DoD Program Protection

Kristen J. Baldwin
Principal Deputy
Office of the Deputy Assistant Secretary of Defense
for Systems Engineering, OUSD(AT&L)

NDIA Program Protection Summit / Workshop
Mclean, VA | May 20, 2014

Many Supply Chain 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.

Emerging Threats

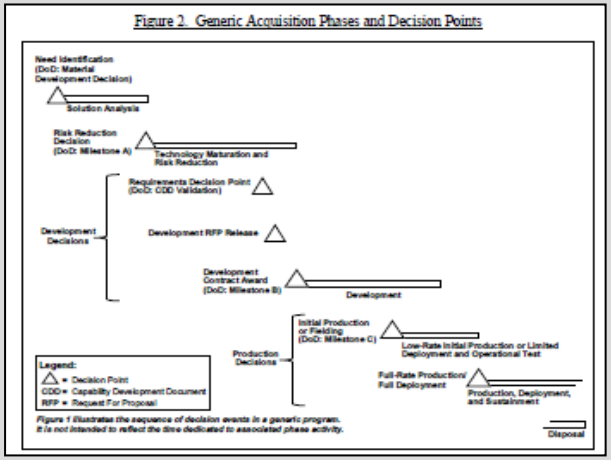
New threats, cyber security attacks, and trust issues that combine two or more threats

DoD Program Protection focuses on risks posed by malicious actors

Malicious Supply Chain Risk

- ***Threat*:**
  - Nation-state, terrorist, criminal, or rogue developer who gain control of systems through supply chain opportunities, exploit vulnerabilities remotely, and/or degrade system behavior
- ***Vulnerabilities:***
  - All systems, networks, and applications
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Consequences:***
  - Loss of critical data and technology
  - System corruption
  - Loss of confidence in critical warfighting capability; mission impact

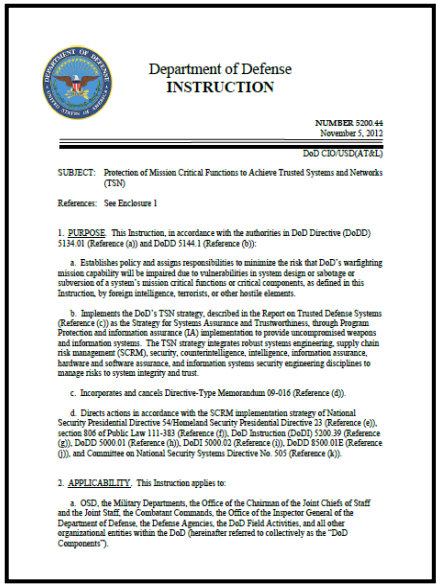
Access points are throughout the lifecycle…



…and across multiple supply chain entry points

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

DoD Trusted Systems and Networks Strategy and Policy



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").

Promulgated in DoDI 5200.44, requiring:

- **Risk management 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**, including supply chain risk management, software and hardware assurance, secure design patterns
  - **Testing and Evaluation**, to detect HW/SW vulnerabilities
  - **Intelligence analysis** to supplier acquisition strategies
- **DoD-unique application-specific integrated circuits (ASICs) must be procured from trusted certified suppliers**
- **Plans and mitigations documented in program protection and information assurance activities**

Program Protection Interim DoDI 5000.02

- **Program Protection is the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle.**
  - Also supports international partnership building and cooperative opportunities objectives by enabling the export of capabilities without compromising underlying U.S. technology advantages

- **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 Methodology

Criticality Analysis

- Based upon mission threads, determine system critical components
- Analyze component vulnerability to malicious exploit
- Identify potential component suppliers

Supplier Threat Assessment

- DIA Conducts All-source Analysis and submits Threat Report to Component Focal Point

Countermeasures

- Determine countermeasures to address vulnerabilities: OPSEC, trusted suppliers, system security engineering, hardware/software assurance

Program Protection Plan

- Engineering risk/cost tradeoff analysis to determine system security requirements
- Acquisition strategy mitigations for supplier threat (e.g. blind buy, trusted source)
- Evaluate mitigations over time with intel, engineering, and test; update PPP at major milestones

Contractor

- RFP includes Supply Chain and security requirements
- Design reviews continually assess security risk

