Space and Missile Systems Center

SMC Initiatives

NASA Electronic Parts and Packaging Program (NEPP) Electronics Technology Workshop

28 Jun 2017

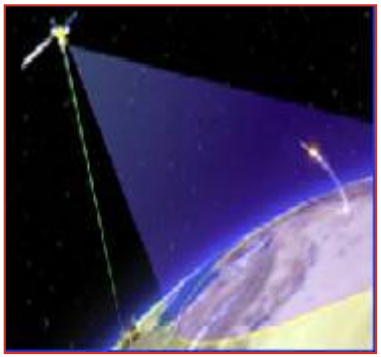
David Davis

SMC Chief Systems Engineer

SMC & PEO/Space Mission Overview

SPACE AND MISSILE SYSTEMS CENTER

WE DEVELOP, ACQUIRE, FIELD AND SUSTAIN SYSTEMS IN FOUR MAJOR MISSION AREAS



Space Superiority

Space Situation Awareness
- SBSS
- Space Fence

Defensive Counter Space
Offensive Counter Space

Space Support

Launch Systems
Spacelift Range
Sat Control & Network

Force Application

Conventional Missiles
Prompt Global Strike

Space Force Enhancement

Milstar/AEHF/EPS
DSCS/GBS/WGS
GPS
DSP/SBIRS
DMSP
NDS (Nuclear Detection)

Developing, Delivering, and Supporting Military Space and Missile Capabilities to Preserve Peace and Win Conflicts

Space System Development

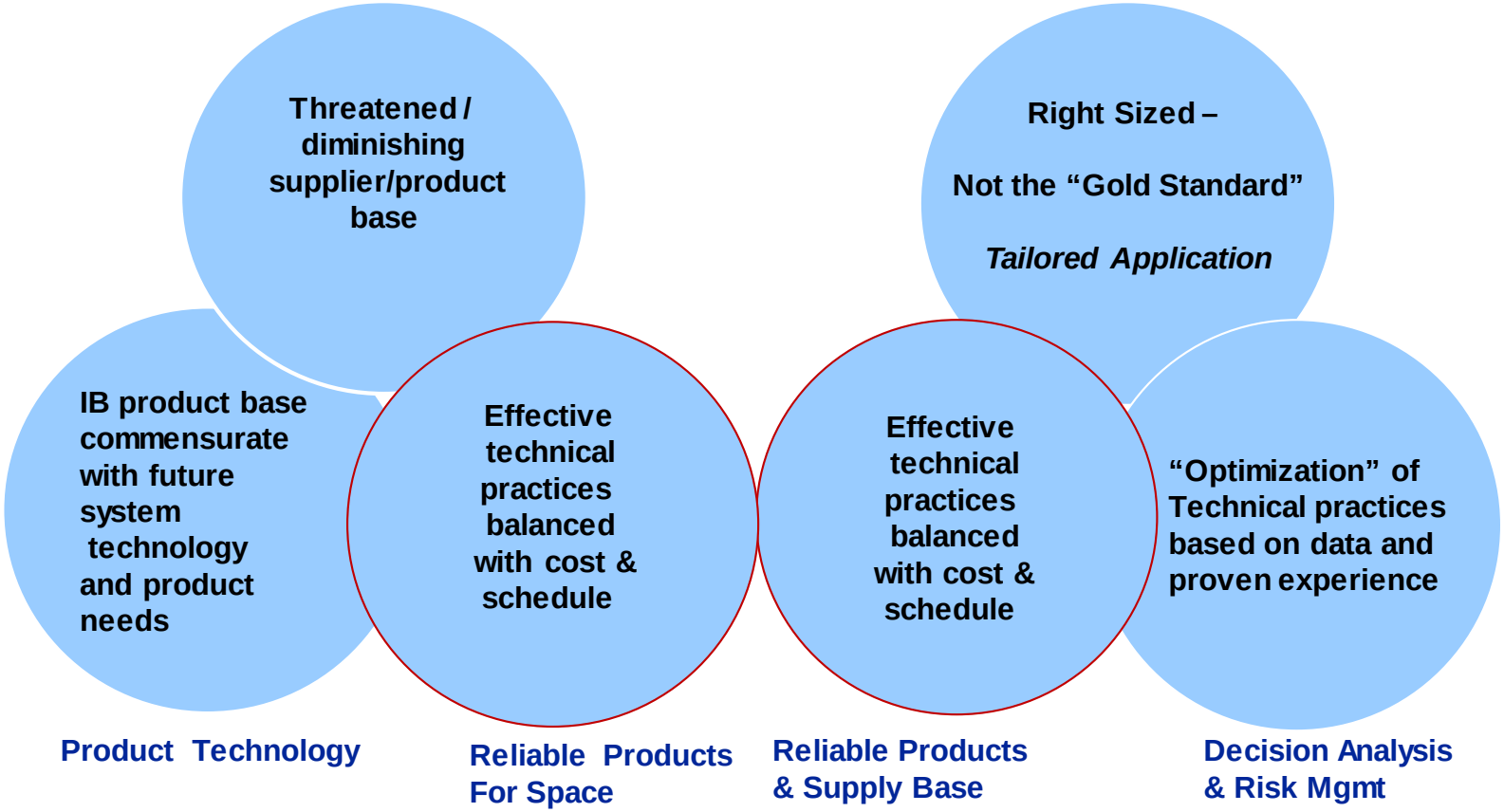
- Launch is a "one-strike-and-you're-out" business
- Spacecraft must work by remote control for 15 years
  - Hostile environment
  - "Small" failures can cripple or end mission
  - No Beta Testing/LRIP and No On-Orbit Repair
  - Mandates Unique, High-Confidence Mission Assurance Culture

