The Operator Link in Cyber Security Evaluations

Presented by Robert Wojciechowski, Technical Director (IPS), Integrated Suitability and Methodology Evaluation Directorate, U.S. Army Evaluation Center

For ITEA Cyber Workshop

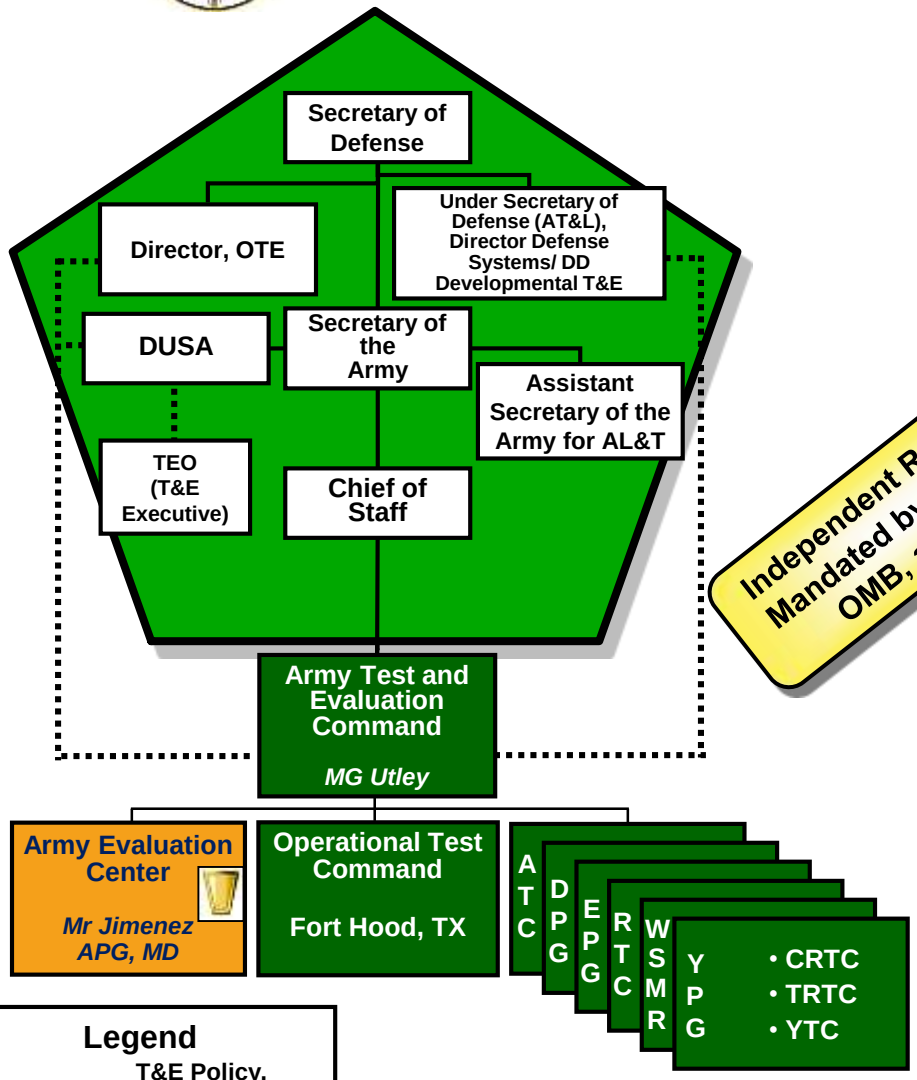
24-26 February 2015

U.S. Army Test and Evaluation Command

Purpose

- Explain ATEC's and AEC's mission and organization
- Provide a warfighter perspective by discussing observations and soldier feedback from recent suitability evaluations of C4ISR programs

Where We Fit



Independent Reporting Mandated by US Code, OMB, and OSD

Why We Do It

- **General Orders No. 13, Signed CSA 16 Oct 06**
- **LAW (Section 139, Title 10, U.S. Code)**
  - Establish office of Director, Operational Test and Evaluation
  - Requires annual report to Congress for oversight systems
- **LAW (Section 2366, Title 10, U.S. Code)**
  - Live Fire Test & Evaluation
    - Requires survivability testing of major systems meant to protect their occupants
    - Requires lethality testing of munitions
    - Requires a LFT&E test report to congressional defense committees.

LAW (Section 2399, Title 10, U.S. Code)

- Defense Appropriations Act
  - Requires **independent** Initial Operational Test & Evaluation (IOTE) before proceeding beyond low-rate initial production (LRIP) for all major defense acquisition programs
  - Three qualifications - production or production-like materiel; typical users; realistic conditions
  - Limits system contractor involvement in **IOTE**

- **LAW (Section 2400, Title 10, U.S. Code)**
  - Low-Rate Initial Production (LRIP)
    - Quantities for IOTE are established by the DOT&E for oversight systems, and by OTAs for others

AR 73-1: "USATEC is the Army's independent operational test activity"

U.S. Army Evaluation Center

We are the E in Test and Evaluation

AEC Mission Statement: To plan, support, conduct and provide independent evaluations, assessments, and experiments in order to provide essential information to decision-makers.

AEC Core Competencies:

a. Evaluate effectiveness, suitability, and survivability (ESS) independently

b. Verify system safety

c. Direct test strategy

ESS + S

AEC Vision Statement: AEC continues to grow as the premier Department of Defense independent evaluation center through fair, honest and accurate system assessments.

Motto – ***Understanding***

Operational Suitability

AR 73-1: The degree to which a system can be satisfactorily placed in field use with consideration given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistics supportability, and training requirements.