Test & Evaluation

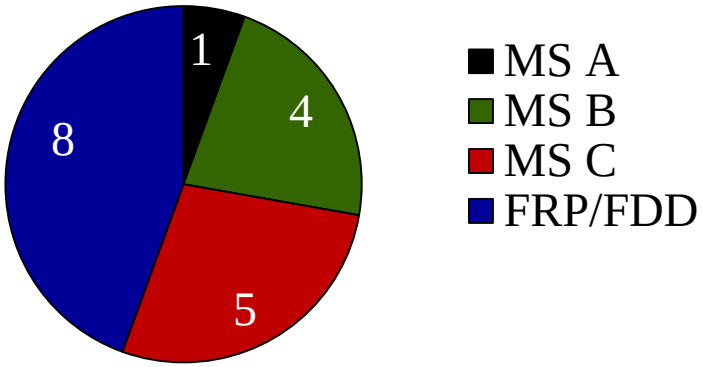
- HW/SW vulnerability detection
- Contractor, DT, OT assessment of mitigations

Program Protection Activity - Integral Part of SE Process

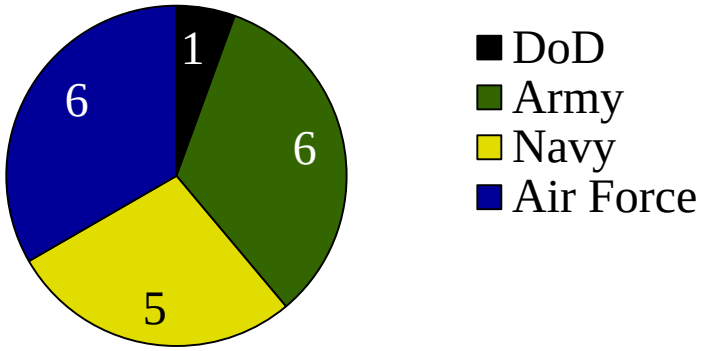
PPP Approval Statistics
ACAT ID/IAM

47 PPPs Approved	
FY 2010	4
FY 2011	7
FY 2012	5
FY 2013	18
FY 2014 (to date)	13

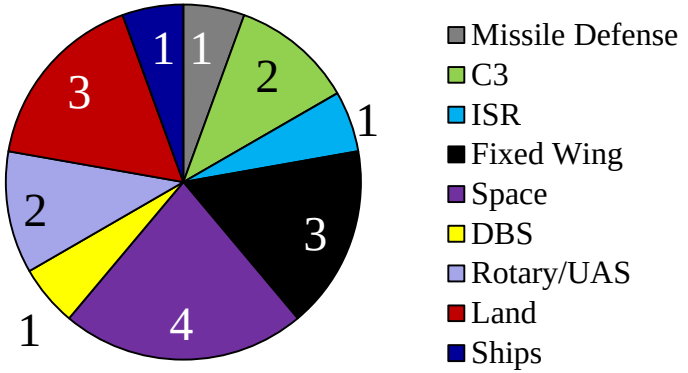
FY13 PPPs by Milestone



FY13 PPPs by Service



FY13 PPPs by Domain



Program Protection Outline and Guidance signed July 18, 2011

Security Engineering Challenges

- **Incorporation of security engineering as a discipline of systems engineering**
  - Engineering methodology, processes, and practices
  - System security engineering workforce
- **Quantification of security risks**
  - Vulnerability detection, and validated mitigation
- **Articulation of security requirements**
  - Threat-driven, evolving over time
  - Risk-based affordable trade off analysis; Measurable, testable system specifications
- **Protection of technical data**
  - Consequences of unclassified controlled technical information losses
  - Government and Industry mitigation of supply chain exploitation

Major Actions Underway

- **Updating Program Protection guidance and training**
  - Establishing a discipline for system security engineering
- **Implementing DFARS Clause 252.204-7012, "Safeguarding Unclassified Controlled Technical Information"**
  - Working with industry and contracting community
  - Providing guidance, working through procedures
- **Joint Federated Assurance Center for HW/SW**
  - Required by Section 937 of FY14 NDAA
  - Provides network of vulnerability analysis detection and mitigation support to programs; and R&D improvement (resource limited)
- **Trusted microelectronics strategy to move beyond ASICs**
  - FPGAs, Microprocessors, Logic Application Specific Standard Products, Memories, A-D Converters, Interface Chips
- **Anti-Tamper Policy and Guidance updates**
  - DoD Instruction for AT, AT Technology oversight, guidance updates

System Security Engineering

- **Industry plays an important role:**
  - Integrating SSE into SE methods, processes and tools
  - Investing in research, tools, and processes to protect systems and supply chains
  - Developing flexible security architectures for designed-in protections
  - Developing and applying SE and SSE skills (anti-tamper, cybersecurity, supply chain, software assurance, …)
  - Developing SSE metrics
- **Together we can begin to address the challenges and move toward a shared goal of delivering trusted systems**

Thank you to our hosts and attendees for supporting this Program Protection Summit and Workshop

Questions