Policy Perspective: The Current and Proposed Security Framework

Ms. Kristen Baldwin, DASD(SE)

August 16, 2016

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Outline

- **Design as critical method to addressing trust/assurance**
- **We have a new strategy**
  - Need access to state of the art while maintaining an acceptable level of risk
  - Concerned with historical reliance upon a single trusted foundry
  - Long-term strategy for leveraging JFAC and new assurance technology
  - We want to maintain U.S. tech edge in this technology
- **Areas to address**
  - Policy
  - Standards – we see trust and assurance as a competitive advantage
  - Future technologies
- **Questions**

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Spectrum of Supply Chain Risks

Quality Escape	Reliability Failure	Fraudulent Product	Malicious Insertion	Reverse Engineering	Information Losses
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.	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.	Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.	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.	Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.	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.

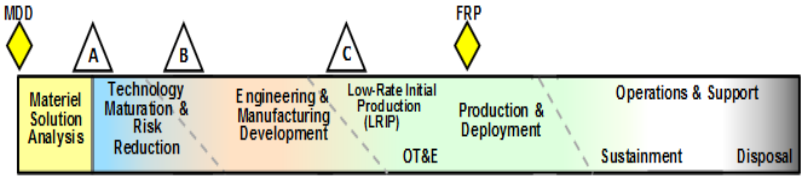
DoD Program Protection focuses on risks posed by malicious actors

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Ensuring Confidence in Defense Systems

- ***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…

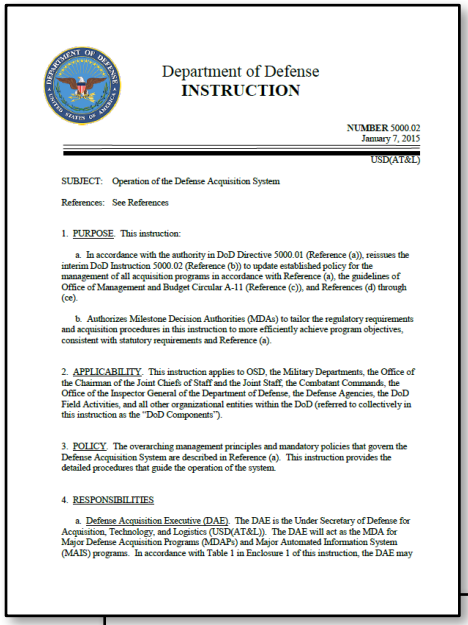


…and across numerous supply chain entry points

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

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

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).

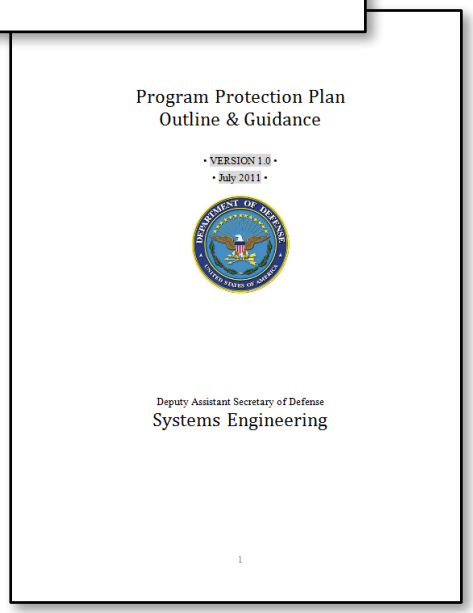
b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

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



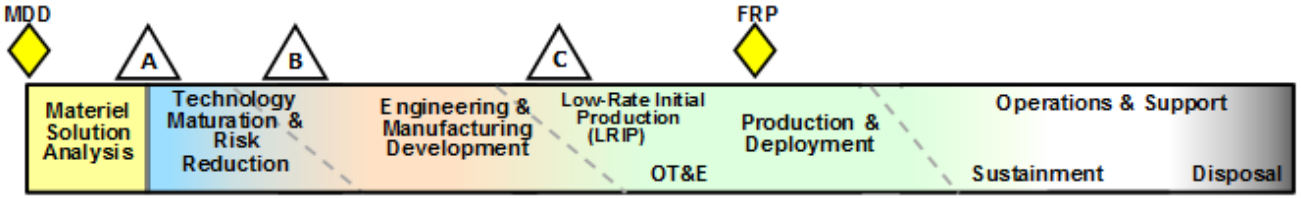
Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

