Net Centric Information Environment – Transcending Force Development

Presented to:

NDIA Net Centric Operations Conference
Norfolk, VA
March 6, 2007

Kristen Baldwin
Deputy Director, Software Engineering & System Assurance
OUSD(AT&L)

Outline

- How Net Centric Information applies to Force Development
  - The problem, and a proposed solution framework
- Building Net Centric Solutions:
  - Complex, integrated, Systems of Systems
- Net Centric Enablers (areas that need attention)
  - Integrated Management Information
  - Systems of Systems
  - Software Engineering
  - System Assurance

The Force Development Problem

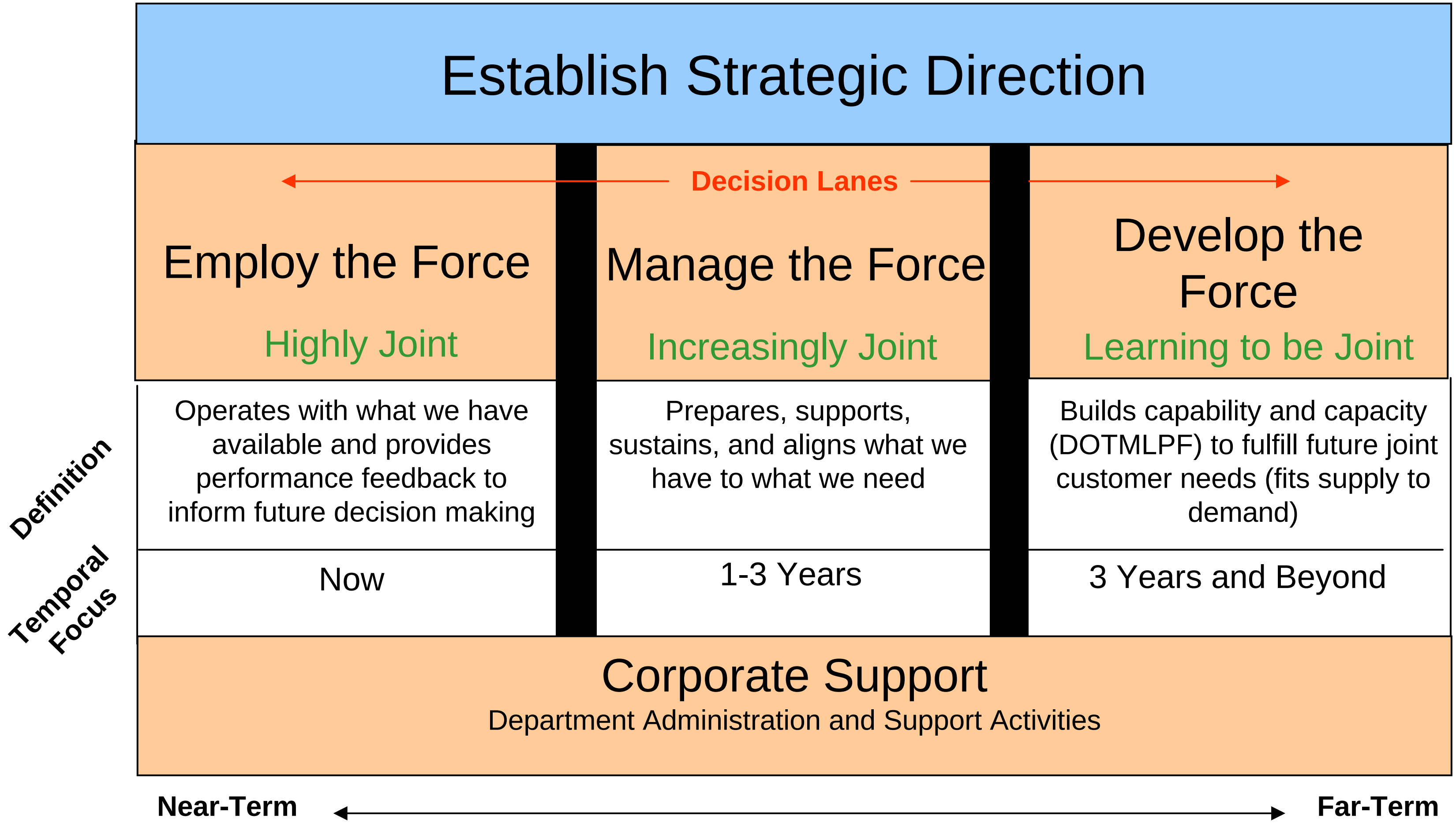
- Lack of synchronization of major processes – timing, context, performance management
- Investment decisions currently detached from Defense strategic direction and joint warfighting concepts (bottom up)
- Choice is made without broader context of risk and value
  - Decisions are component centric and lack portfolio context
  - Ad hoc process for determining where to divest
- Resource and investment decision authority rests with the DSD
- Lack of information transparency and integration across the enterprise

