2010 NDIA T&E SYMPOSIUM OTA COMMANDERS' ROUNDTABLE

A Navy perspective on Information Assurance
-having systems that work when needed

2 March 2010

Bill McCarthy
Deputy Director
Operational Test & Evaluation Force

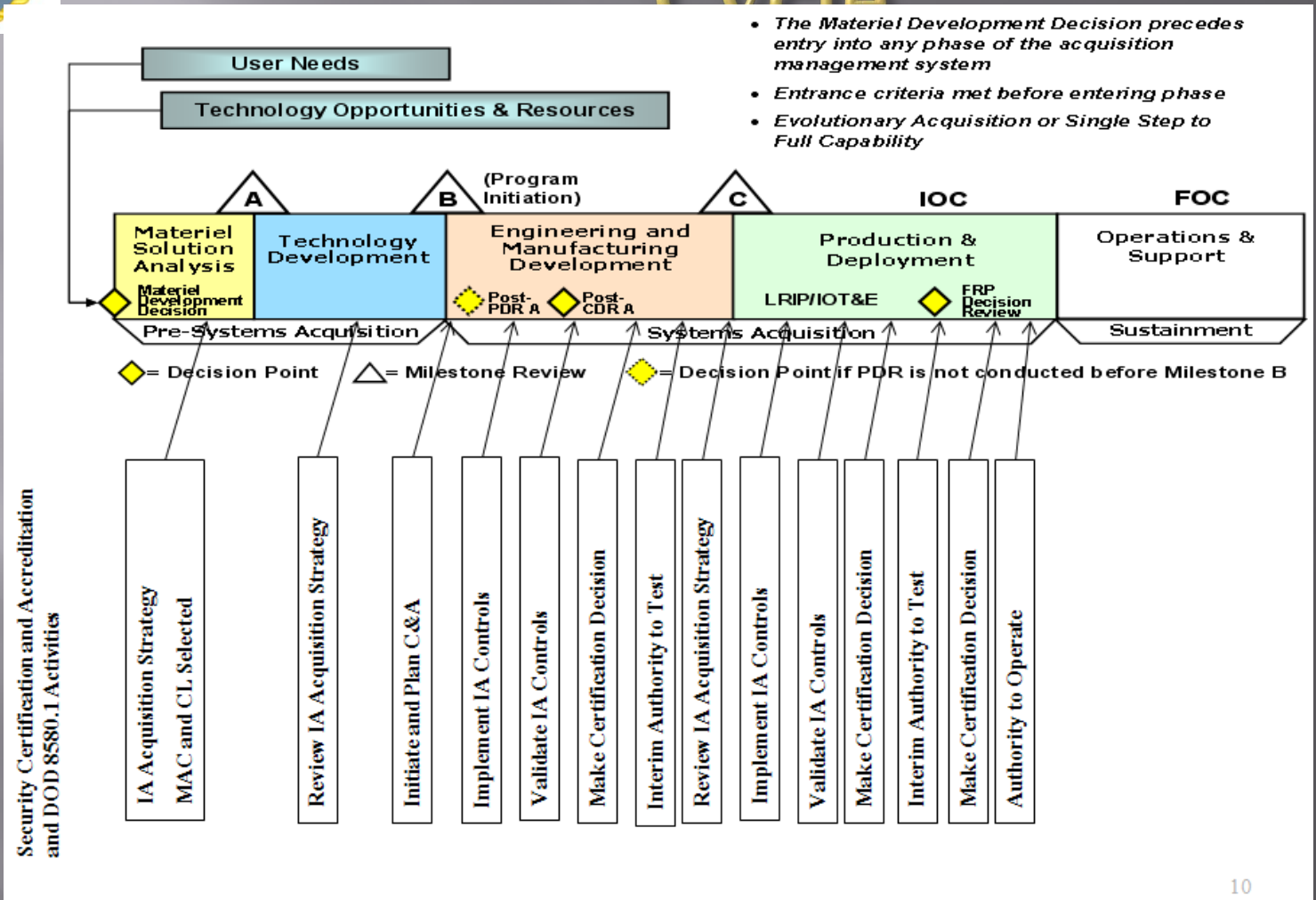
Common Challenges

- "Cyber" is still a relatively new warfare domain
- The cadre of truly experienced personnel is small and while growing, will take literally years to fully develop
  - We are all competing for the same talent pool
- The threat is ubiquitous and is rapidly evolving
- There are often expectation mis-matches – there is not necessarily agreement as to the goal or desired outcome of testing