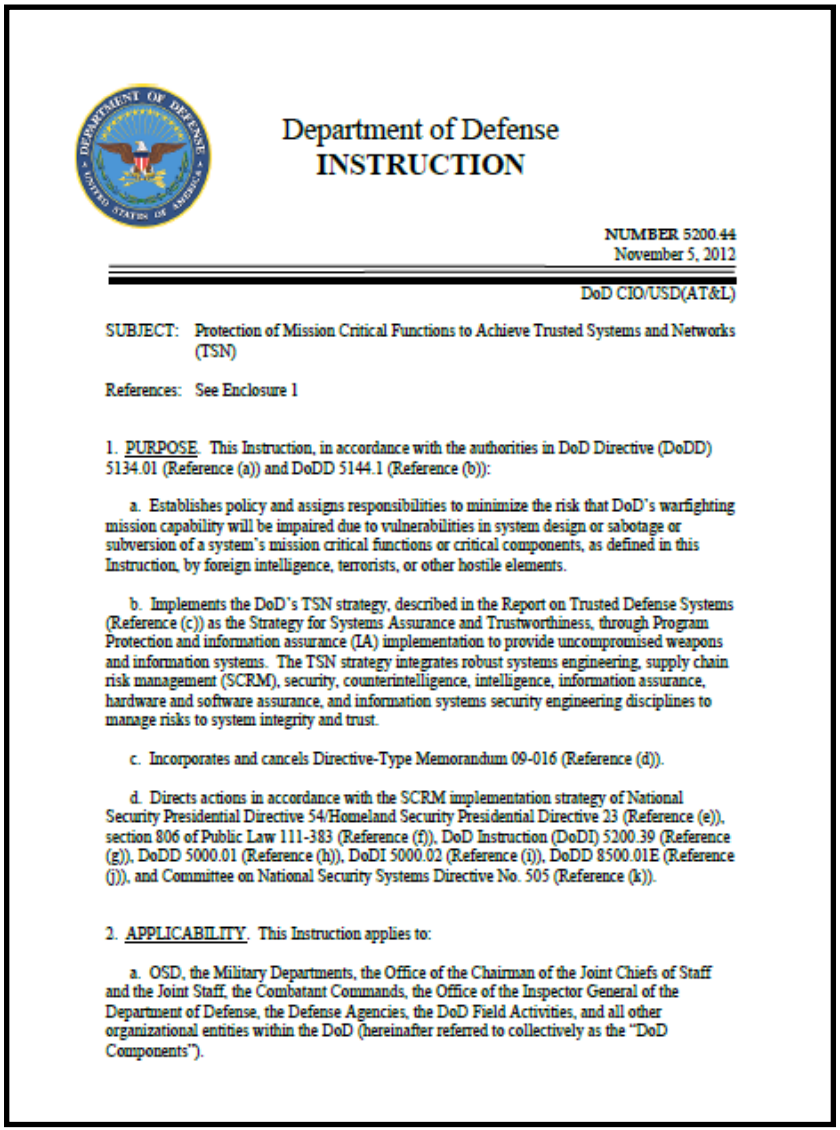
1

- **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



Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Trusted Systems and Networks DoD Instruction 5200.44



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**

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Joint Federated Assurance Center

- **JFAC is a federation of DoD software and hardware assurance (SwA/HwA) capabilities and capacities**
  - To support programs in addressing current and emerging threats and vulnerabilities
  - To facilitate collaboration across the Department and throughout the lifecycle of acquisition programs
  - To maximize use of available resources
  - To assess and recommend capability and capacity gaps to resource
- **Innovation of SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques to mitigate risk of malicious insertion**
  - R&D is key component of JFAC operations
  - Focus on improving tools, techniques, and procedures for SwA and HwA to support programs
- **Federated Organizations**
  - Army, Navy, AF, NSA, DMEA DISA, NRO, MDA laboratories and engineering support organizations; Intelligence Community and Department of Energy

The mission of JFAC is to support programs with SwA and HwA needs

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Trusted Microelectronics Suppliers (e.g. Trusted Foundry)