Institutional Reform and Governance Roadmap (IR&G)

- IR&G Co-Leads: Mr. Krieg, USD(AT&L); LTG Sharp, D,JS
- DSD Roadmap Direction
  - Create or invigorate empowered horizontal organizations to integrate priority areas
  - Improve Department effectiveness and efficiency to include exploring a portfolio based approach to defense planning, programming and budgeting
  - Move toward common data structures/approaches at enterprise level
  - Implement new acquisition policies, procedures and processes for dramatic improvements by all measures

Source: DSD Memo 5 January 2006

IR&G Framework: Corporate Decision Lanes



Establish Strategic Direction

Decision Lanes

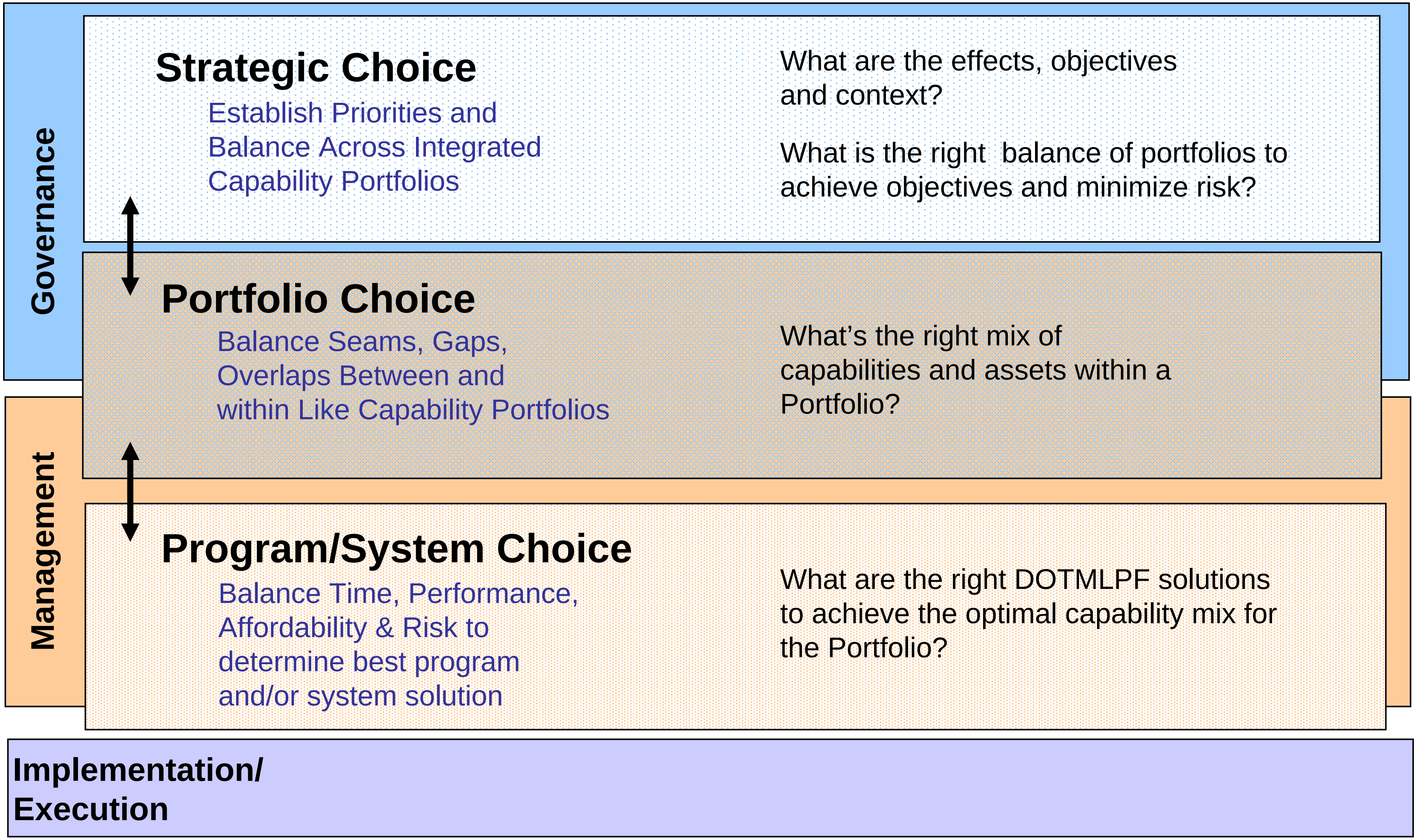
	Employ the Force	Manage the Force	Develop the Force
	Highly Joint	Increasingly Joint	Learning to be Joint
Definition	Operates with what we have available and provides performance feedback to inform future decision making	Prepares, supports, sustains, and aligns what we have to what we need	Builds capability and capacity (DOTMLPF) to fulfill future joint customer needs (fits supply to demand)
Temporal Focus	Now	1-3 Years	3 Years and Beyond

