Driving Technical Excellence into Programs

Raytheon Systems Engineering and Software Symposium

March 29, 2006

Mark D. Schaeffer

Acting Director, Defense Systems
Director, Systems Engineering

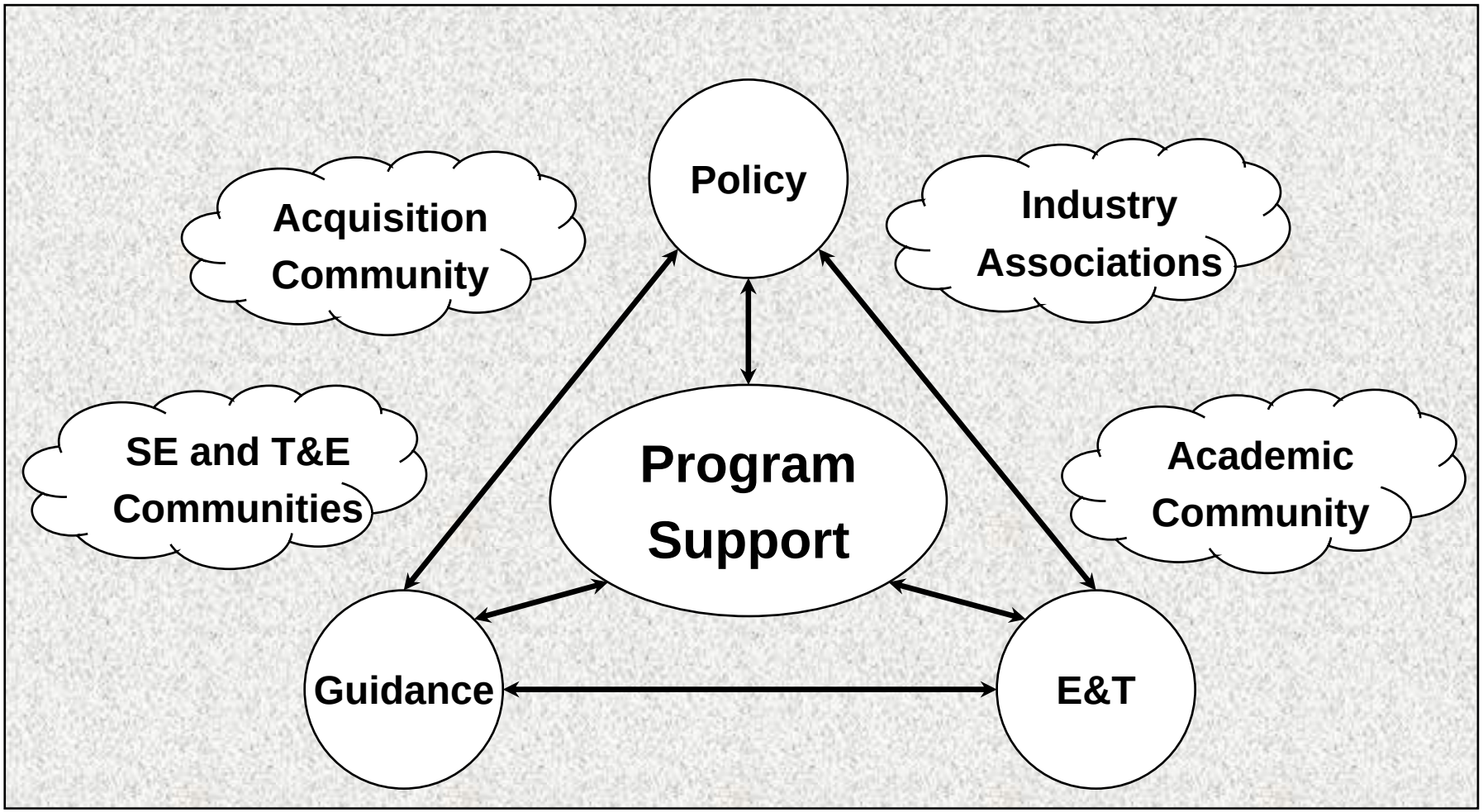
Office of the Under Secretary of Defense (AT&L)

What We Have Done To Revitalize Systems Engineering

- Established SE Forum—senior-level focus within DoD
- Issued Systems Engineering (SE) policy
- Issued guidance on SE and Test & Evaluation (T&E), integrating Developmental T&E with SE focused on effective, early engagement of both
- Instituted system-level assessments in support of OSD major acquisition program oversight role
- Working with Defense Acquisition University to revise SE, T&E, and enabling career fields curricula
- Leveraging close working relationships with industry and academia

Necessary but not sufficient!

