DoD Software Assurance Concept of Operations

April 18, 2006

Dr. Larry Wagoner
NSA
l.wagone@radium.ncsc.mil

Agenda

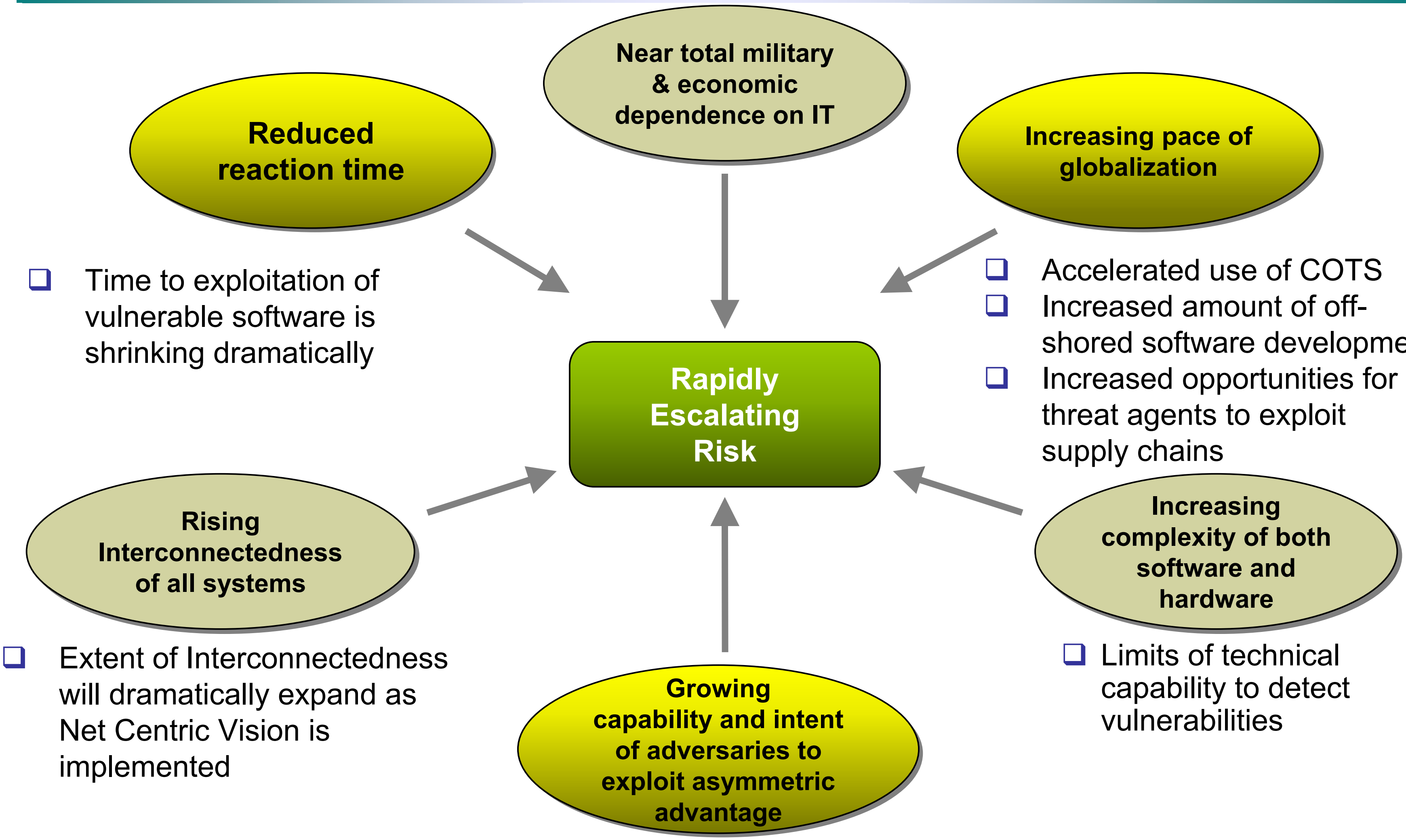
- ❑ Software Assurance (SwA) Problem
- ❑ DoD Response and Guiding Principles
- ❑ DoD SwA CONOPS
  - » Prioritization
  - » Engineering in depth
  - » Supplier Assurance
  - » Science and Technology
  - » Industry Outreach

Software Assurance (SwA) Problem

- ❑ ***Scope***: Software is fundamental to the Global Information Grid (GIG) and critical to all DoD weapons, business and support systems
- ❑ ***Threat agents***: Nation-state, terrorist, criminal, rogue developer who:
  - » Gain control of IT/NSS/Weapons through supply chain opportunities
  - » Exploit vulnerabilities remotely
- ❑ ***Vulnerabilities***: All IT/NSS/Weapons (including systems, networks, 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

Software assurance (SwA) is the level of confidence that software is free of vulnerabilities, either intentionally or unintentionally designed or inserted during the software development and/or the entire software lifecycle.