Corporate Support

Department Administration and Support Activities

Near-Term ↔ Far-Term

IR&G Governance and Management Framework: Three Levels of Choice



Governance

Strategic Choice

Establish Priorities and Balance Across Integrated Capability Portfolios

What are the effects, objectives and context?

What is the right balance of portfolios to achieve objectives and minimize risk?

Portfolio Choice

Balance Seams, Gaps, Overlaps Between and within Like Capability Portfolios

What's the right mix of capabilities and assets within a Portfolio?

Management

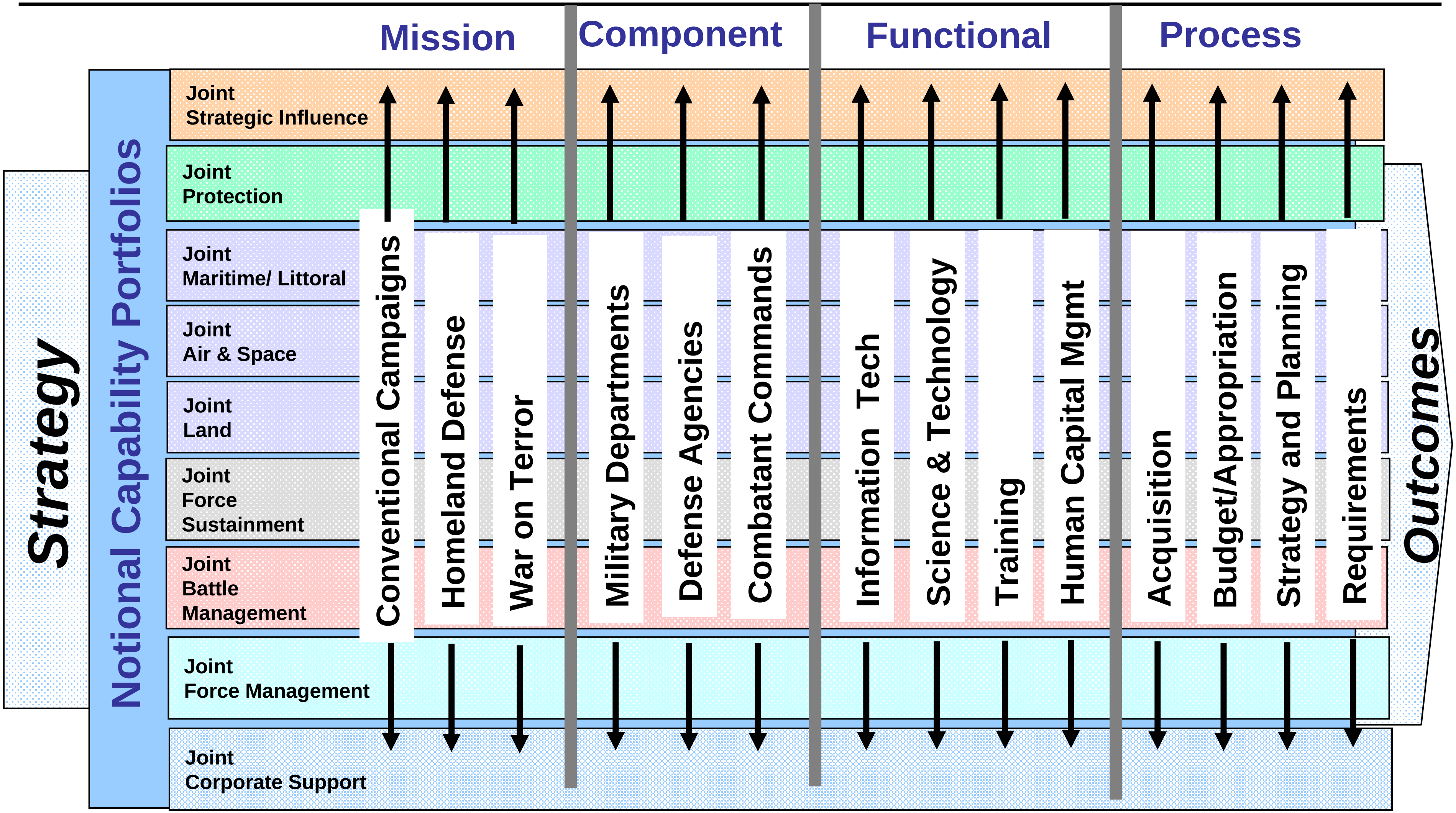
Program/System Choice

Balance Time, Performance, Affordability & Risk to determine best program and/or system solution

What are the right DOTMLPF solutions to achieve the optimal capability mix for the Portfolio?