No "flight Testing" and No Service Calls in Space Mandates Unique, High-Confidence Mission Assurance Culture

Balancing the Needs for Space Acquisition

Space Industrial Base

Specs & Standards



Must Assure Critical Requirements and Industrial Supply Capability Necessary to Support Current and Future USG Space Programs

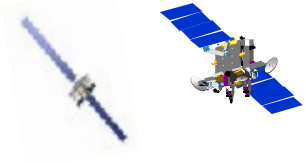
Space and Missile Systems Center

Future NSS Space Programs

SMC Next Generation Programs

- The Changing Space Landscape
  - Evolving and greater threats (contested, congested, competitive)
  - Higher dependency on space systems (both military and commercial)
  - Funding constraints (DoD budgets flat at best)

- Challenges to the Current Architecture
  - Inflexible constellations (hard to maintain and replenish)
  - Lack of Resilience
  - Technology Stagnation and lack of competitive forces
  - Shrinking Industrial Base
  - Rising Cost



- Current architecture does not adequately address these new challenges
- AFSPC developing future resilient/affordable architectures and near-term investment strategies

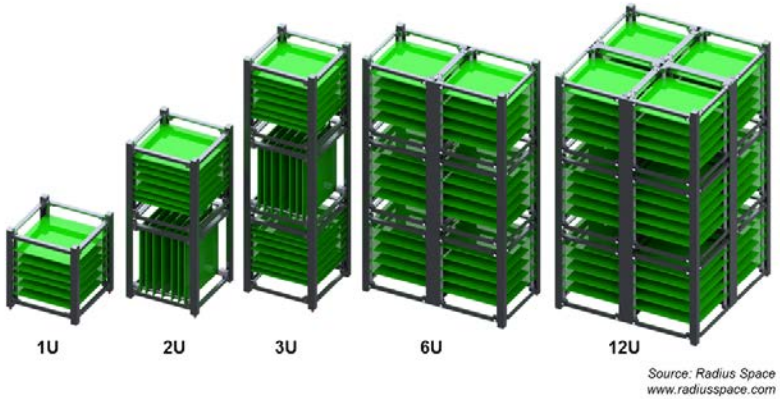
Compelling need for alternative space architecture options