Systems Engineering Revitalization Framework



Driving Technical Excellence into Programs!

Driving Technical Rigor Back into Programs "Portfolio Challenge"

- Defense Systems was tasked to:
  - Review program's SE Plan (SEP) and T&E Master Plan (TEMP) for major acquisition programs (ACAT ID and IAM)
  - Conduct program support reviews (PSRs)
- Portfolio includes:
  - Business Systems
  - Communication Systems
  - C2ISR Systems
  - Fixed Wing Aircraft
  - Unmanned Systems
  - Rotary Wing Aircraft
  - Land Systems
  - Ships
  - Munitions
  - Missiles

Systems Engineering and T&E Support to Over 150 Major Programs in Ten Domains

Driving Technical Excellence into Programs

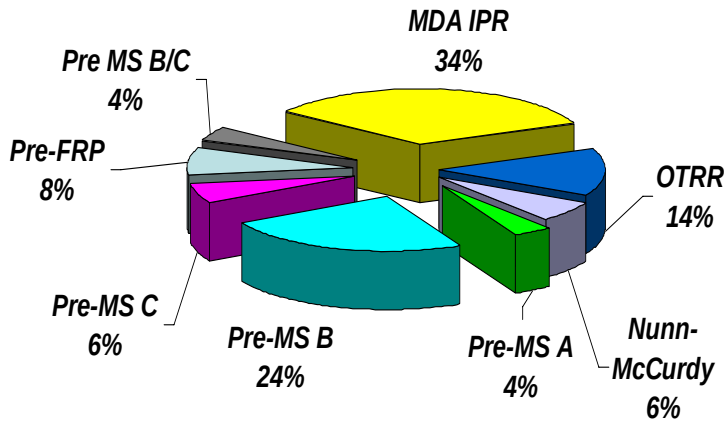
Topic	Systems Engineering	Test & Evaluation	Risk Management	Exit Criteria	Acquisition Strategy
Focus Areas	Requirements	V&V Traceability	Risk ID	Mission Systems	Mission Capability
	Organization & Staffing	Test Resources	Risk Analysis	Support	Resources & Management
	Technical Reviews	Test Articles	Risk Mitigation Planning	Manufacturing	Technical Process
	Technical Baseline	Evaluation	Risk Tracking	R & M	Technical Product
	Linkage w/ Other Program Mgmt & Controls	Linkage w/ Other Program Mgmt & Controls	Evidence of Effectiveness	Net Centric	Enterprise Environment
Product	SEP	TEMP	RM Plan	Phase Exit Criteria	ASR/APB

Examples

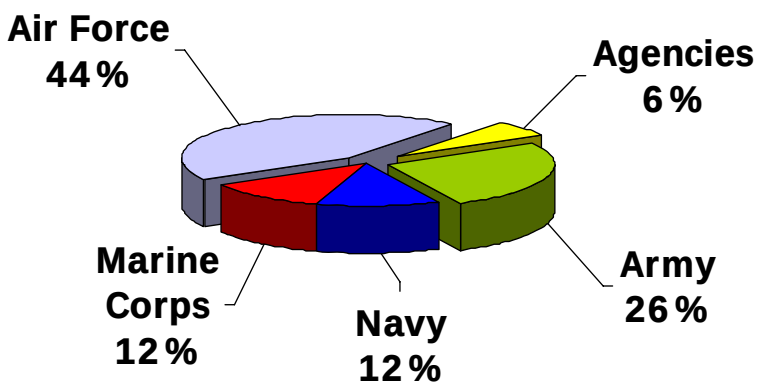
Program Support Review Activity
(since March 2004)