Implementation/ Execution

Portfolios provide Structure for Horizontal & Vertical Integration



A capability portfolio taxonomy is needed to enable this integration

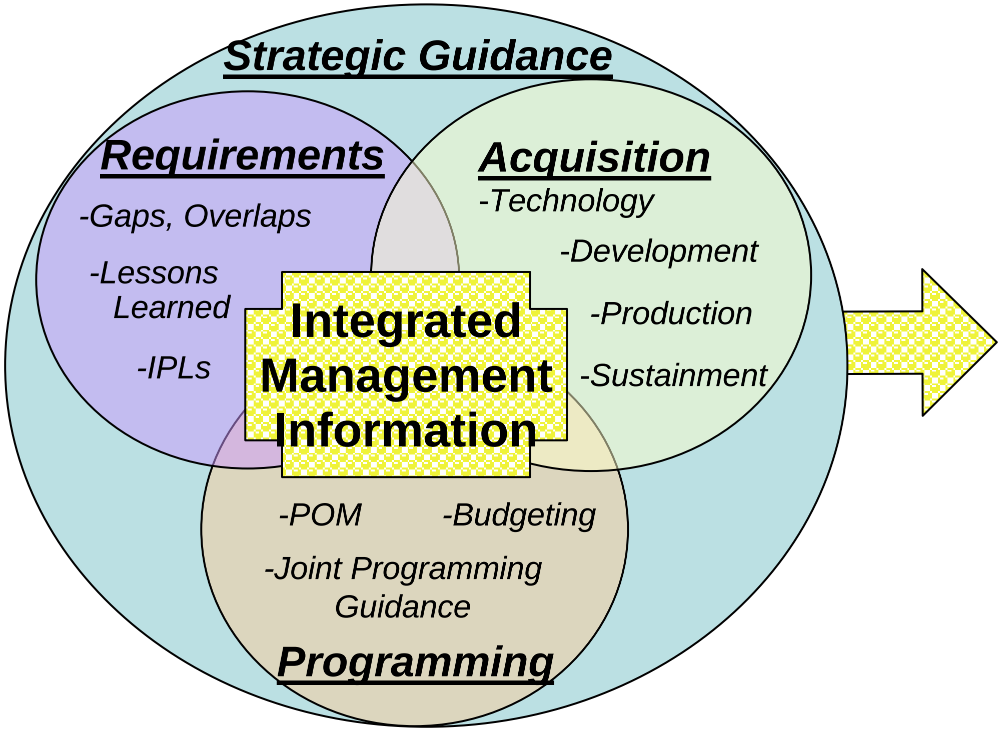
Acquiring Defense Capabilities

What Have We Learned?

- Capability needs will be satisfied by groupings of legacy systems, new programs, and technology insertion – Systems of Systems (SoS)
- Issues:
  - Scale: Size of defense enterprise makes a single integrated architecture infeasible
  - Ownership/Management: Individual systems are owned by the military component or agencies
  - Legacy: Current systems will be part of the defense inventory for the long-term and need to be factored into any approach to SoS