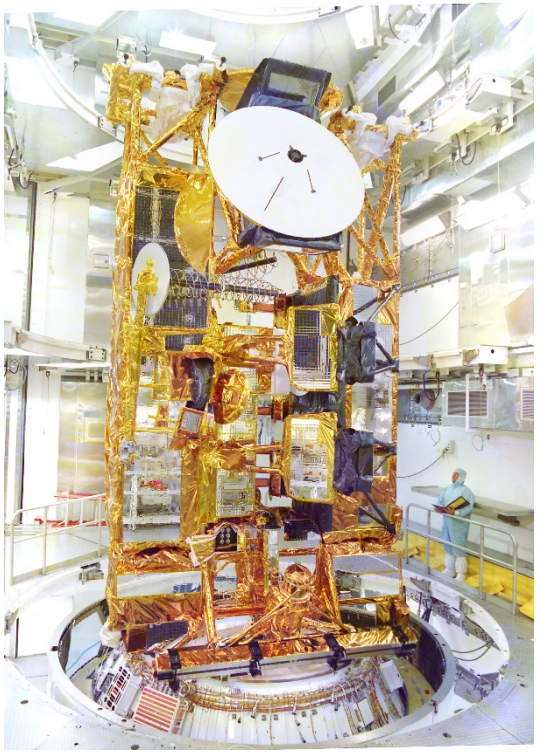
SMC Architecture Studies On-going – Next "Programs of Record" TBD

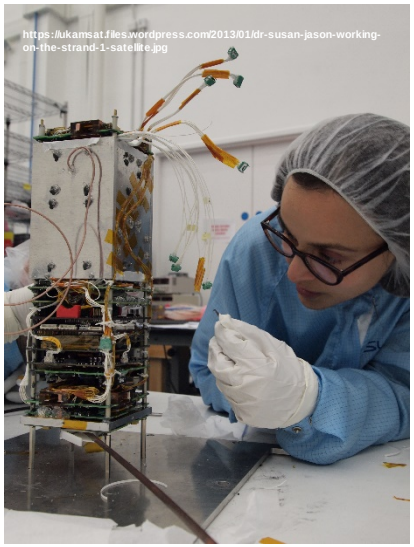
Space Enterprise Vision - Basis of Future Space Systems Architectures

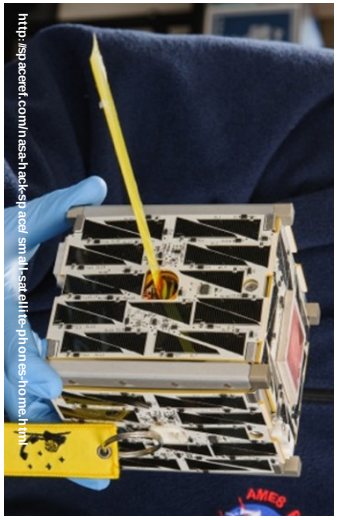
- In 2015, AFSPC/CC Gen Hyten called for a new Space Vision that he still endorses as STRATCOM/CC
  - Gen Raymond, the new AFSPC/CC is also a strong advocate of the new Space Vision
- November 2016, CNN War In Space TV special, highlighted threats that are real today!
- In the past, DoD requirements resulted in designs that focused on long-term functionality and long (15 year) operational lives
  - Time to think about 5 year designs, lower complexity, and block builds
  - Allows us to keep pace with rapidly evolving threats to on-ramp newest improvements, lower launch cost, etc.
- Acquisition processes and development cycles too slow to respond to dynamic threats
  - Pursuing prototypes, seeking new contractual vehicle's, RCOs, ORSs, OTAs, BAAs, Universities etc., adaptation of commercial methods and innovations where possible
  - Disaggregation of strategic and tactical, proliferation, small sats, hosted payloads, etc
- Need to seriously pursue enterprise solutions and how multiple systems, integrated together, could be more resilient than individual systems going it alone
  - Must learn to more synergistically operate as an enterprise, not just as independent platforms

Nano, Cube, Small…….Sats









Testing Foundation/Principles

- High reliability required of all launch and space equipment achieved by the designs, design margins, and by the manufacturing process controls imposed at each and every level of assembly
  - Design & design margins assure equipment capable of performing in launch and space environment.
  - Manufacturing process controls intended to assure a quality product is manufactured that meets design requirements - any changes required made based on a known baseline
- Qualification tests conducted to demonstrate that the design, manufacturing process, and acceptance program produce mission items that meet specification requirements
  - In addition, the qualification tests will validate the planned acceptance program including test techniques, procedures, equipment, instrumentation, and software.
- Qualification Hardware subjected to qual testing will be produced from the same drawings, using the same materials, tooling, manufacturing process, and level of personnel competency as used for flight hardware.
- Acceptance tests conducted to demonstrate the acceptability of each deliverable item
  - Tests demonstrate conformance to specification requirements and provide quality-control assurance against workmanship or material deficiencies.
  - Acceptance testing is intended to stress screen items to precipitate incipient failures due to latent defects in parts, materials, and workmanship.

