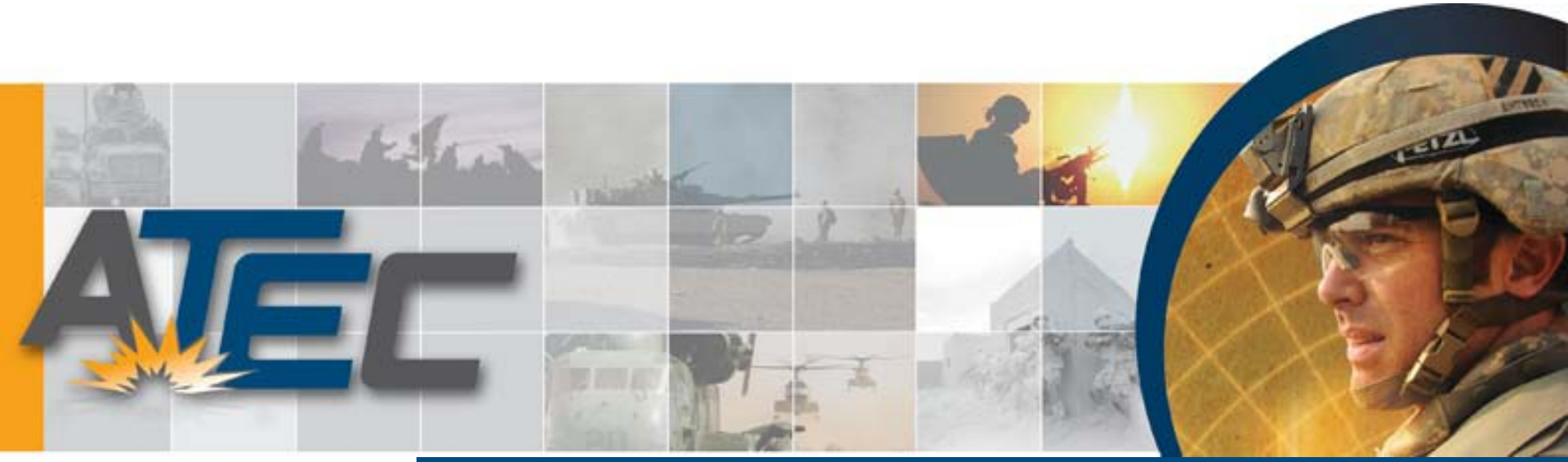


Implementation of Defense Test & Evaluation in a Net-Centric World

MG Roger Nadeau

2 March 2010

Army Proven
Battle Ready

Outline

- Information Assurance Challenges
- Information Assurance Opportunities
- Information Assurance Issues
- Implementation of the 21 Jan 09 DOT&E Procedures for OT&E of IA in Acquisition Programs.

Information Assurance Challenges

- Combat Developer Requirements: Net Ready-Key Performance Parameter vice Fight Through Computer Network Attack.

- DOT&E Six Step Procedures: Need a common understanding and application across all Services, within DOT&E, and application to Business Systems and Tactical/Operational/Strategic Systems.

- Materiel Developer Requirements: Certification vice MDA review of Effectiveness, Suitability, and Survivability.