  - Changing Operations: Changing threats and concepts mean that new (ad hoc) SoS configurations will be needed to address changing, unpredictable operational demands
  - Criticality of Software: SoS are constructed through cooperative or distributed software across systems
  - Enterprise Integration: SoS must integrate with other related capabilities and enterprise architectures

Enabling Choice:
Integrated Management Information

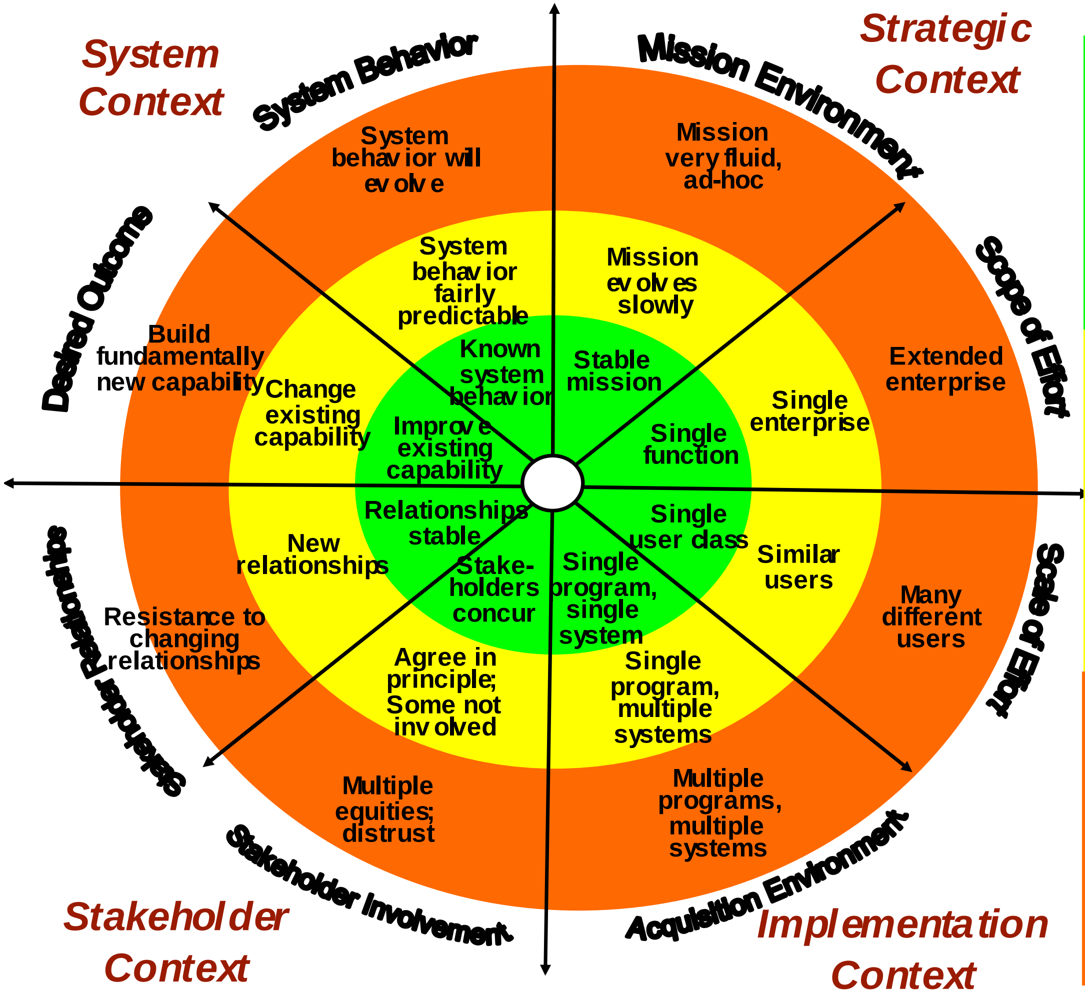
- Transparent information enables strategic decision-making
- Common language to serve all Department activities: Operational as well as Force Development
  - Common link - Capabilities



