs with risk-based options



Systems Engineering: Critical to Acquisition Success



Innovation, Speed, and Agility
<http://www.acq.osd.mil/se>