DoD Software Engineering and System Assurance

New Organization – New Vision

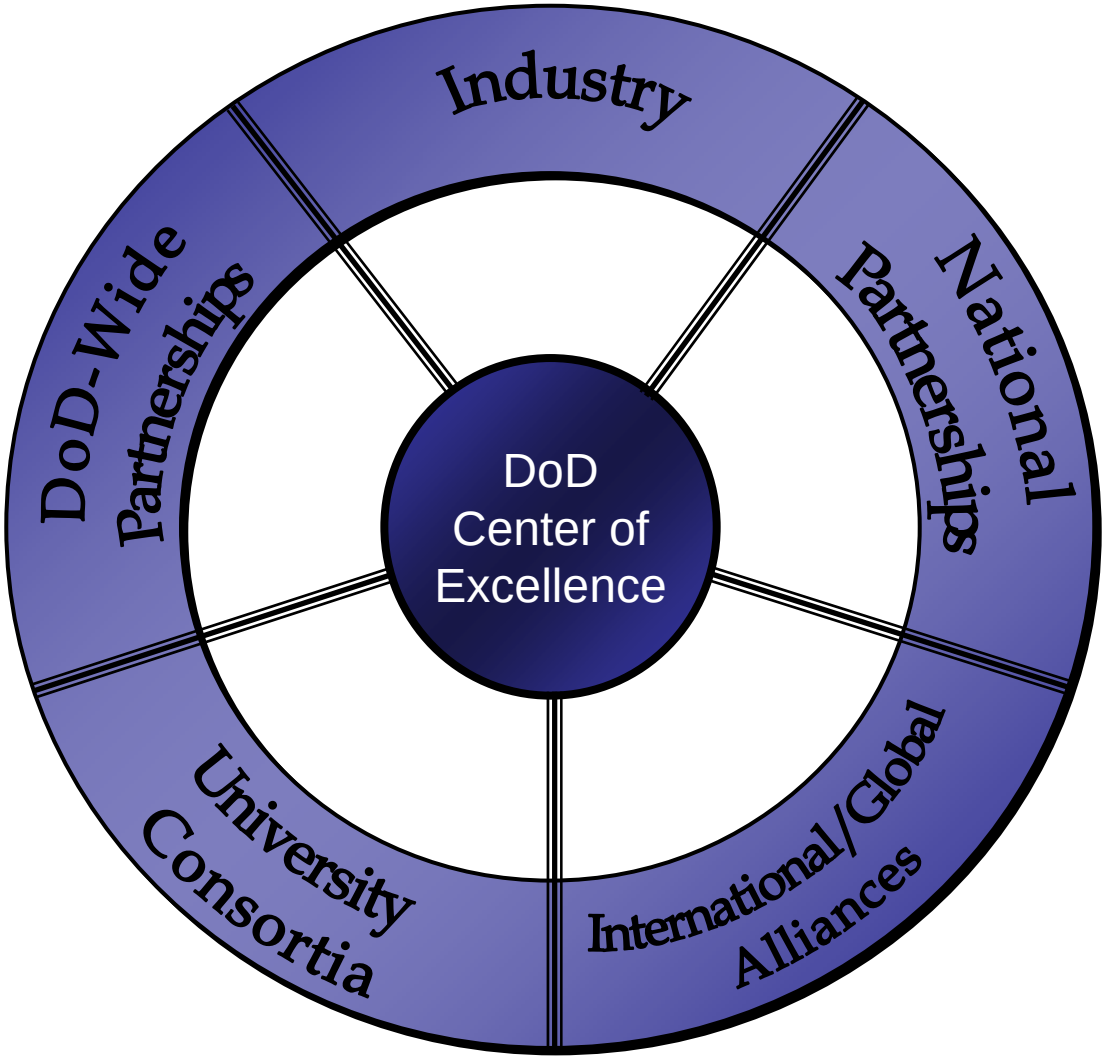
Kristen Baldwin

Deputy Director, Software Engineering and System Assurance

Office of the Under Secretary of Defense

Acquisition, Technology and Logistics

Establishing a DoD Engineering Center of Excellence



DoD Engineering Center of Excellence

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

Elements of a DoD Strategy for Software

- Support Acquisition Success
  - Ensure effective and efficient software solutions across the acquisition spectrum of systems, SoS and capability portfolios
- Improve the State-of-the-Practice of Software Engineering
  - Advocate and lead software initiatives to improve the state-of-the-practices through transition of tools, techniques, etc.
- Leadership, Outreach and Advocacy
  - Implement at Department and National levels, a strategic plan for meeting Defense software requirements
- Foster Software Resources to meet DoD needs
  - Enable the US and global capability to meet Department software needs, in an assured and responsive manner

Promote World-Class Leadership for Defense Software Engineering

Getting Started – What are we Doing?

- Identify software issues, needs
  - Software Industrial Base Study
  - NDIA Top Software Issues Workshop
  - Defense Software Strategy Summit
- Creating opportunities, partnerships
  - Established network of Government software POCs
  - Chartered the NDIA Software Committee
  - Information exchanges with Government, Academia, and Industry
  - Planning the Systems & Software Technology Conference, June 18-21, Tampa, FL
- Executing focused initiatives
  - CMMI Integrity, CMMI-ACQ, CMMI Guidebook
  - Engineering for System Assurance
  - SoS Systems Engineering Guide
  - Providing software support to acquisition programs
  - Software reference curriculum
  - Software/SE integration

*Top Software Issues**

1. The impact of requirements upon software is not consistently quantified and managed in development or sustainment.
2. Fundamental system engineering decisions are made without full participation of software engineering.
3. Software life-cycle planning and management by acquirers and suppliers is ineffective.
4. The quantity and quality of software engineering expertise is insufficient to meet the demands of government and the defense industry.