Multiple Data Views:

- Systems vs. Capabilities
- Capabilities vs. Strategic Goals
- System Context
- Highly dependent programs (Joint Enablers)
- S&T vs. future needs
- Portfolio Efficiency
- Portfolio Affordability
- ……

Profiling Systems of Systems



Typical program domain

- Traditional systems engineering
- Chief Engineer inside the program; reports to program manager

Transitional domain

- Systems engineering across boundaries
- Work across system/program boundaries
- Influence vs authority

Messy frontier

- Political engineering (power, control...)
- High risk, potentially high reward
- Foster cooperative behavior

MITRE

Source: Renee Stevens

Characterizing the System of Systems Environment

- Community Involvement: Stakeholders, Governance
  - **System:** stakeholders generally committed only to the one system
  - **SoS:** stakeholders more diverse; stakeholders from each system involved will have some interest in the other systems comprising the SoS
- Employment Environment: Mission environment, Operational focus
  - **System:** mission environment is relatively stable, pre-defined, and generally well-known; operational focus is clear
  - **SoS**: emphasis on multiple missions, integration across missions, need to ad hoc operational capabilities to support rapidly evolving mission objectives
- Implementation: Acquisition/Test and Validation, Engineering
  - **System**: aligned to ACAT Milestones, specified requirements, a single DoD PM, SE with a Systems Engineering Plan (SEP), test and validating the system is possible
  - **SoS**: multiple system lifecycles across acquisition programs, involving legacy systems, developmental systems, and technology insertion with multiple DoD PEOs, PMs and operational and support communities; testing is more difficult and test and validation can be distributed and federated.