- **The Defense Microelectronics Activity (DMEA) certifies trusted suppliers for DoD-unique microelectronic designs (e.g. ASIC chips)**
  - There are over 70 trusted suppliers certified by DMEA
- **The IBM Trusted Foundry contract provided microelectronics trust and access for 11+ years to many DoD, intelligence and NASA programs**
  - Broad use by acquisition and technology programs, and special capabilities
  - The IBM TF produced state-of-the-art technology nodes; some of which were IBM-unique
- **GlobalFoundries (GF) acquired IBM's foundry operations in July 2015**
  - In March 2016, DoD awarded a new contract with GF to retain access to the two foundries that provided DoD trusted microelectronics parts
  - **DoD programs are advised to execute life-time buys (LTBs) of production-ready parts while GF Trusted Foundry is available**
- **DoD has established a program to address long term trusted access to microelectronics**
  - Provide an alternative trust model and eliminate reliance on sole source foundries
  - New approach will consist of secure microelectronics design and packaging technologies that protect CPI, provide assurance and trusted chain of custody
  - **DoD programs and industry partners are being identified for piloting and transition of the new trust model**

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Long-Term Strategy Time Line

DoD Trusted Foundry Program Consolidation - Defense Microelectronics Activity (DMEA)

Transition → Newly Established Trusted Foundry Contract

Sustained Network of Trusted Certified Suppliers

Trusted and Assured Microelectronics Program:

Alternate Source for Trusted Photomasks

Preparation activities → Capability Development → Deploy new capability

Verification and Validation (V&V) Capabilities and Standards for Trust

Preparation activities → Improve capabilities and capacity, and provide support to program needs, for analysis of microelectronics trust

Identify and develop standards, practices, and partnerships to improve availability of trust from commercial providers

Advanced Technology and Alternative Techniques for Microelectronics Hardware Trust

Preparation activities → Capability development and demonstration → Deploy new capabilities

2015 2016 2017 2018 2019 2020 2021 2020 2023 2024

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Long Term Trusted Foundry Strategy

Supports activities to ensure critical and sensitive integrated circuits are available to meet DoD needs

Program goals:

- Protect microelectronic designs and intellectual property (IP) from espionage and manipulation
- Advance DoD hardware analysis capability and commercial design standards, e.g., physical, functional, and design verification and validation
- Mature and transition new microelectronics trust model that leverages commercial state-of-the-art (SOTA) capabilities and ensures future access

Technical challenges:

- Develop alternate trusted photomask capability to preserve long-term trusted access and protection of IP
- Scale/enhance the government's ability to detect security flaws in integrated circuits
- Leverage academic and industry research for assuring trust from any supplier

Program partners:

- DoD science & technology (S&T), acquisition communities, academia, industry

Provides technical solutions that can be leveraged by government and industry to enable microelectronics trust

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Teaming and Partnerships are Key to Success

Many stakeholders are involved in the success of the long-term strategy:

- Leadership from OSD, Services, Agencies
- Performers including NSWC Crane, DMEA, DARPA, and other DoD S&T organizations and laboratories
- Integration and support of functions of:
  - DoD Trusted Foundry Program
  - DMEA Trusted Supplier Accreditation Program
  - Joint Federated Assurance Center
  - Microelectronics trust S&T and transition activities
- Building and leveraging partnerships with Defense and commercial industry and academia
- Coordination with other U.S. Government agency partners