- PSRs/NARs completed: 33
- AOTRs completed: 7
- Nunn-McCurdy Certification: 3
- Participation on Service-led IRTs: 4
- Technical Reviews: 3
- Reviews planned for rest of FY06
  - PSRs/NARs: 12+
  - AOTRs: 2
  - Nunn-McCurdy: 2

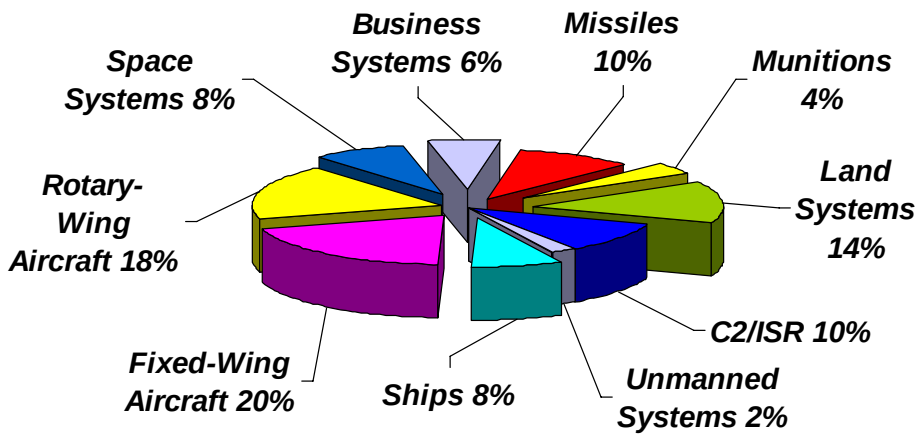
Reviews by Program Event



Service-Managed Acquisitions



Programs by Domain Area



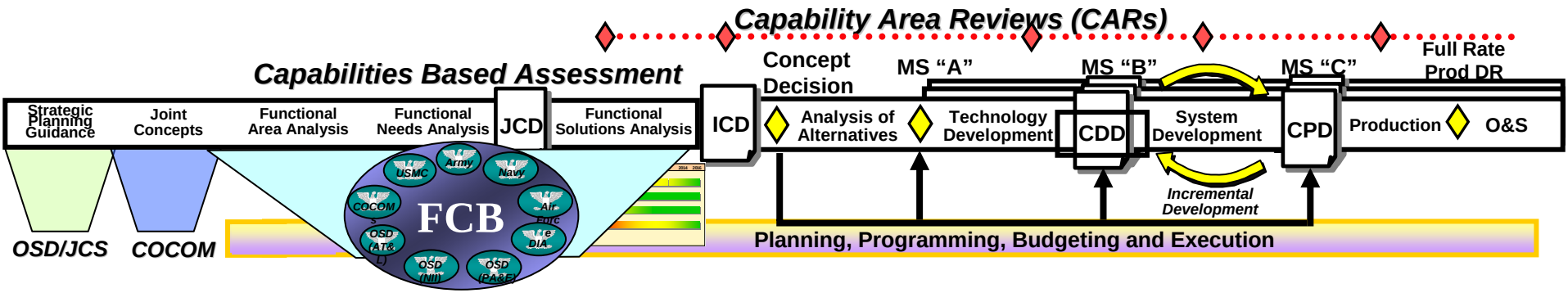
Representative Issues*

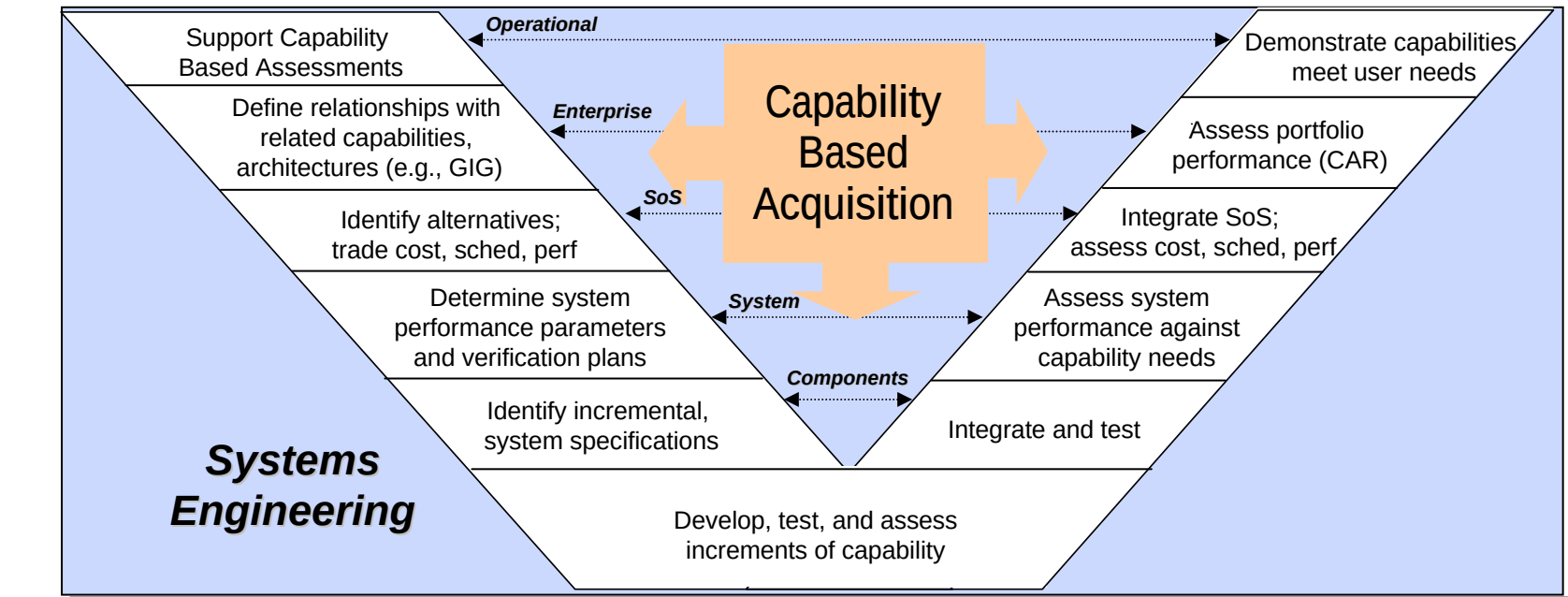
- Program Requirements
  - Changing requirements without coordinating with program manager nor considering dependent program offices
