NSA Center for Assured Software

High Confidence Software and Systems Conference

April 18, 2006

Software Assurance Definition

DoD Software Assurance Initiative

DoD Software Assurance Tiger Team

- The level of confidence that software is free of exploitable vulnerabilities, either intentionally designed into the software or accidentally inserted

- And that the software functions in a manner as expected.

Problem Statement (1)

"The ubiquity of software and its development and usage without consistent engineering, has resulted in ad hoc management and mitigation efforts in a race to protect systems against breaches"

NII Sponsored

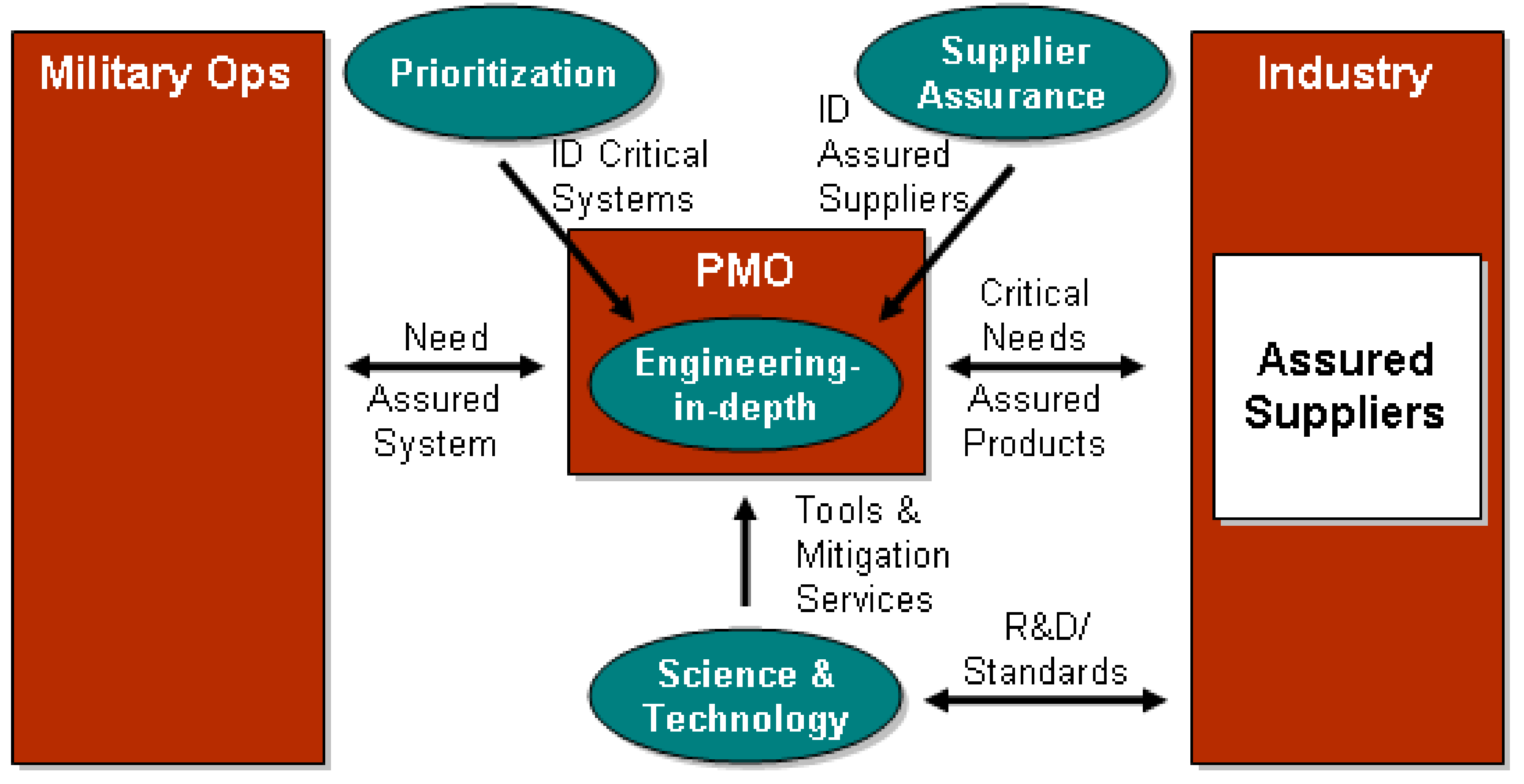
Software Assurance Tiger Team

Problem Statement (2)

There’s too much software

There’s too little assurance

DoD SwA CONOPS: Interacting Processes



Science & Technology

- Provide software evaluation services
- Use tools to detect vulnerabilities
- Coordinate DoD R&D for vulnerability detection and mitigation
- Work with industry to develop standards/solutions
- Recommended a DoD Executive Agent for Software Vulnerability Mitigation and Discovery
  - Establish a DoD Center for Assured Software

NSA Center for Assured Software (CAS)

- Stood up in November, 2005
- A Focal Point for Software Assurance (SwA) Issues with the following objectives:
  - Partner with our customers, government, the private sector and academia to identify SwA Issues and resolutions
  - Develop and utilize tools and methods to analyze the trustworthiness of software

NSA Center for Assured Software (CAS) (cont)

- Objectives (cont)
  - Evaluate mission critical components
  - Establish/Identify software standards and practices to increase the availability of assured software products

CAS Technical Philosophy

Threat Mitigation Assumptions

- We will never have "100% guaranteed assurance"

- Need to make attack as cost prohibitive as possible

Software Assurance Observation (1)

- Continues to be difficult to measure
  - Very labor intensive
    - Does not scale well
- Prone to human error
  - Often do not prevent flaws that our customers expect us to catch
  - Not reproducible or repeatable
- Unpredictable
- Low emphasis on automated tools

