DoD Software Assurance (SwA) Update

Systems and Software Technology Conference
May 2, 2006

Ms. Kristen Baldwin
OUSD(AT&L)/Defense Systems
kristen.baldwin@osd.mil

Briefing Agenda

- Problem Definition
- Vision of Success
- DoD SwA CONOPS
- Policy and Guidance Recommendations
- SwA CONOPS Assessments
- SwA Business Case Status
- Industry Outreach
- FY06 Plans and Way Ahead

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 IT/NSS/Weapons through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities***: All IT/NSS/Weapons (incl. 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

Vision of Success

Strategic Level:

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

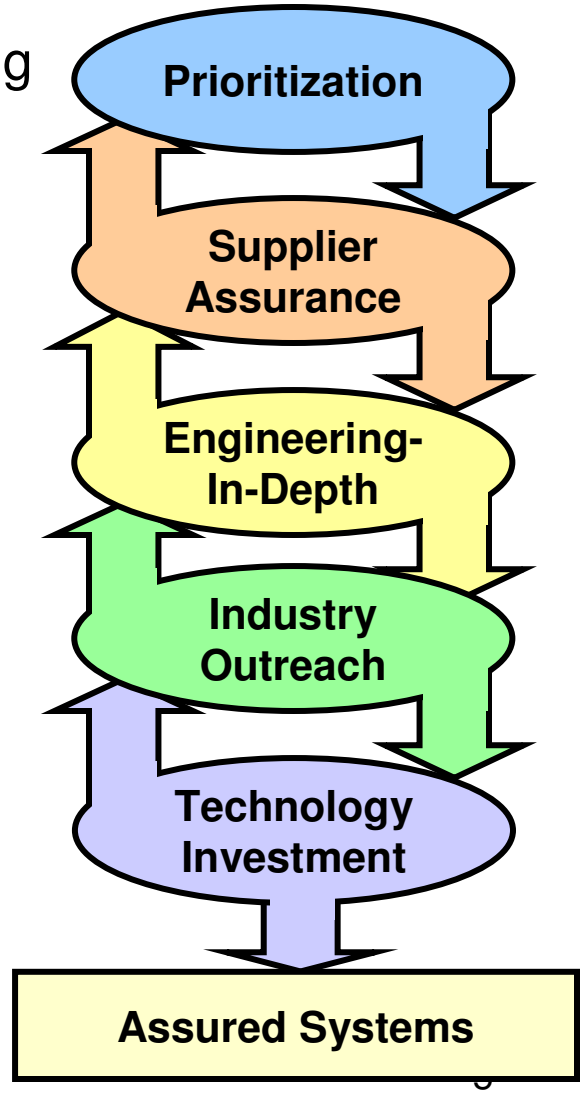
Tactical Level:

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

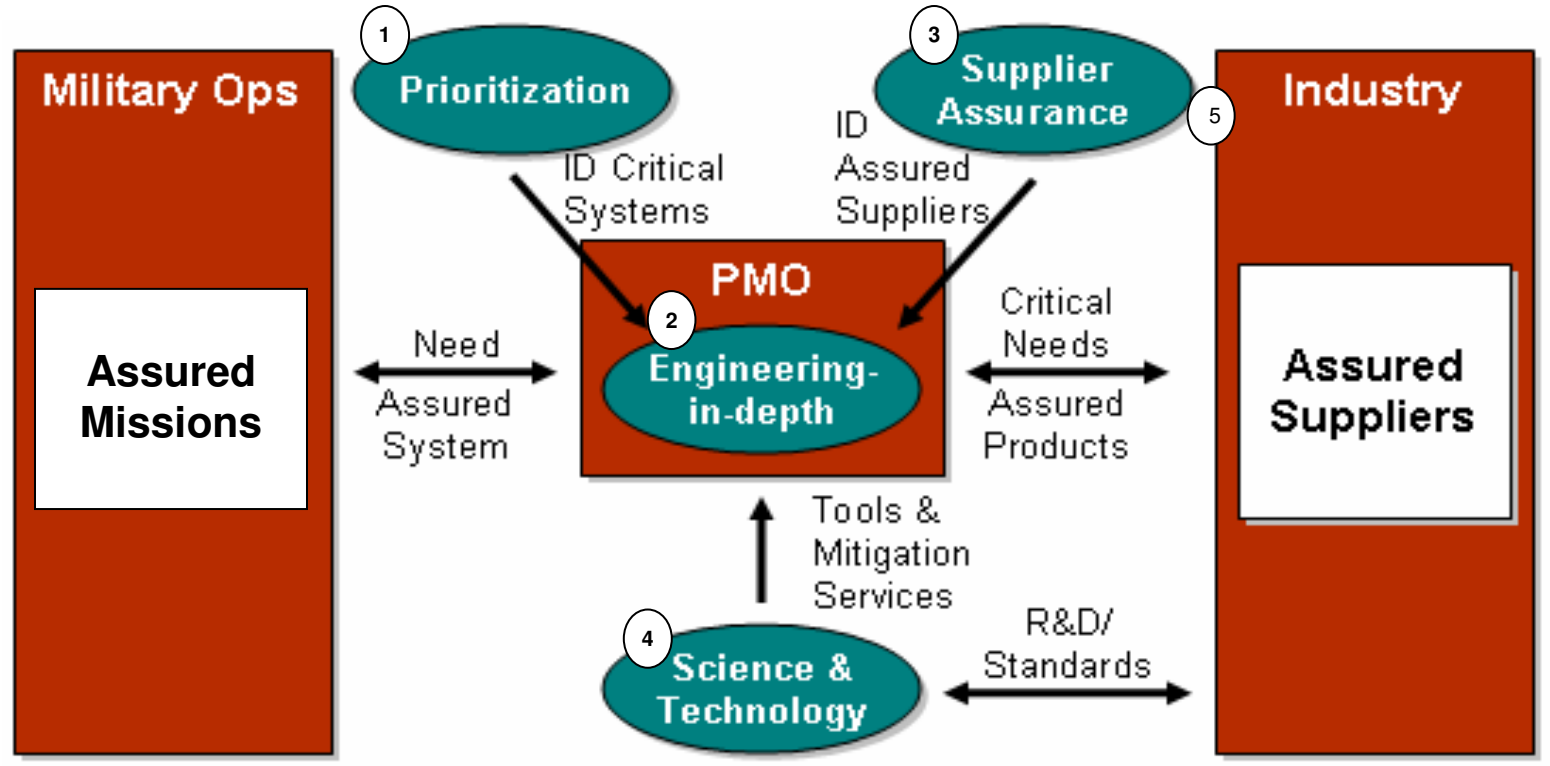
DoD Implements a balanced strategy for managing risk from software vulnerabilities to achieve mission effectiveness (Success)