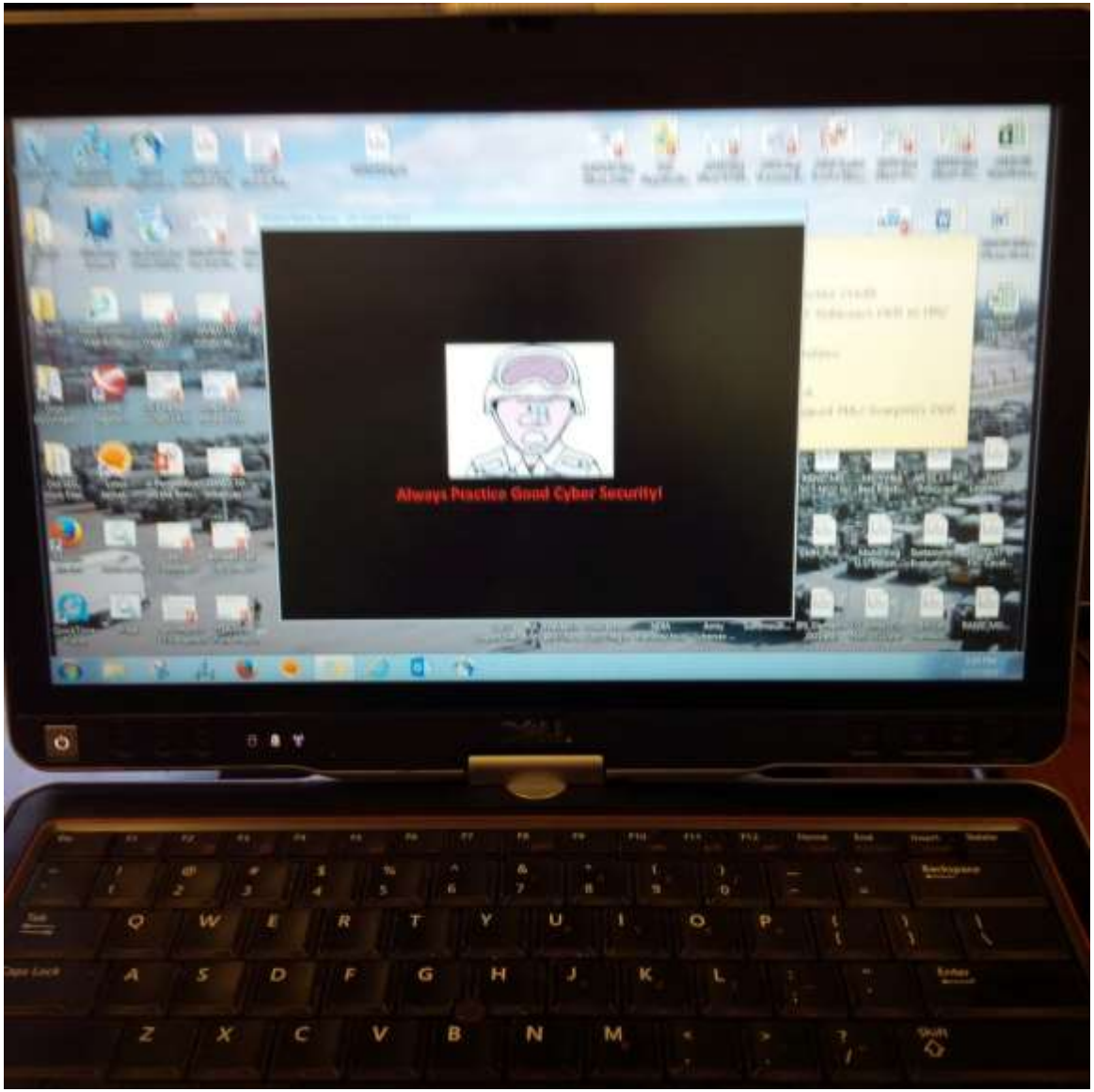
Working definition:

- Suitability = [RAM + IPS + HSI + other] DOTML-PF
- Safety of maintainers, transporters, supply, and other support personnel

Evaluation approach

- Information requirements (and questions)
- Data source matrix:
  - Effective
  - Suitable
  - Survivable
  - Safe
- Operationally realistic environment:
  - Missions
  - Environment
  - Threat
- Requirements + Doctrine + Policy + Regulations

ESS + S


Always Practice Good Cyber Security!

Recent Observations - RAM

- Reliability – required vs. demonstrated
- Attack window = no reliability faults?
- Faults vs. rapidly recoverable event (RRE)
  - Rebooting → lost work and time
- Incident chargeability – system (hardware or software) or operator?
- Fragile designs (components, USB connections, cables)
- System of systems (SoS) and system of SoS root cause and failure analyses
- Weather effects (water, hot/cold)

Recent Observations - IPS

- General purpose users (GPUs)
- Operator, maintainer, S6, and leader training:
  - Is rebooting an official repair technique? When?
  - Component-level focus (vs. network system)
- Troubleshooting (expected & unusual conditions)
- Help Desk
- Organic (including LARs) vs. FSR maintenance
- Special tools, equipment, and skills
- Electrical power (vehicle, dismounted, tactical, grid)
- Batteries (types, life, re-charging)

Recent T&E Observations - HSI

- Black box = “blind faith”
- Training – scope and retention
- Displays (glare, icons)
- Workload
- Usability (complexity, capabilities)
- Control panels – gloves, touch screens
- Integration onto dismounted warrior (basic load)
- User trust and confidence in their TTPs, equipment, and security

Summary

- Realistic operational testing:
  - Trained soldiers – operators, maintainers, S6, and leaders
  - Up-to-date SOPs and TTPs
- Difficult to duplicate and isolate reliability problems; “Noise of the Network”
- Recognizing an attack, protecting the network, and restore lost capability
- Soldier trust and confidence in equipment and operational security

Commercial market drives soldier expectations