Software Assurance Observation (2)

- Highest level of Software Assurance ultimately “reaches back” to the developer’s desk
  - Assurance gained after development is “fleeting”
  - “After Development Analysis/Testing” has a very important role in establishing assurance but developmental assurance should play a larger role in the overall assurance paradigm

What Should the Future Look Like

- Fully "graded" software assurance scale
  - guidance on how to apply it
  - better ways to measure software assurance indicators
- More emphasis on the role of the development process.
- More confidence in the result of lower assurance evaluations

What Should the Future Look Like (cont)

Tools

Tools

Tools

CAS "domain of operation"

Role of Formal Methods

Developmental Processes

Binary analysis tools/techniques

Source Code analysis tools/techniques

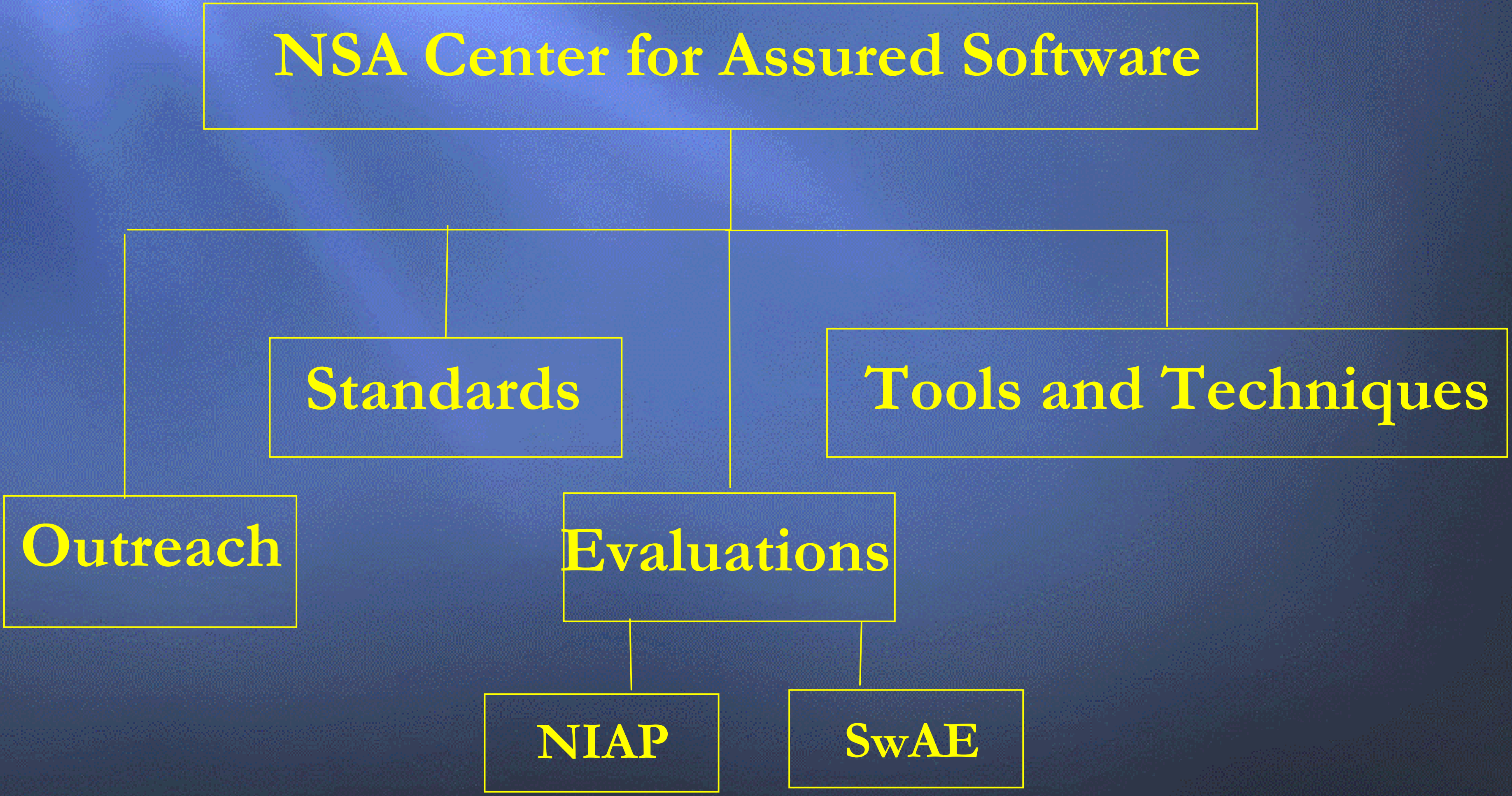
Product Evaluation

Requirements | Design | Implementation | Testing | Deploy | Maintenance

Safe Language Standards

Development Tools/techniques

What we look like today…



NSA Center for Assured Software

Outreach

Standards

Evaluations

Tools and Techniques

NIAP

SwAE

Where we are working today …

- NIAP
  - Fully operational
  - Beginning to address recommendations from the GAO and IDA NIAP review reports

- Software Assurance Evaluations
  - CAS is evaluating specific software of interest to NSA in the context of a pilot
    - First report due to be delivered this month

Where we are working today (cont) …

- A repeatable SwAE methodology based upon available tools
  - Involves a tools survey as wells as incorporating lessons learned from our pilot

- Strategies for :
  - Public Software Assurance Standards participation
  - Internal NSA Software Assurance Standards and compliance
  - Outreach
  - High Assurance

Center for Assured Software

Kris Britton

TD, NSA Center for Assured Software

rkbritt@missi.ncsc.mil

410-854-4543