5. Traditional software verification techniques are costly and ineffective for dealing with the scale and complexity of modern systems.
6. There is a failure to assure correct, predictable, safe, secure execution of complex software in distributed environments.
7. Inadequate attention is given to total lifecycle issues for COTS/NDI impacts on lifecycle cost and risk.

***NDIA Top Software Issues Workshop August 2006**

Software Engineering Issues for Consideration

- Requirements growth 10X (% functionality and program content) 1960s – Present*
- Impact of requirements upon software is not consistently quantified and managed in development or sustainment**
- Software life-cycle planning and management by acquirers and suppliers is ineffective**
- Quantity and quality of software engineering expertise is insufficient to meet the demands of government and the defense industry**
- Traditional software verification techniques are costly and ineffective for dealing with the scale and complexity of modern systems**
- Failure to assure correct, predictable, safe, secure execution of complex software in distributed environments**
- Inadequate attention given to total lifecycle issues for COTS/NDI impacts on lifecycle cost and risk**

Effectively Addressing Software Issues Overdue

* CSIS Software Industrial Base Study

** NDIA Top SW Issues meeting, Aug 06

DoD Software -- What We're Seeing*

- Software systemic issues are significant contributors to poor program execution
  - Software requirements not well defined, traceable, testable
  - Immature architectures, COTS integration, interoperability, obsolescence (electronics/hardware refresh)
  - Software development processes not institutionalized, planning documents missing or incomplete, reuse strategies inconsistent
  - Software test/evaluation lacking rigor and breadth
  - Schedule realism (compressed, overlapping)
  - Lessons learned not incorporated into successive builds
  - Software risks/metrics not well defined, managed

*Based on ~65 program reviews to date

OUSD(AT&L)/SSA
FOCUSED INITIATIVES

SW Issue/GAP Workshop Findings

*based on NDIA Top SW Issues, OSD Program Support Reviews, and DoD Software Summit findings

Primary Software Focus Groups*

Software Acquisition Management
- Standards – O, N
- DAG Ch 4/7 – O, AF
- Prog Spt – O, All
- Contract Language – A, M, N
- SW Estimation – GAP
- Lifecycle Policy – AF
- Risk Identification - GAP