Challenges in Acquisition Life Cycle

- Upfront definition of IA requirements is a prerequisite for integrated testing
- IA controls "inheritance" is not understood by the implementing Program Manager
- Program Managers often fail to consider
  - IA in RFP, PDR, CDR, Contracts, CDRLs
  - Supply Chain Risks
- Integration Challenges
  - Need for realistic operational environment s with end-to-end test venues
- Current certification & accreditation process was not designed to support rapid software development
  - Process can be slow and inflexible
  - Process does not readily account for incremental changes
- System developers, certification & accreditation authorities, and testers need to collaborate and share IT test results
  - Program managers perceive they are paying several times for IA

IA in the Acquisition Life Cycle



IA in the "Notional" Systems Engineering Life Cycle

SE Process

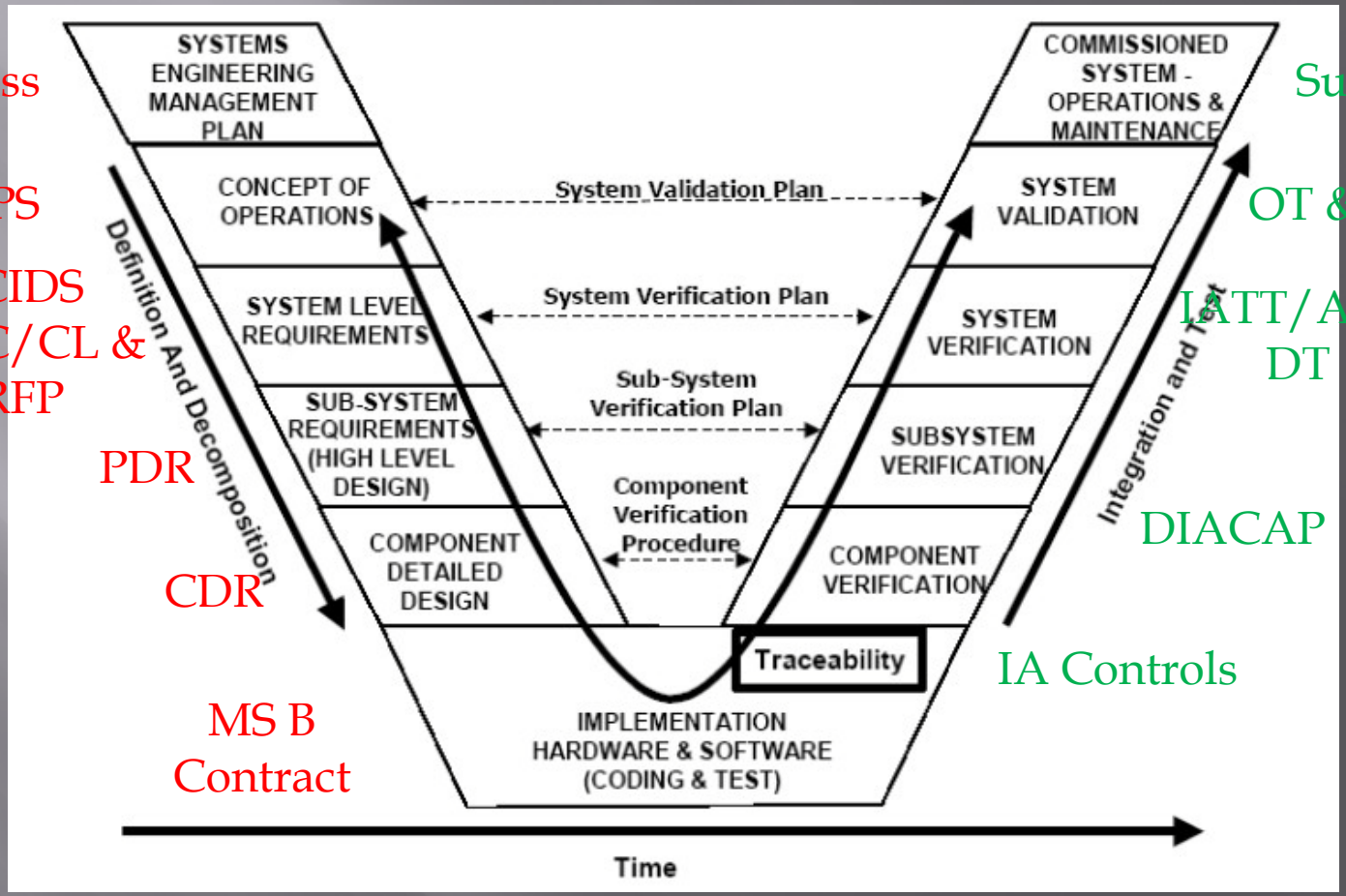
CONOPS

JCIDS
MAC/CL &
RFP

PDR

CDR

MS B
Contract



Sustainment

OT &E

IATT/ATO
DT

DIACAP

IA Controls

Navy Challenges

- Ships are inherently high demand - low density assets
- Most legacy platforms (ships, in particular) are an amalgamation of systems
  - Legacy hardware & software
  - COTS and open source code
- Individual platforms are limited in number and often rely upon a relatively small set of interface points to connect with the GIG.