  - Missing Joint CONOPs
  - Poorly addressing Interoperability with Joint Forces
- Event-driven Technical Reviews
  - Missing System Functional Review and Preliminary Design Review during System Development and Demonstration Phase
  - Not conducting Production Readiness Review prior to Low Rate Initial Production decision
  - Missing or poorly defined entry / exit criteria

Compelling Need to Engage with Programs Early in Process

* Based on systemic analysis of 14 PSRs to date

Systems Engineering Engagement

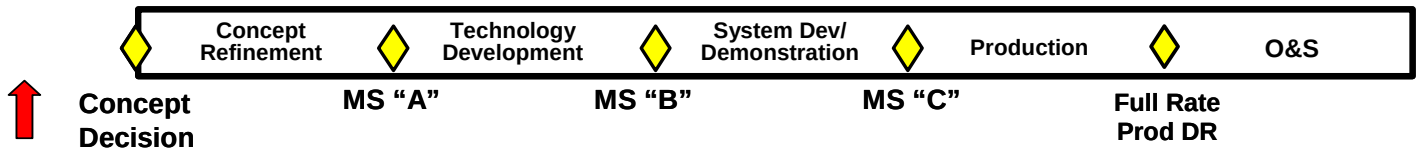




Acquiring Capabilities: What Have We Learned?