Software Development Techniques
- Agile – O, SEI
- Architecture – A, SEI
- COTS – SEI
- Open Source – AF
- Sustainment – GAP
- SW Interoperability – GAP
- SW Test - GAP

SW & SE Integration
- Requirements – GAP
- SE/SW Process Int – O
- SW Council – N
- SW Dev Plan – N
- SW in SEP – N
- SW in Tech Reviews – N
- SW Quality Attributes - GAP

Ongoing Initiative Owners
- O – OSD/SSA
- A – Army
- N – Navy
- AF – Air Force
- M – MDA
- SEI
- DCMA
- GAP – No activity

Knowledge Sharing
- Standards – O, N
- DAG Ch 4/7 – O, AF
- Prog Spt – O, All
- Contract Language – A, M, N
- Estimation – GAP
- Lifecycle Policy – AF
- Risk Identification - GAP

Data and Metrics
- SW Metrics – A, O
- SW Cost – O
- SW EVM – DCMA
- SW Estimation - GAP

Human Capital
- Education Sources – N, A
- Leadership Training – A, SEI
- SETA Quals – GAP
- SW Human Cap Strategy – GAP
- Industrial Base – O
- University Curriculum – O
- Worforce Survey - AF

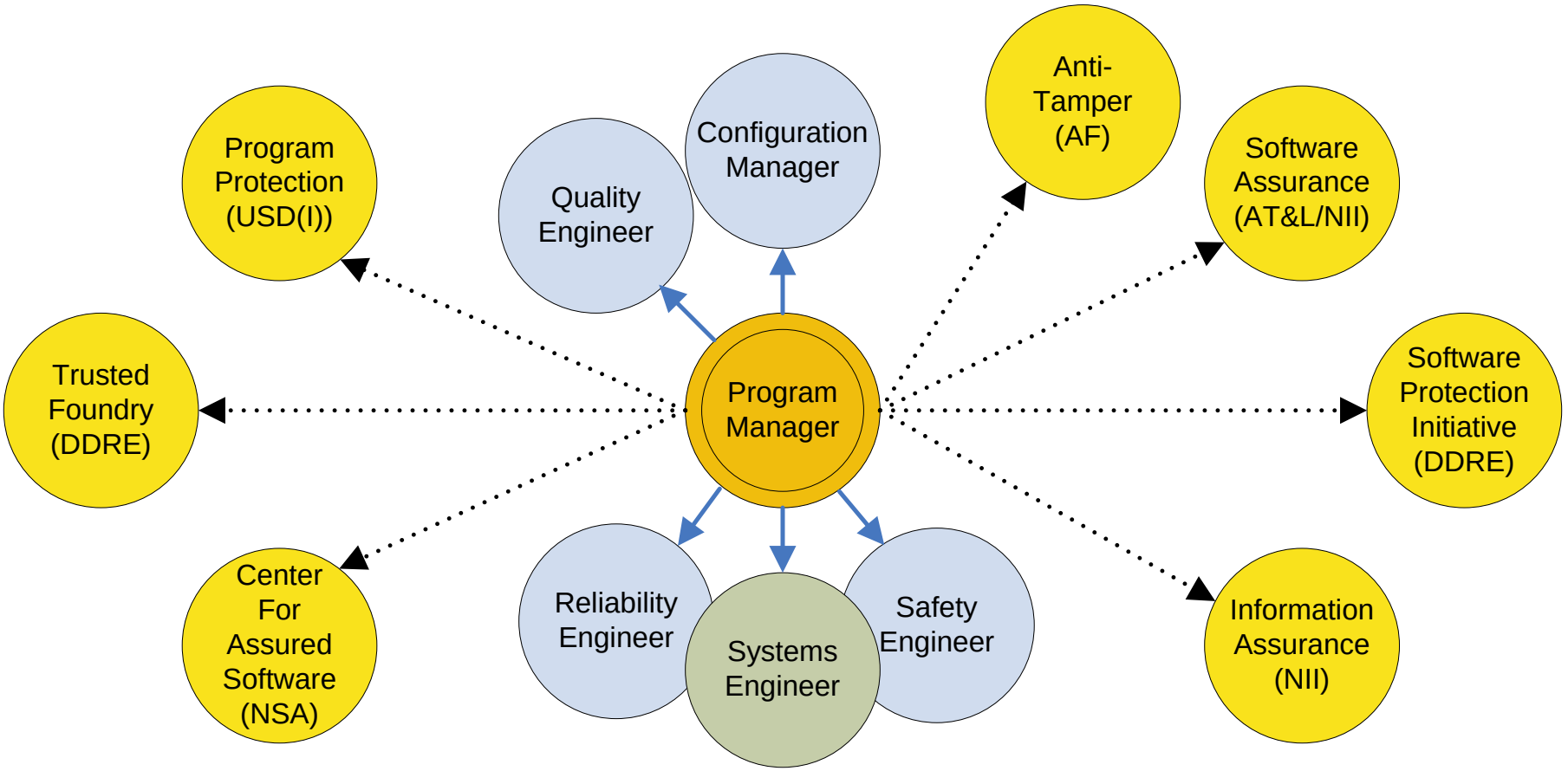
Ongoing SW Initiatives (w/owners) and Gaps binned to Focus Groups