The System Assurance Problem

- Growing system complexity makes vulnerabilities (*malicious*, *exploitable logic*) within SoS much more difficult to discover and mitigate
- Commercial components are highly desirable from standpoint of program cost, schedule and performance, *but:*
  - Risks inherent due to globalization of production
- High Assurance Components are difficult and expensive to make, and deliver limited functionality
- *How do we acquire SoS with mission-worthy system-level assurance properties?*

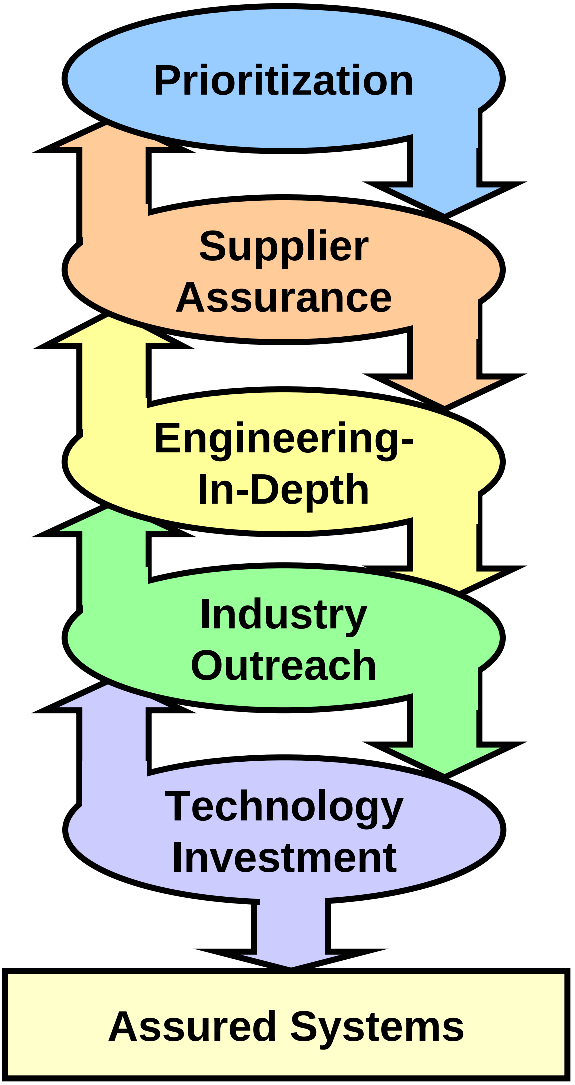
System Assurance Definition

Level of confidence that system functions as intended and is free of exploitable vulnerabilities