Testing Foundation/Principles

- **Rationale for Retest**
  - Retest is the repeat of previously conducted tests due to a redesign, a change in a manufacturing process, a test discrepancy, an increase in flight environments, or rework of items previously tested
    - Minor changes in design, manufacturing processes, flight environments, or rework can have a significant effect on the reliability of flight hardware
  - Requalification After Redesign – verification that design modifications have not introduced unpredictable failure mechanisms in the hardware
  - Requalification After Process Change - assurance that new process has not had a deleterious effect on the capability or reliability of the hardware
    - Assure that unpredictable changes have not been induced in manufactured hardware
- **Piece Part Production Lot**
  - A production lot of parts refers to a group of parts of a single part type; defined by a single design and part number; produced in a single production run by means of the same production processes, the same tools and machinery, same raw material, and the same manufacturing and quality controls.
  - All parts in the same lot have the same lot date code, batch number, or equivalent identification.

Foundational Principles Will Need To Be Adapted For Future Systems

SMC Standard SMC-S-011

31 July 2015

Supersedes:
SMC-S-011 (2008)

SPACE AND MISSILE SYSTEMS CENTER STANDARD

PARTS, MATERIALS, AND PROCESSES CONTROL PROGRAM FOR LAUNCH VEHICLES

SMC 011 Parts Selection

- **Mission critical Component**
  - System/circuit performing a function required to meet the mission objectives or flight safety requirements, regardless of redundancy or implementation scheme
- **ELV Space PMP Baseline required for Category I**
  - Category I - Mission Critical & Single String or Mission Critical & Single point Failure
- **Program PMP Baseline allowable for Category II**
  - Category II - Mission Critical and Redundant
  - Selection based on WCCA, Worst Case Derating, Redundancy, Mission reliability, Survivability
    - Prescribed part screening and class selection no longer required
    - Knowledge of manufacturer part control, technology, & failure modes
  - Baseline established by Contractor and approved by Parts, Materials, & Processes Control Authority (PMPCA)
- **Non Mission Critical Applications**
  - Do no harm analysis

Use of Automotive Parts

- **Objective:**
  - **Understand how suppliers implement their automotive product line in accordance with the AECQ100 requirements to include design, wafer fab, probe, assembly and test**
  - **Understand of qualification and process controls implementation to assure reliability and minimize lot to lot variations**

Improving Mission Success of CubeSats

Planned publication date for this product is Sept 2017

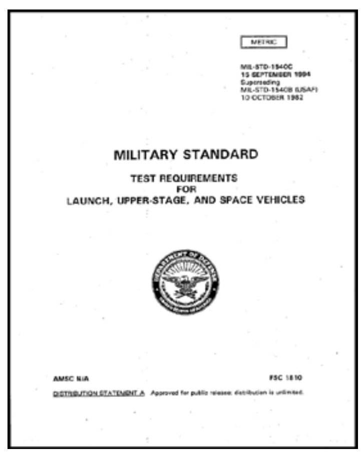
Product will be essentially a Best Practices Guide

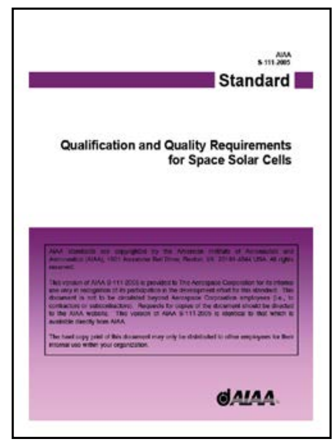
SMC Specifications & Standards Program

SMC Compliance Standards List

SPACE AND MISSILE SYSTEMS CENTER

- SMC Technical Baseline
  - 69 documents
- Includes all four space system segments
  - Military (MIL-STD)
  - International (ISO)
  - Industry (AIAA, IEEE, SAE, etc))
  - SMC Standards
- Reflects current best practices
- Updated periodically
- SMC Instruction 63-106, 31 July 15
- Applies to all new development, acquisition and sustainment contracts
- Contractual compliance through the supplier chain, as appropriate