Factors Giving Rise to SwA Problem Are Accelerating



Near total military & economic dependence on IT

Reduced reaction time

- Time to exploitation of vulnerable software is shrinking dramatically

Increasing pace of globalization

- Accelerated use of COTS
- Increased amount of off-shored software development
- Increased opportunities for threat agents to exploit supply chains

Rapidly Escalating Risk

Rising Interconnectedness of all systems

- Extent of Interconnectedness will dramatically expand as Net Centric Vision is implemented

Increasing complexity of both software and hardware

- Limits of technical capability to detect vulnerabilities

Growing capability and intent of adversaries to exploit asymmetric advantage

DoD is banking on the integrity of software/hardware devices

Background of DoD Response

- In July 2003, the Assistant Secretary of Defense for Networks and Information Integration [ASD(NII)] established the Software Assurance Initiative to examine software assurance issues
- On 23 Dec 04, Undersecretary of Defense for Acquisitions, Technology and Logistics [USD(AT&L)] and ASD(NII) established a Software Assurance (SwA) Tiger Team to:
  - Develop a holistic strategy to reduce SwA risks within 90 days
  - Provide a comprehensive briefing of findings, strategy and plan
- On 28 Mar 05, Tiger Team presented its strategy to USD(AT&L) and ASD(NII) and was subsequently tasked to proceed with a follow-on Implementation Planning Phase
- Implementation Planning Phase closing out – Pilot Phase to begin

Guiding Principles for DoD SwA Strategy

- Understand problem from a systems perspective
- Response should be commensurate with risk
- Sensitive to potential negative impacts
  - Degradation of our ability to use commercial software
  - Decreased responsiveness/ increased time to deploy technology
  - Loss of industry incentive to do business with DoD
  - Minimize burden on acquisition programs
- Leverage and extend relationships with:
  - National, international, and industry partners
  - Other DoD initiatives, e.g., Trusted Foundry, Information Assurance

Vision of Success

Strategic Level:

The SwA CONOPS is integrated into existing DoD processes, such that decision makers balance software risk (threat) with affordability, technical feasibility and operational capability

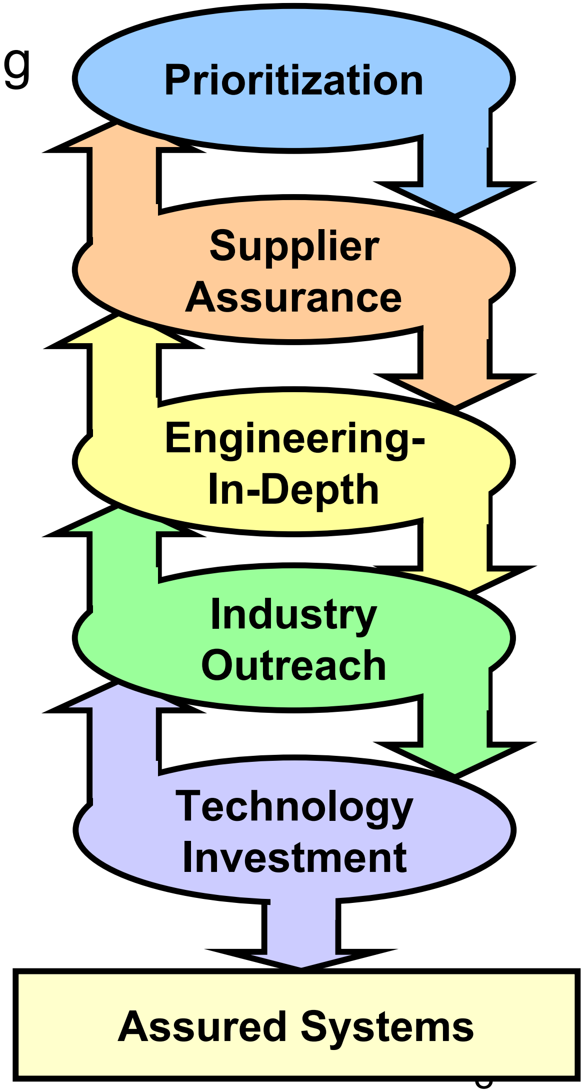
Tactical Level:

DoD systems’ ability to provide intended capabilities is not compromised by attempts to create and exploit software vulnerabilities

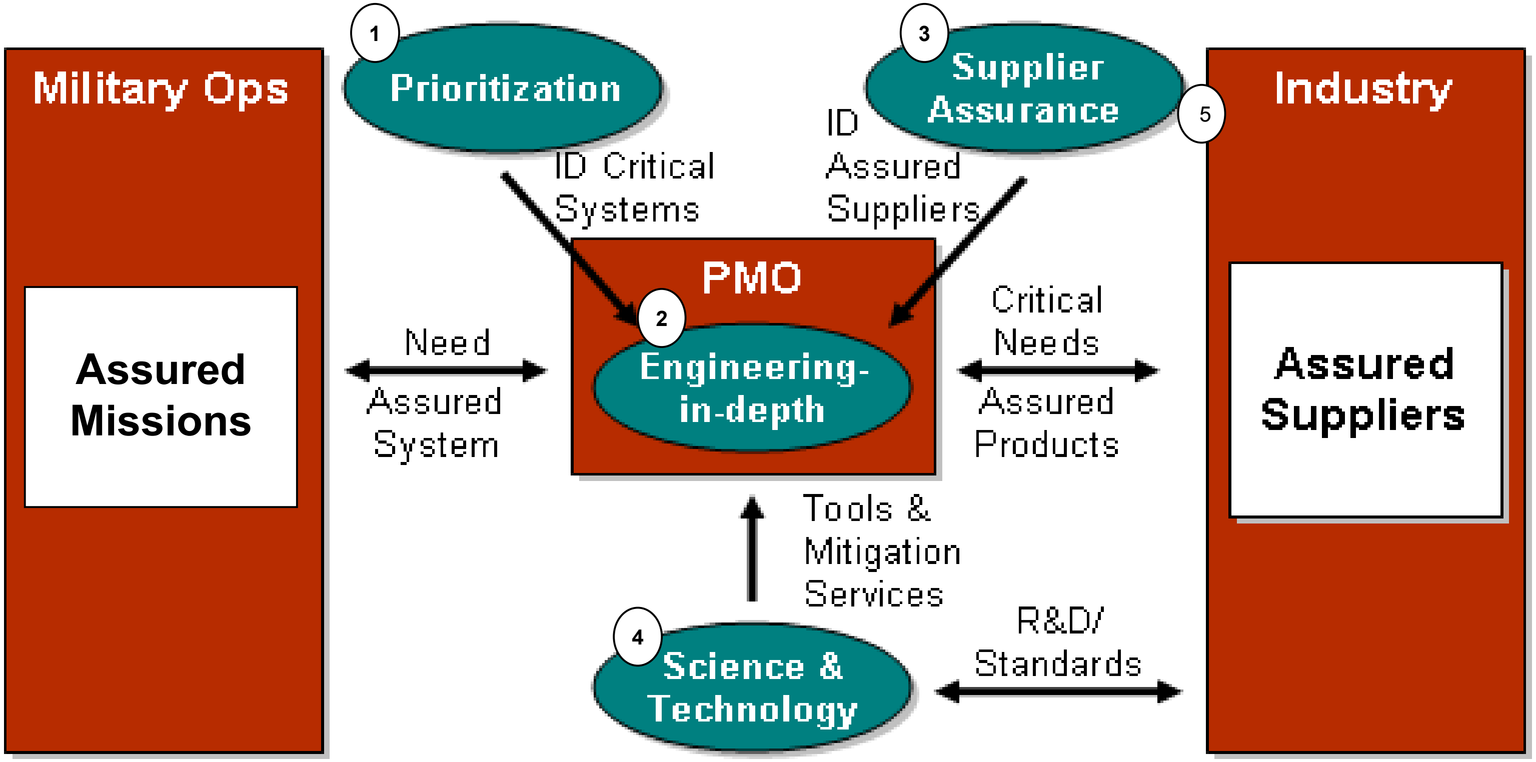
DoD Implements a balanced strategy for managing risk from software vulnerabilities to achieve mission effectiveness