System Assurance

- We continue to be concerned with assurance of our critical DoD assets:
  - Critical information
  - Critical technologies
  - Critical systems
- Observations:
  - Increasing numbers of network attacks (internal and external to DoD)
  - Broader attack space
  - Malicious intent
- Trends that exacerbate our concerns:
  - Globalization of our contracts, expanding the number of international participants in our system developments
  - Complex contracting arrangements that further decrease transparency below prime, and visibility into individual components

These trends increase the opportunity for access to our critical assets, and for tampering

System Assurance Context for the PM



System Assurance Definition

Level of confidence that a system functions as intended, is free of exploitable vulnerabilities, and protects critical program information

Consequences of Fragmented Systems Assurance Initiatives

- Lack of Coherent Direction for PMs, and others acquiring systems
  - Numerous, uncoordinated initiatives
  - Multiple constraints for PMs, sometimes conflicting
  - Loss of time and money and lack of focus on applying the most appropriate engineering for systems assurance for each system
- Synergy of Policy – Multiple ownership
  - Failure to capitalize on common methods, instruction among initiatives
- DoD Risk Exposure
  - Lack of total life cycle view
  - Lack of a focal point to endorse system assurance, resolve issues, advocate PM attention
  - Lack of system-of-systems, architecture perspective on system assurance
  - Potential for gaps in systems assurance protection