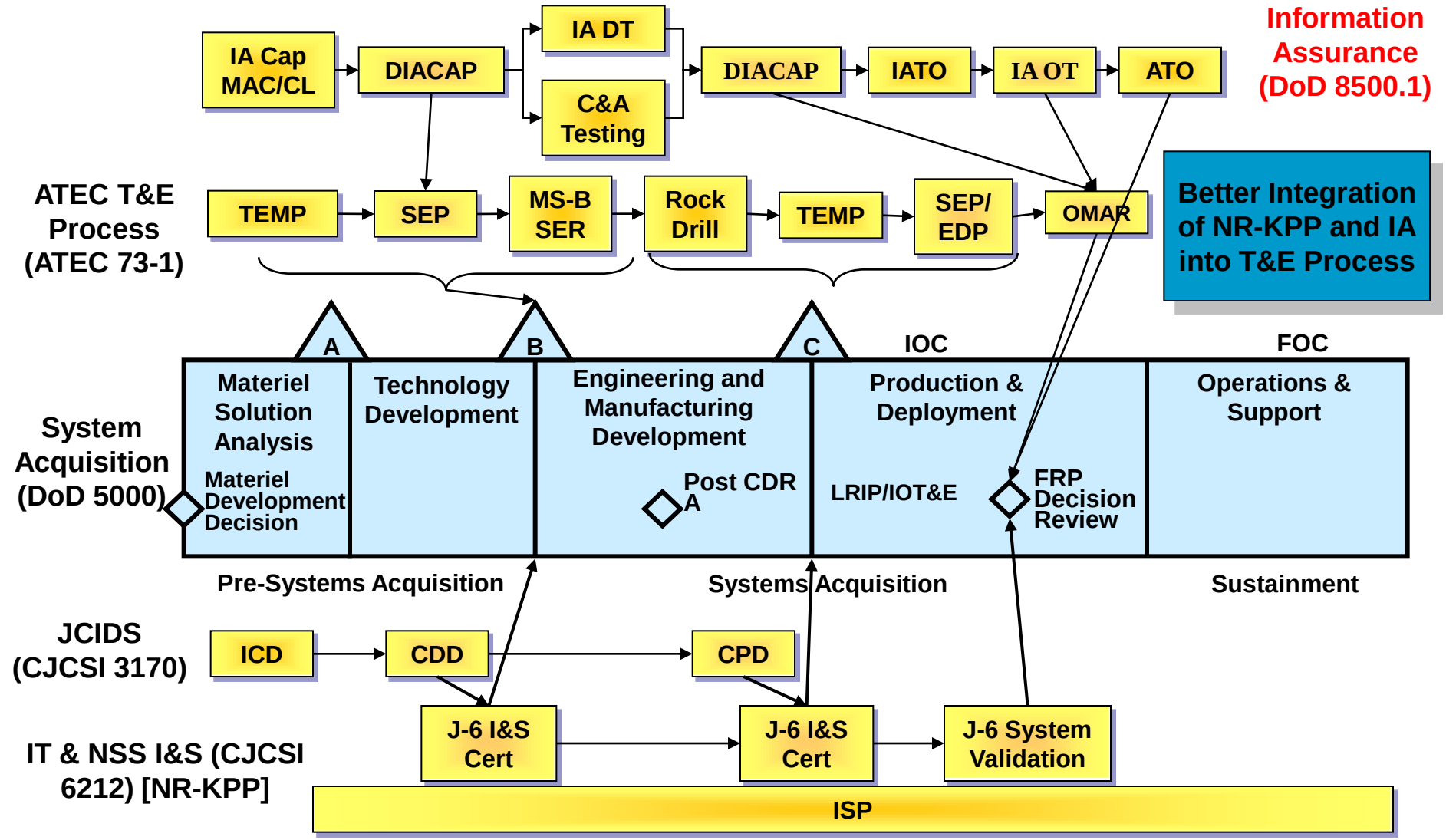
Information Assurance Challenges (2)

- IA OT&E Planning: Planning and resourcing to ensure appropriate integration of DT, OT, and “threat” into the evaluation.

- Threat Representation: Policy, Threat Manager, Threat Computer Network Operations Team, Test Threat Support Package, Memorandum of Agreement, and Threat Accreditation Working Group.

- Policy
  - DoDI 5000.02
  - AR 380-53
  - ATEC PAM 73-1
  - ATEC IA Technical Note

Information Assurance Opportunities



IA Opportunities (2)

- Collaboration: DOT&E WG(all OTAs), ATEC IA WG, CIO/G6, ARL/SLAD, AMSAA, TSMO
- Refining our Methodology with Future Protection, Detection, Reaction, and Restoration Evaluations
  - GFEBS LUT 2010
  - IBCT LUT 2010
  - JTRS GMR/HMS LUT 2010
  - GCSS-Army LUT 2010
  - THAAD LUT 2010
  - WIN-T IOT&E 2011
  - UAS ER/MP 2011
  - DTS LUT 2011
  - FBCB2 LUT 2011
  - JTRS IOT&E 2011
  - JTRS GMR IOT&E 2012
  - DCGS-A IOT&E 2013

IA Opportunities (3)

- FOT&E: ATEC COCOM IATF
  - US Army as a Service
    - All active division and Corps networks, devices, and applications are looked at from an IA perspective during their MRX prior to going to the CENTCOM AOR
  - USCENTCOM
    - CENTCOM requests ATEC IATF by name to look at their Service components forward HQs networks, devices, and applications within the AOR as well as any standing Joint and or combined Task Force.
  - USEUCOM, USAFRICOM, USSOCOM,USSOUTHCOM,USFK
    - The IATF also looks at the networks, devices, and applications riding not only the garrison networks but also the Service Components as well as the Joint Task Force tactical networks belonging to each of these COCOMs.

Information Assurance Issues

- Holistic evaluation approach to complex System of System Interoperability and Computer Network Defense
  - NR-KPP metrics are compliance-based checklists, open to individual interpretation.
    - Lack system and operational mission requirements
    - ATEC developing mission-based T&E strategy to assess interoperability activity
  - NR-KPP is too broad and vague to alleviate interoperability issues.

- IA OT&E for Army Capability Sets Acquisition and ARFORGEN
  - ATEC System Team working on Operational Evaluation Strategy to include data sources.
  - ATEC IA Working Group addressing this challenge to seek best way to integrate IA OT&E into the evaluation process.

Implementation of DOT&E Procedures for OT&E of IA

- 21 Jan 09 Procedures supersede the 21 Nov 06 DOT&E Policy for OT&E of IA in Acquisition Programs.
  - Determination of Policy applicability (Step 1)
  - Initial IA Review (Step 2)
  - OT&E IA Risk Assessment (Step 3)

  → Procedural Steps

  - Operational IA Vulnerability Evaluation (Step 4)
  - Operational PDRR Evaluation (Step 5)
  - Continuity of Operations Evaluation (Step 6)

  → OT Steps

Evaluate a system's

PROTECT, DETECT, REACT, RESTORE

capabilities in an operationally realistic environment