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



DoD Software Assurance CONOPS Elements



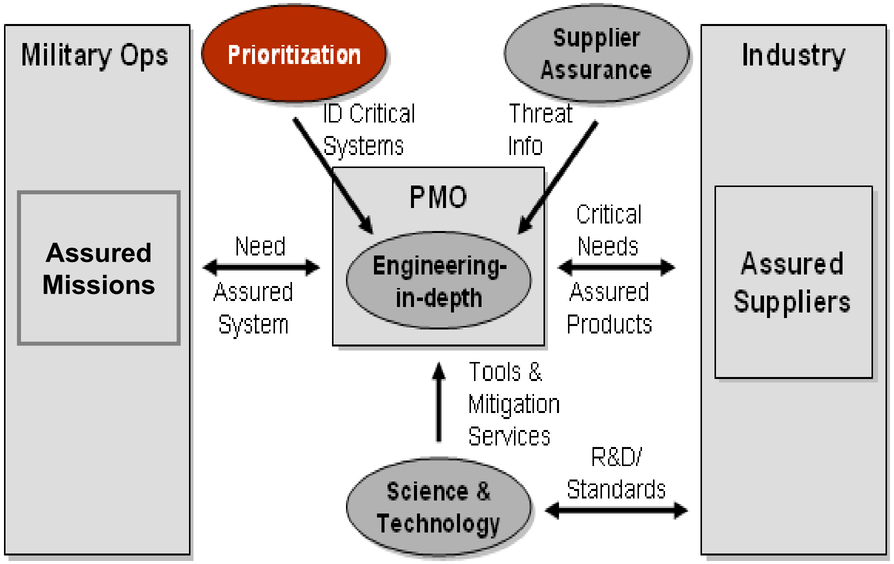
The strategy components interact with military operations, acquisition, and industry to produce assured systems

Software Assurance CONOPS: Prioritization

1

Prioritization

- ❑Prioritization will happen early within the requirements/acquisition processes
  - » leveraging the functional capability boards of the JCIDS process
  - » prioritization decision by milestone A
- ❑Identify ubiquitous software for mitigation
- ❑Programs for the acquisition of critical systems use engineering-in-depth processes
- ❑Long Term Schedule: Prioritization process will be a deliberative action by a stakeholder community
  - » Joint Staff, COCOMs, Services
  - » Portfolio Management Mission Areas
- ❑Short Term Schedule: Focus on new high-risk acquisitions, for example:
  - » Major DoD Acquisitions;
  - » Systems connected to classified networks
  - » Classified Programs
  - » Systems Identified at the discretion of DoD Leadership