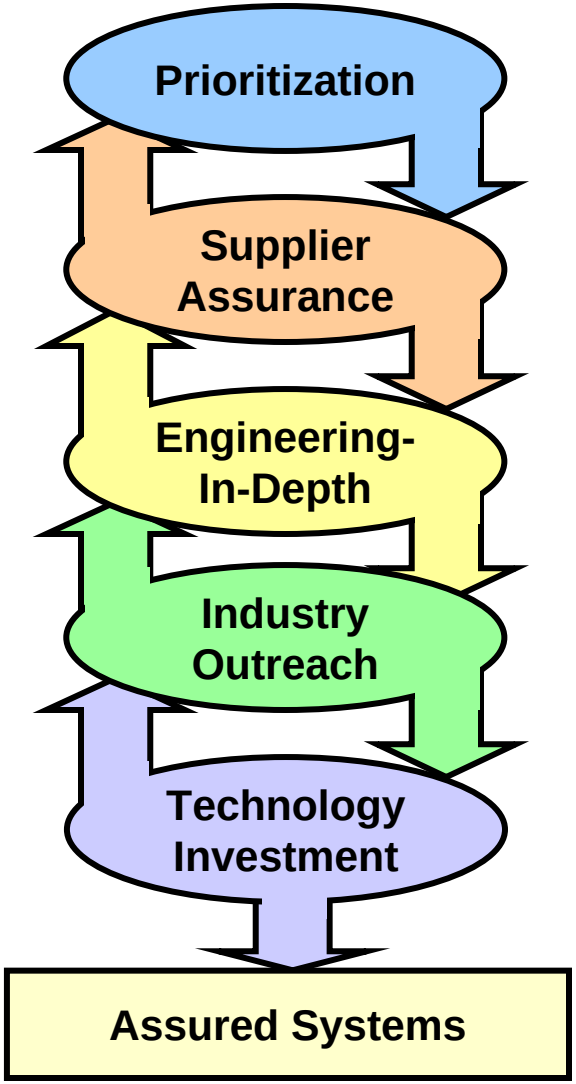
Path Forward

- Create a 'framework' to integrate multiple security disciplines and policies
  - Leverage 5200.39: expand CPI definition to include system assurance and total life cycle
- Use the Program Protection Plan (PPP) to identify CPI and address assurance for the program
  - Link plans (e.g., Anti-Tamper, Software Protection, System Engineering, Assurance Case)
- Modify Acquisition and System Engineering guidance to integrate system assurance across the lifecycle
  - Milestone Decision Authority visibility
  - Guidebook on Engineering for Assurance for program managers/engineers

Raise the bar:	
Awareness	- Knowledge of the supply chain - Who has access to our critical assets
Protection	- Protect critical assets through security practices - Engineer our systems for assurance

What Does Success Look Like?

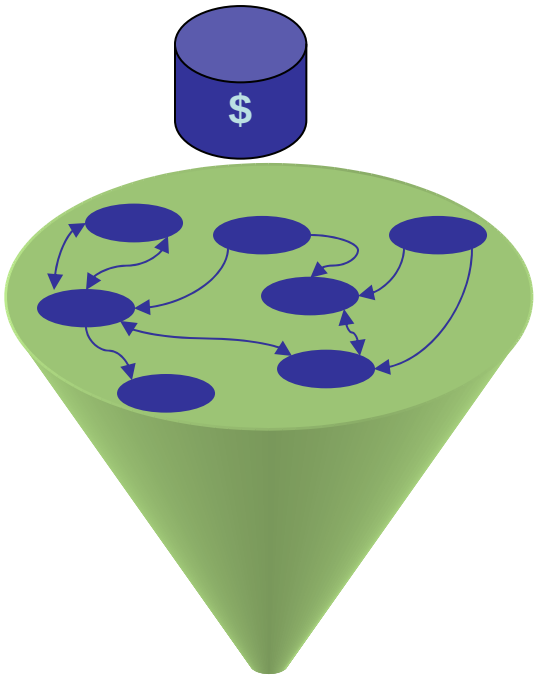
- The requirement for assurance is allocated among the right systems and their critical components
- DoD understands its supply chain risks
- DoD systems are designed and sustained at a known level of assurance
- Commercial sector shares ownership and builds assured products
- Technology investment transforms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