Functional Areas of SMC Standards

Standard Practices

- Program/Subcontract Management
- Systems Engineering
- Architecture Development
- Design Reviews
- Configuration Management
- Quality Assurance
- Logistics
- Manufacturing /Production Management
- Parts Management (non-space)
- Parts Management (space)
- Risk Management
- System Safety
- Occupational Safety and Health
- Reliability/Availability

Subsystem/Component Standards

- Electrical Power, Batteries
- Electrical Power, Solar Cells/Panels
- Electromagnetic Interference & Control
- Environmental Engineering; Cleanliness
- Human Systems Integration
- Interoperability
- Maintainability
- Mass Properties
- Moving Mechanical Assemblies
- Ordnance
- Pressurized Systems & Components
- Information Assurance/Program Protection
- Software Development
- Structures
- Survivability
- Test, Space & Ground

➢ *Industry consensus standards developed or adopted for use on SMC contracts*

S.2943 - National Defense Authorization Act for Fiscal Year 2017

- SEC. 875. Use of commercial or non-Government standards in lieu of military specifications and standards.
  - (a) In general.—The Secretary of Defense shall ensure that the Department of Defense uses commercial or non-Government specifications and standards in lieu of military specifications and standards, including for procuring new systems, major modifications, upgrades to current systems, non-developmental and commercial items, and programs in all acquisition categories, unless no practical alternative exists to meet user needs. If it is not practicable to use a commercial or non-Government standard, a Government-unique specification may be used.
  - (b) Limited use of military specifications.
- (1) IN GENERAL.—Military specifications shall be used in procurements only to define an exact design solution when there is no acceptable commercial or non-Government standard or when the use of a commercial or non-Government standard is not cost effective.
- (2) WAIVER.—A waiver for the use of military specifications in accordance with paragraph (1) shall be approved by either the appropriate milestone decision authority, the appropriate service acquisition executive, or the Under Secretary of Defense for Acquisition, Technology, and Logistics.
- (c) Revision to DFARS.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall revise the Defense Federal Acquisition Regulation Supplement to encourage contractors to propose commercial or non-Government standards and industry-wide practices that meet the intent of the military specifications and standards.
- (d) Development of non-government standards.—The Under Secretary for Acquisition, Technology, and Logistics shall form partnerships with appropriate industry associations to develop commercial or non-Government standards for replacement of military specifications and standards where practicable.

Long-Term Strategy for DoD Trusted Foundry Needs

Cybersecurity / Supply Chain Risk Management (SCRM)

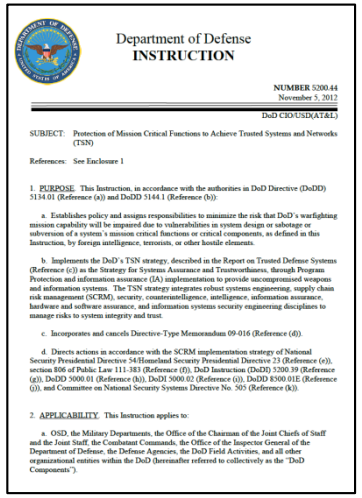
Kristen J. Baldwin
Principal Deputy
Office of the Deputy Assistant Secretary of Defense for Systems Engineering, OUSD(AT&L)

Trusted/Cyber/SCRM Policy

Trusted Systems and Networks (TSN)

- **DoDI 5200.44, August 25, 2016**
  Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

Strategy for Systems Assurance and Trustworthiness, through Program Protection and cybersecurity implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust."



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)).