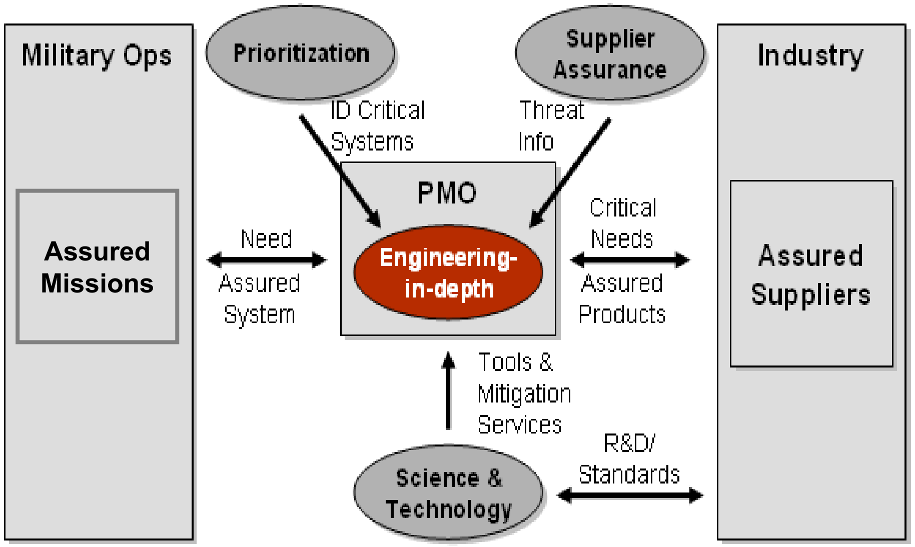


Software Assurance CONOPS: Engineering-in-Depth

2

Engineering-in-Depth

- ❑Engineering-in-depth (EiD) is the application of systems engineering processes to meet the new SwA requirements
  - » Established for critical system acquisition programs through a Key Performance Parameter (KPP)
- ❑EiD will achieve SwA cost-effectively by:
  - » Minimizing the number and criticality of components which require greater assurance
  - » Managing the residual risks inherent in the use of less assured products
  - » Achieved through design techniques (graceful degradation, isolation, multi-pathing, replaceable modules, etc.)
- ❑Programs procure critical components from suppliers with requisite supplier assurance levels (SALs) or perform additional risk mitigation
- ❑EiD is aided by
  - » Industry's creation of products with standards-based assurance properties
  - » S&T vulnerability mitigation tools and services



Software Assurance CONOPS: Supplier Assurance

3

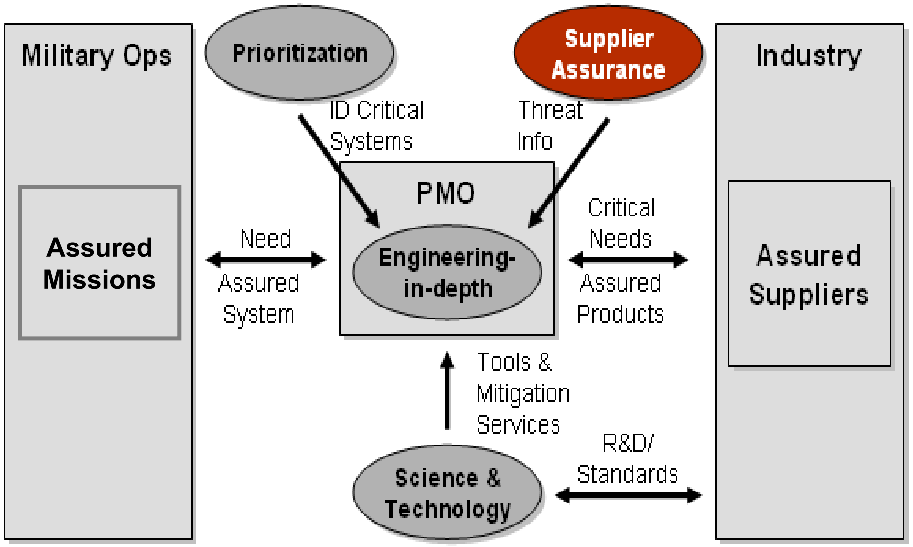
Supplier Assurance

❑Supplier assurance is the use of all source information to categorize suppliers according to the level of risk they represent to DoD

- » Represented as supplier assurance levels
- » Based on all source data and supplier-provided information
- » Considers foreign control of suppliers and outsourcing of technology and product development
- » Considers Security Related Practices and Procedures followed by suppliers

❑SAL will be available to the PMO

❑Requests for proposals (RFPs) involving critical components will require high SAL