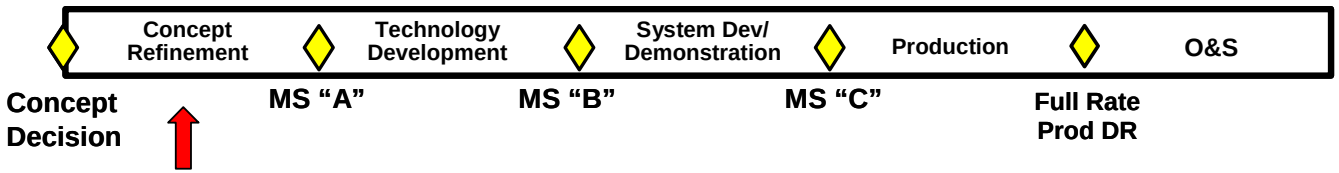
- Early involvement in requirements determination is critical
  - Identify range of solution opportunities
  - Shape key performance parameters based upon analysis of affordability, risk, urgency of need
- Capability needs will be satisfied by groupings of legacy systems, new programs, and technology insertion—systems-of-systems
  - Solutions will cross organizational and funding “stovepipes”
  - Acquisition must focus early (pre-MS B) on integrated design feasibility, full lifecycle considerations, and technology maturity
  - Solutions must integrate with other related capabilities and enterprise architectures (e.g., Global Information Grid)
- Management oversight of capabilities has ripple effects on individual programs
  - Broad context and knowledge of interrelationships are critical to decision-making

Key Knowledge Prior to Concept Decision



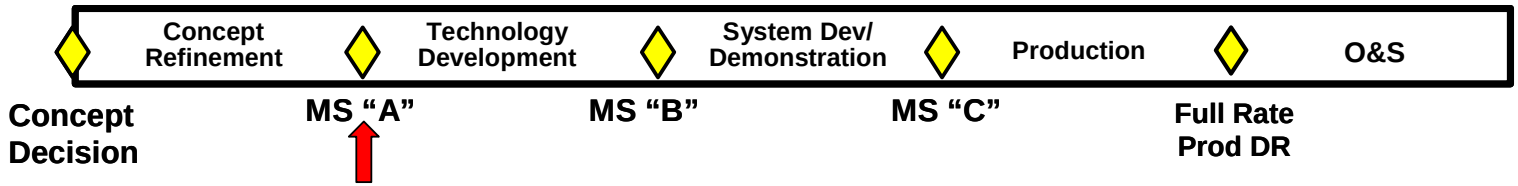
- What is the capability gap?
- What scenarios does the capability affect?
- How does the need fit with within current force structure?
- What is the set of solution options to meet the capability need? (Technology insertion, upgrade, COTS / GOTS, new system / system of systems, non-materiel options)
- What is the design feasibility? (Technology maturity, reliance on other systems / interfaces, has the solution ever been done before)
- Are resources available? Is the solution affordable?
- Which performance parameter is driving the solution?
- What is the best development strategy? (Single development, incremental, combination)

Key Knowledge Prior to Milestone A



- What is the development strategy? (Best design approach)
- What are key interfaces and related systems? Have impacts and relationships been addressed?
- What are the emerging key performance parameters (Trade between cost, time and requirements)
- What is the level of technology maturity? (Where is risk reduction needed, what are options if technology does not mature?)
- What are the acquisition strategy options? (What suppliers exist, incremental steps)
- What is the verification and validation strategy? (Modeling and simulation, incremental testing activity)
- What are the supportability drivers?