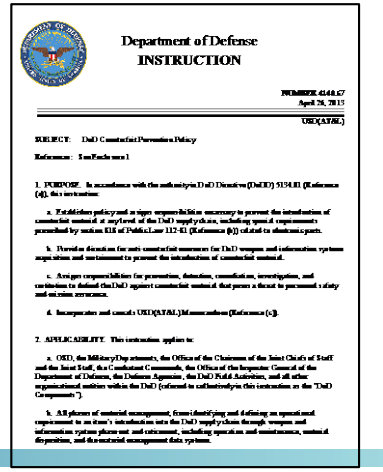
2. APPLICABILITY. This Instruction applies to:

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").

Counterfeit Prevention

- **DoDI 4140.67, April 26, 2013**
  DoD Counterfeit Prevention Policy

"Establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit materiel at any level of the DoD supply chain"



Department of Defense
INSTRUCTION

NUMBER 4140.67
April 26, 2013

USD(AT&L)

SUBJECT: DoD Counterfeit Prevention Policy

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5134.01 (Reference (a)), this instruction:

a. Establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit material at any level of the DoD supply chain, including special requirements prescribed by section 818 of Public Law 112-81 (Reference (b)) related to electronic parts.

b. Provides direction for anti-counterfeit measures for DoD weapons and information systems acquisition and sustainment to prevent the introduction of counterfeit material.

c. Assigns responsibilities for prevention, detection, remediation, investigation, and restitution to defend the DoD against counterfeit material that poses a threat to personnel safety and mission assurance.

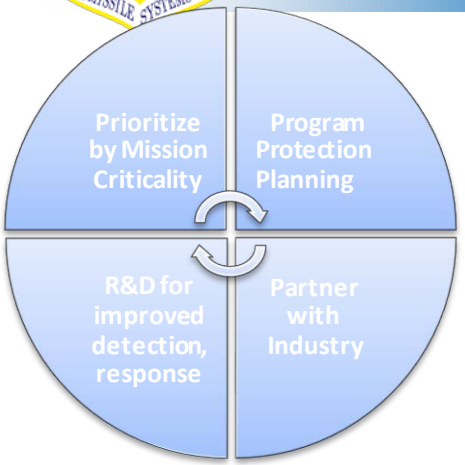
d. Incorporates and cancels USD(AT&L) Memorandum (Reference (c)).

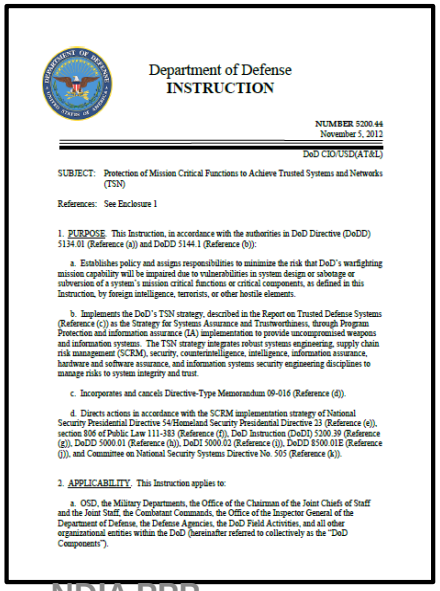
2. APPLICABILITY. This instruction applies to:

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 (referred to collectively in this instruction as the "DoD Components").

b. All phases of material management, from identifying and defining an operational requirement to an item's introduction into the DoD supply chain through weapon and information system phase out and retirement, including operation and maintenance, material disposition, and the material management data systems.

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**

Spectrum of Supply Chain Risks

SPACE AND MISSILE SYSTEMS CENTER

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.

Reverse Engineering

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.

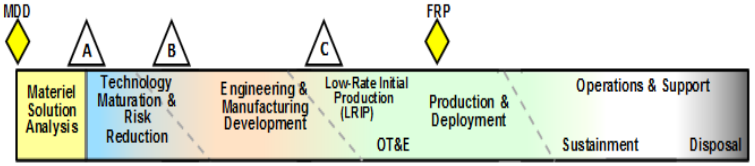
DoD Program Protection focuses on risks posed by malicious actors