Software Assurance CONOPS: Science and Technology

4

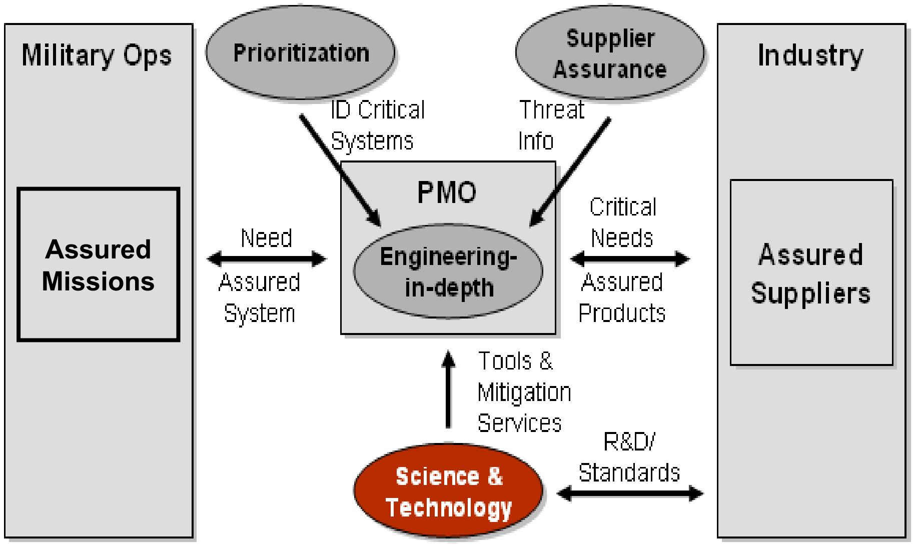
Science and Technology

❑The DoD Science & Technology (S&T) processes aim to achieve transformational solutions for the SwA problem, while providing state-of-the-art technical resources to the engineering-in-depth (EiD) process

- » Identifies unmet needs while supporting EiD
- » Works with industry to develop standards
- » Coordinates DoD R&D for vulnerability detection and mitigation
- » Provides vulnerability detection/prevention/ mitigation tools & services to DoD programs (inc. advice on commercial tools and services)
- » Acts as the “evaluator of last resort” on PMO request (does *not* evaluate everything)

❑NSA will act as Executive Agent for Software Assurance

- » Draft Directive written
- » Focus is on S&T

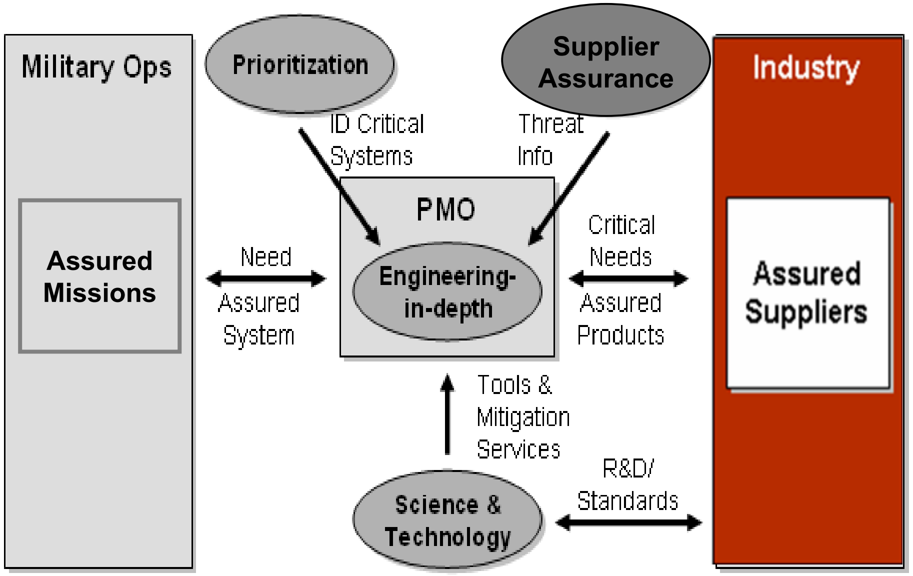


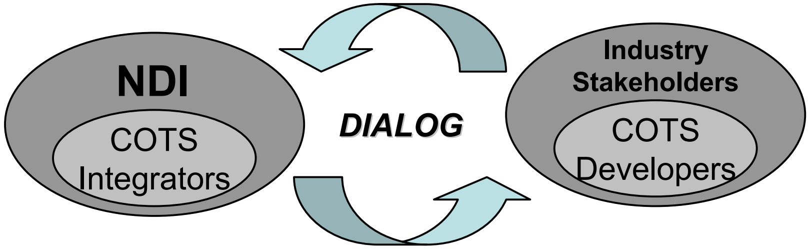
Software Assurance CONOPS: Industry Outreach

5

Industry Outreach

- Extending DoD community to engage in system assurance strategy
  - NDIA established a systems assurance committee; AIA & GEIA connected to efforts
  - Developing a systems assurance handbook
- OMG established a SwA committee
  - Developing Industry end-to-end reference models (RM), products, standards, requirements
    - Product level assurance properties → Systems of known assurance
    - Express RM/Standards/Requirements in modeling language
  - Identify methods for validating compliance with requirements/ standards, using industry-developed tools
- Lack of extensive commitment and participation by Industry





The End.