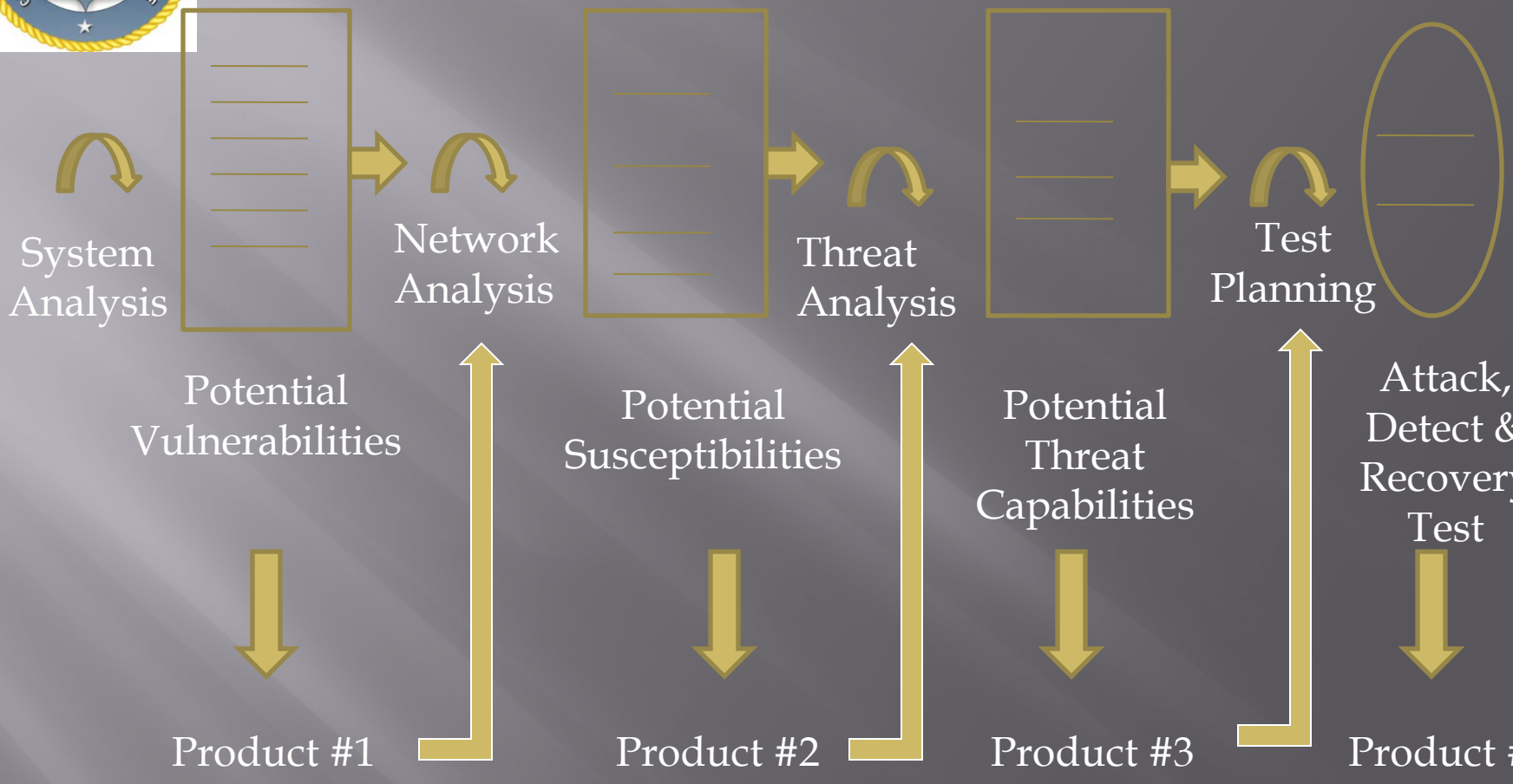
Some thoughts…

- IA/CND test and evaluation requires a holistic approach that views contractor testing, government DT and OT as a continuum
  - Program Managers must work to integrate Government and Contractor Developmental Testing
- The evaluation strategy must be based upon sound architectural views that provide sufficient rigor
  - The OT&E community should support JFCOM efforts to improve the quality of net-centric architectural views
- New tools must be developed to support the collection of system performance data without unduly impacting the performance of the system under test
- A new paradigm for examining how we assess the ability of our systems to support combat operations in the face of cyber attack is needed

A Suggested Analytical Process

- Determine the *criticality* of the system and the security *required*
- Assess *non-physical* and *physical* vulnerabilities
- Consider susceptibility to *espionage, disruption* or *malicious manipulation*
- Assess threat capability and test using *the types of exploits likely to be encountered in the operational environment*
- Assess recovery and repair, (recognizing that unlike kinetic attack, *detection of the attack may not be obvious*.)