Ensuring Confidence in Defense Systems

SPACE AND MISSILE SYSTEMS CENTER

- ***Threat:***
  - Adversary who seeks to exploit vulnerabilities to:
    - Acquire program and system information
    - Disrupt or degrade system performance
    - Obtain or alter US capability
- ***Vulnerabilities:***
  - All systems, networks and applications
  - Intentionally implanted logic (HW/SW)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
  - Controlled defense information resident on, or transiting supply chain networks
  - Loss or sale of US capability that provides a technological advantage
- ***Consequences:***
  - Loss of data; system corruption
  - Loss of confidence in critical warfighting capability; mission impact
  - Loss of US capability that provides a technological advantage

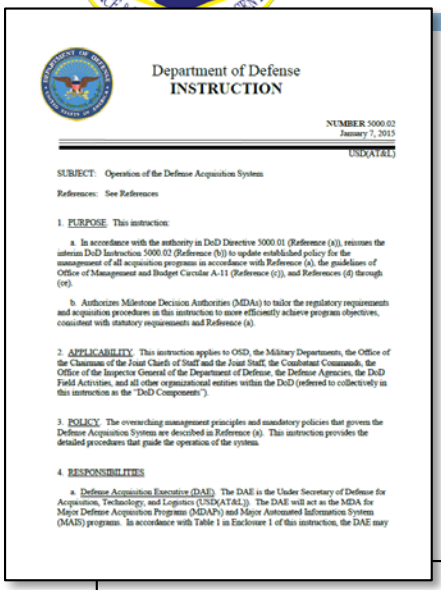
Access points are throughout the acquisition life cycle…



…and across numerous supply chain entry points

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

Program Protection Planning Policy



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).

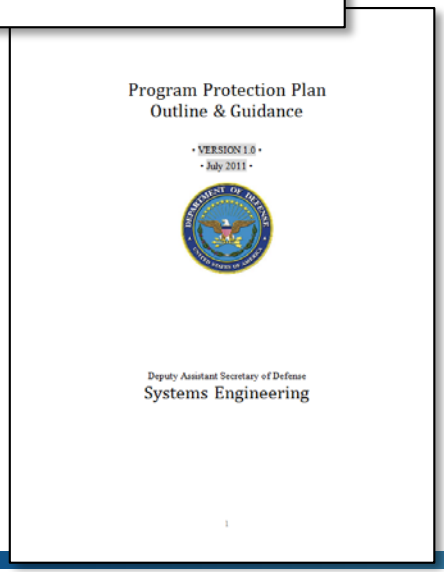
b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

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

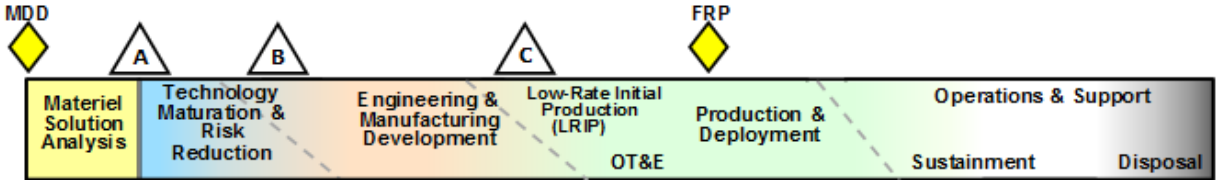


Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

- System Security Engineering is accomplished in the DoD through program protection planning (PPP)
- DoDI 5000.02 requires program managers to employ system security engineering practices and prepare a Program Protection Plan to manage the security risks to critical program information, mission-critical functions and information
- Program managers will describe in their PPP:
  - Critical Program Information, mission-critical functions and critical components, and information security threats and vulnerabilities
  - Plans to apply countermeasures to mitigate associated risks:
    - Supply Chain Risk Management
    - Hardware and software assurance
  - Plans for exportability and potential foreign involvement
  - The Cybersecurity Strategy and Anti-Tamper plan are included



Summary

- **Support evolving new architectures - SEV**
  - **Affordable and resilient**
- **Establish appropriate acquisition and mission assurance practices consistent with the program resiliency strategy/risk**
  - **Acquisition processes and development cycles which are more responsive to dynamic threats**
  - **Program Cost Models**
- **Establish practices and mitigation expectations for System Security Engineering / Trust/ SCRM**
  - **Trust, anti-tamper, cybersecurity, supply chain, software assurance, etc**

Thank You