Milestone A: Key Decision Criteria



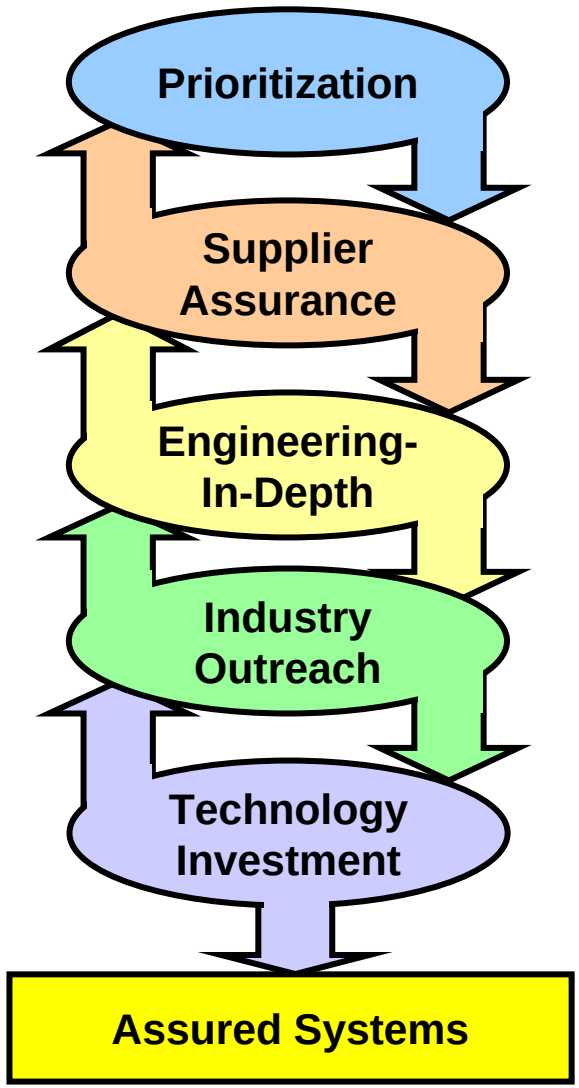
- Requirement is reasonable (Draft KPPs)
- Solutions can be delivered within time and budget constraints
- Strategy addresses impacts to related systems
- Technologies are either mature, or will be demonstrated
- Engineering and test issues have been identified; and activities are in place
- Funding has been budgeted
- Sources of needed development support have been verified

Software Assurance (SwA) Problem

- Scope: Software is fundamental to the GIG and critical to all weapons, business and support systems
- Threat agents: Nation-state, terrorist, criminal, rogue developer who:
  - Gain control of Information Technology, National Security Systems, and Weapon Systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- Vulnerabilities: All Information Technology, National Security, and Weapons Systems (including systems, networks, and applications)
  - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- Consequences: The enemy may steal or alter mission critical data; corrupt or deny the function of mission critical platforms

What Does Success Look Like?

- The requirement for assurance is allocated among the right systems and their critical components
- DoD understands its software supply chain risks
- DoD systems are designed and sustained at a known level of assurance
- Commercial sector shares ownership and builds assured products
- Technology investment transforms the ability to detect and mitigate software vulnerabilities



NDIA System Assurance Committee Charter

- Extend community to engage in system assurance strategy to start bridging the gap between:
  - Weapons systems and the enabling technologies communities
  - Traditional DoD industrial base and commercial industry
  - DoD and critical infrastructure (e.g., telecom, finance, energy, medical)
- Vet and comment on recommendations coming out of DoD strategy
- Develop a System Assurance Handbook
- Leverage standards activities
- Chairs
  - Paul Croll, NDIA SED
  - Kristen Baldwin, OUSD(AT&L)
  - Mitchell Komaroff, OASD(NII)

Government-Industry Handbook on System Assurance

- How do you allocate requirements for assurance
  - Identification of critical components
  - Sensitivity analysis
- Robust design and life cycle considerations
  - How do you engineer for system assurance?
  - Leveraging dependability (reliability, availability, and maintainability)
- Demonstration of Assurance properties
  - Verification and Validation
  - Certification and Accreditation
  - Test and evaluation
- Supporting engineering practices
  - Risk management
  - Configuration management

Identify Opportunities to Enhance Systems Engineering Guidance to Reflect System Assurance Practices

Striving for Technical Excellence

- All programs shall develop a SE Plan (SEP)
- Each PEO shall have a lead or chief systems engineer who monitors SE implementation within program portfolio
- Event-driven technical reviews with entry criteria and independent subject matter expert participation
- OSD shall review program's SEP for major acquisition programs (ACAT ID and IAM)

- Technical planning
- Technical leadership
- Technical execution

Technical excellence

Strong technical foundation is the value of systems engineering to the program manager

Way Ahead for Systems Engineering…

- OSD's fundamental role is to set policy, provide relevant and effective education and training, and foster communication throughout the community—much has been accomplished

- OSD cannot do everything…nor should we

- Services, Agencies, and Industry must take ownership of the institutionalization of Systems Engineering across all programs—ACAT I to ACAT IV

… It's Beginning!