Proposed Analytical Process

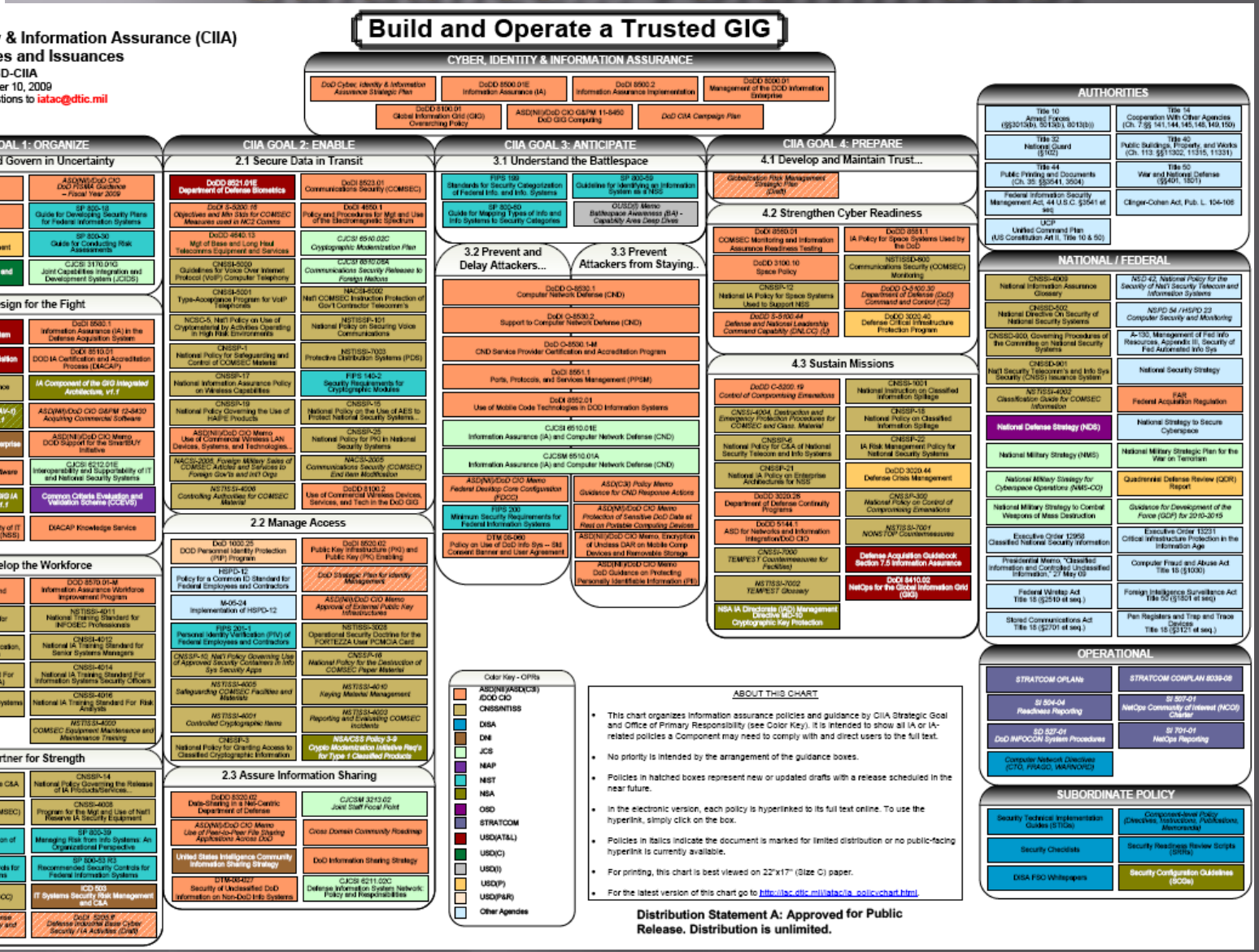


Summary

- Challenges are similar, yet different:
  - Well defined requirements
  - CONOPS
  - Instrumentation
  - Skilled personnel

- Bottom line – we are confronted with a rapidly evolving warfare domain with associated risks and opportunities - we need to get this right!

IA Policy and Guidance…Voluminous!



Bill McCarthy
Deputy, Operational Test & Evaluation Force
Norfolk, VA
757.282.5546 Ext. 3900
William.mccarthy@cotf.navy.mil