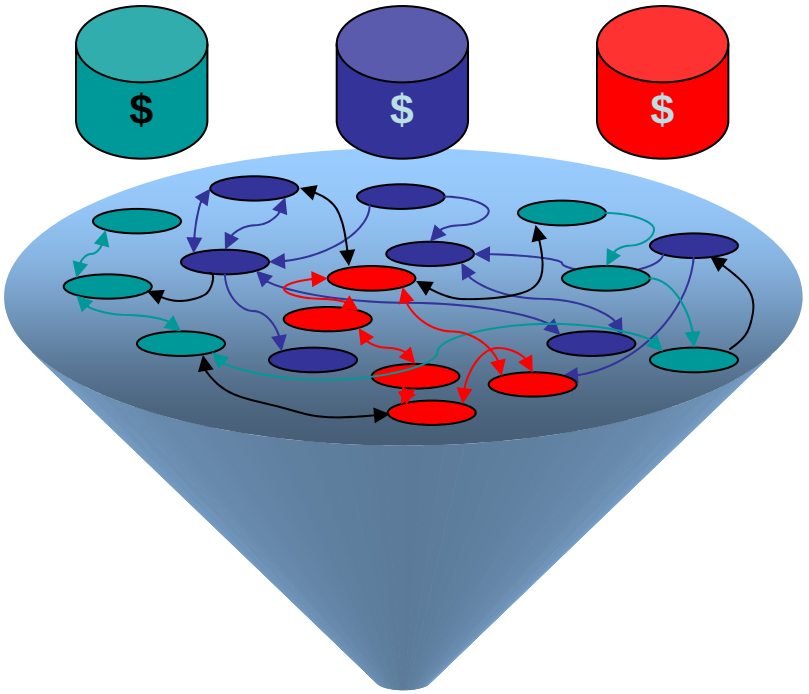


System of Systems

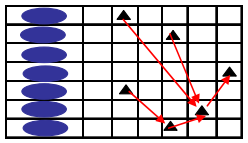
- Why SoS
  - Changing operations - changing threats and concepts mean that new (ad hoc) SoS configurations will be needed to address changing, unpredictable operational demands
  - Legacy - given defense budget projections, current systems will be part of the defense inventory for the long-term and need to be factored into any approach to SoS
- Observations/challenges
  - Scale - size of defense enterprise makes a single integrated architecture infeasible
  - Ownership/Management - individual systems are owned by the military component or agencies, introducing constraints on management and SE
  - Criticality of software - SoS typically focus on integration across systems through cooperative or distributed software
  - Role of network - conceptually DoD SoS will be network-based; budgetary and legacy challenges could lead to uneven implementation

System of Systems
The Management Challenge

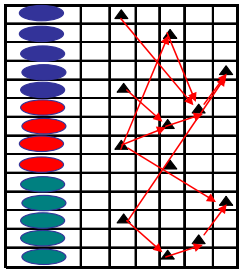




SoS:
Within
Single
Organization



Joint SoS:
Interdependencies
Across
Multiple
Organizations



Political and Cost Considerations impact on Technical Issues

DoD System of Systems SE Guide

SoS Guide Version .9

- Effort led by the Office of the Secretary of Defense
- Collaborative Approach with DoD, Industry, Academia
- Purpose
  - 6 month effort addressing areas of agreement across the community
  - Focus on technical aspects of SE applicable across SoS management constructs
  - Vehicle to capture and debate current SoS experience
- Audience
  - Program Managers and Lead/Chief Engineers

Pilot

- Pilot effort – “Beta test” the SoS guide
  - Structured walkthroughs with practitioners
  - Refine guide content, identify areas for future study
  - Update findings and release Version 1.0 (Fall 2007)

CMMI: New Release and Next Steps

Issues:

- Integrity of CMMI appraisals
- Misperception and misuse of the CMMI by acquirers

Actions:

- Implemented changes to the CMMI v1.2 product suite to ensure:
  - Integrity of appraisals
  - Quality of the product suite
  - Education of acquirers
  - Opportunities for streamlining where appropriate
- Developing a CMMI model for Acquirer process improvement
  - Partnership with General Motors
  - Stakeholders cross DoD, Govt Agencies and Industry
- Writing a CMMI guidebook
  - Help acquirers understand what CMMI is and is not
- DCMA study of actual process implementation

Our Challenge

- Given the shortage of software resources and critical software reliance
  - We cannot afford to be stovepiped
  - We must integrate across cross-functional perspectives to improve our software capability
- We must focus on long standing software issues
  - Leverage ongoing activities to make a difference
  - Invest in collaborative efforts where there are gaps
- Now...
  - Work together to address software issues
  - Contribute to ongoing initiatives: SoS, Sys Assurance, CMMI Guides, more

Become a DoD Center of Excellence