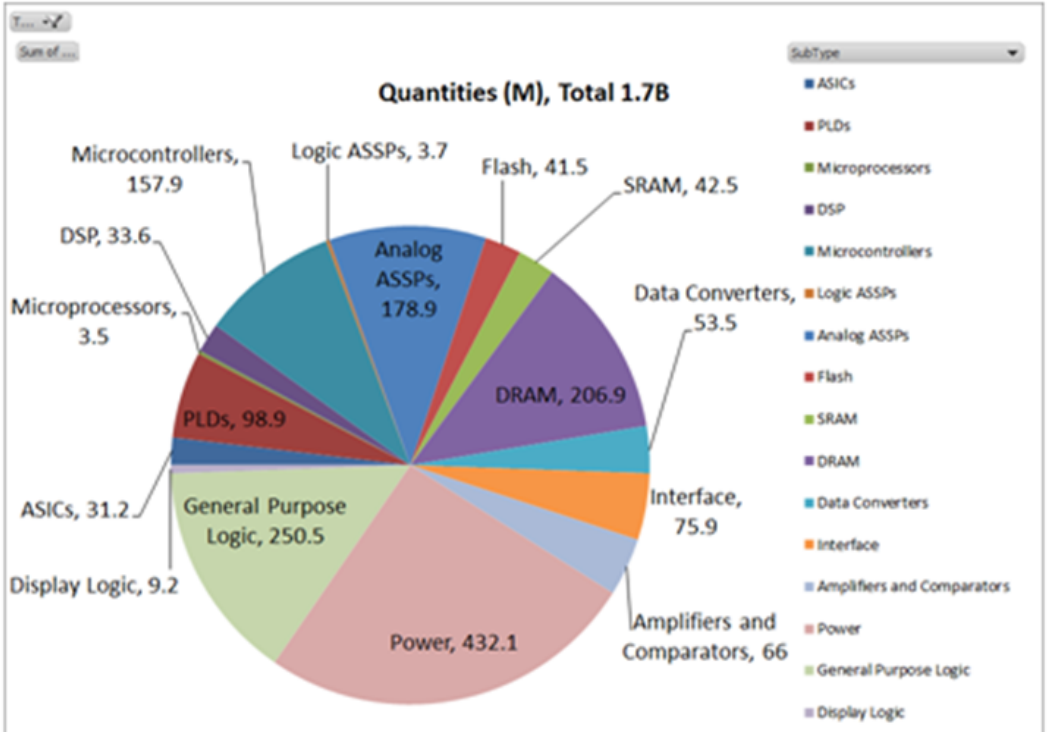
Bottom line – structuring activities to meet acquisition program needs for trust and access to state of the art microelectronics

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Trusted Microelectronics

- **Application Specific Integrated Circuit policy: DoD end use ASICs can only be procured from a DMEA accredited Trusted supplier**
  - Accounts for <2% of the 1.9B ICs DoD acquires per year
  - No trusted supply chain for other than custom ASICs exists
  - In general order of interest for trust: ASICs, FPGAs, Microprocessors, Logic Application Specific Standard Products, Memories, A-D Converters, Interface Chips

- **What is needed:**
  - A risk-based process for identification and prioritization of all critical ICs to address risk mitigation across life-cycle
  - More effective and affordable risk mitigation countermeasures for ICs
  - Continued collaboration between Government, Industry, and academia



Source: Institute for Defense Analysis

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Assurance Strategy for FPGAs

- **FY 2016 goals for this effort:**
  - Produce a coherent, focused strategy/plan for FPGA assurance
    - Leverage existing USG and industry efforts to the maximum extent possible
    - Promote community awareness of related USG efforts via a series of workshops and conference calls sponsored by OASD(R&E), in coordination with the JFAC, NSA and SNL
    - As a community, identify the portfolio of related efforts on which we should focus with the goal of synchronizing and eliminating stove-pipes and separate, single-point solutions when possible
    - Identify gaps and/or activities requiring investment and elevate relevant needs to the Joint Federated Assurance Center (JFAC) Steering Committee (SC) for prioritization and direction regarding resourcing
      - In particular, align with, and inform, the FY 2017 execution plan for the Trusted Foundry Program Element (PE)

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

The Way Ahead

- **Program engagement**
  - Foster early planning for HwA and SwA, design with security in mind
  - Implement expectations in plans and on contract
  - Support vulnerability analysis and mitigation needs
- **Community collaboration**
  - Achieve a networked capability to support DoD needs: shared practices, knowledgeable experts, and facilities to address malicious supply chain risk
- **Industry engagement**
  - Communicate strategy to tool developers
  - Develop standards for common articulation of vulnerabilities and weaknesses, capabilities and countermeasures
- **Advocate for R&D**
  - HwA and SwA tools and practices
  - Strategy for trusted microelectronics that evolves with the commercial sector
- **People!**
  - Improve awareness, expertise to design and deliver trusted systems

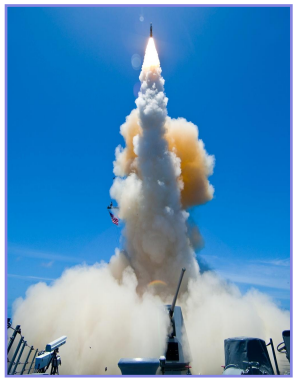
Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

BACKUPS

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

Twitter: @DoDInnovation

Distribution Statement A – Approved for public release by DOPSR; SR# 15-S-1541 applies. Distribution is unlimited.