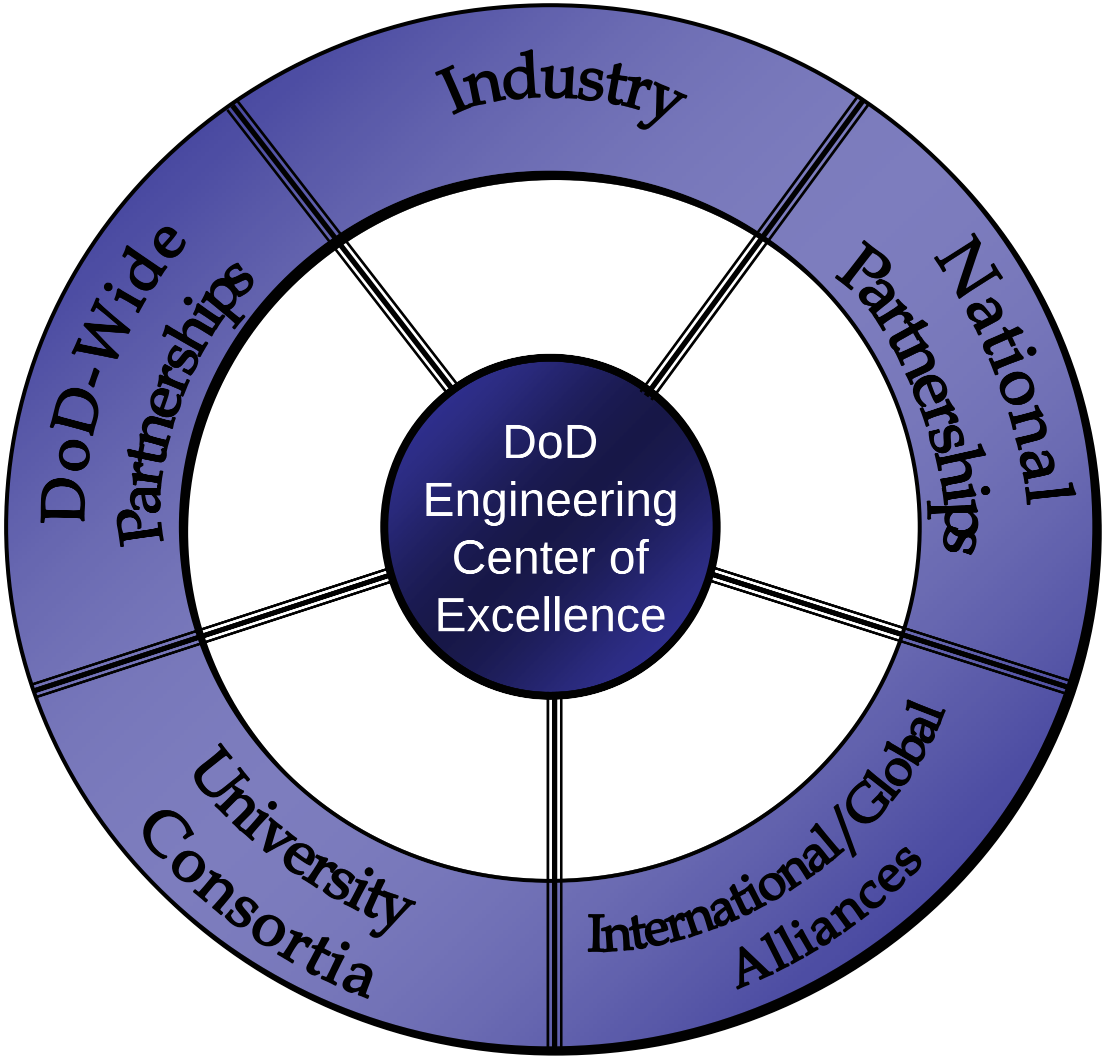
Whether intentionally or unintentionally introduced, designed, or otherwise inserted.

System Assurance: What does success look like?

- The requirement for assurance is allocated among the right systems and their critical components
- DoD understands its 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 system vulnerabilities



Establishing a DoD Engineering Center of Excellence



DoD Software Engineering Excellence

- Support Acquisition Success
- Improve State-of-the-Practice of Software Engineering
- Leadership, Outreach and Advocacy
- Foster Software Resources to Meet DoD Needs

Why Focus on Software: Software Growth in DoD Systems

- Software Requirements Growth (% of functionality provided by software)[1]:
  - 1960s: 8%
  - 1980s: 40%
  - 1990s: 60%
  - 2000s: 80%
- Software Size Growth[2]
  - From < 2M estimated source lines of code in 1980s to > 10M lines of code in 1990s
  - Now approaching 20M ESLOC
- Software Overruns
  - 1994: 16.2% of SW projects completed on-time, on-budget[3]

[1] CSIS/DSB/PM Magazine

[2] CSIS Analysis

[3] Copyright © 1995 The Standish Group International, Inc. All Rights Reserved

[4] Copyright © 2005 The Standish Group International, Inc. All Rights Reserved

DoD Software Engineering & System Assurance Getting Started – What are we Doing?

- Identifing issues, needs
  - Software Industrial Base Study
  - NDIA Top Software Issues Workshop; Defense Software Summit
- Creating opportunities, partnerships
  - Established network of Government software POCs
  - Chartered the NDIA Software Committee, and System Assurance Committee
  - Information exchanges with Government, Academia, and Industry, and International partners
- Executing focused initiatives
  - Handbook on Engineering for System Assurance
  - SoS Systems Engineering Guide
  - Transparent Data for Force Development

We must field assured, reliable, SoS solutions to support Net Centric Operations

Contact Us

Office of the Under Secretary of Defense
Acquisition, Technology and Logistics
Directorate for Software Engineering and System Assurance
3090 Defense Pentagon
Washington, DC 20301-3090
703-602-0851