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



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

Policy and Guidance Update

- Final Draft Directive for SwA Executive Agent
  - Establish NSA as the Executive Agent for Identification and Mitigation of Software Assurance Vulnerabilities
  - Establish a Center for Assured Software to facilitate the EA role
- Draft Instruction for Supplier Assurance
  - Use all source information to identify high assurance suppliers
  - Beginning broader community coordination
- Develop a policy memorandum
  - Delineate the roles and responsibilities to implement the DoD SwA strategy
  - Initiate transition to system assurance
- Develop or update specific policy/guidance as required to implement the strategy elements (e.g. updates to 5000.2, 8500.2)

FY06 SwA CONOPS Assessment

- Objective: Pilot SwA CONOPS with DoD programs prior to issuing DoD SwA Policy and Guidance
- Scope:
  - Assess cost and schedule burden of the SwA CONOPS on 3 Programs of Record (POR): 1 weapon system, 1 space/C4ISR system, 1 ubiquitous system
  - Pilots will perform retrospective assessment of the CONOPS (not the POR), to assess potential impact of SwA policies and procedures
- Expected Output
  - Report containing impact assessment and recommendations; used to refine the SwA CONOPS
  - POR gains insight on potential SwA risks
  - Vetted SwA policy and guidance that better reflects reality
- Status
  - Nominations currently in progress
  - Assessments expected May-Sep 06

Software Assurance Business Case Analysis

- Institute for Defense Analysis tasked to develop a business case for the SwA CONOPS
  - What are the fixed costs of this strategy?
  - How much do the cost and protection increase as coverage increases?
- Progress to date:
  - Modeled fixed costs: Prioritization, Supplier Assurance, S&T
  - Modeled recurring costs: Supplier Assurance, Engineering-in-Depth
- Plans:
  - Update cost projections by participating in Pilot Assessments
  - Finalize business case in FY06

Industry Outreach

- 2 May 05: USD(AT&L)/ASD(NII) memo to Industry
  - Requested participation in an Executive Roundtable
- Subsequent Activities:
  - OMG leveraging ongoing standards activities of ADM to apply meta-model concept to assurance problem
  - NDIA hosted SwA Summit and chartered the System Assurance Committee
  - GEIA will share lessons and collaborate to develop new processes
  - AIA will help integrate SwA processes into mainstream integration activities
- DoD/Industry Executive Roundtable held in December 2005

NDIA System Assurance Committee

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

Govt/Industry Handbook on System Assurance

- How to allocate requirements for assurance
  - Identification of critical components
  - Sensitivity analysis
- Elements of a robust design
  - How do you engineer for system assurance?
  - Leveraging dependability (reliability, availability, maintainability)
- Life cycle considerations
- Demonstration of assurance properties
  - Verification and Validation
  - Certification and Accreditation
  - Test and evaluation
- Supporting engineering practices
  - Risk management
  - Configuration management
- Other….

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

Way Ahead

- Conduct Pilot Assessments of the CONOPS
- Develop and staff policy/guidance
- Transition focus from software assurance to system assurance
- Develop resource implementation plan for FY07 and beyond
- Continue outreach activities

Working together to build a competitive market for assured products