Improving Cybersecurity Test and Evaluation at the Army's Network Integration Evaluation (NIE)

Keith Wise
13 November 2013

U.S. Army Test and Evaluation Command

Agenda

- About AEC and AEC Survivability
- What is NIE?
- Current NIE Cyber testing overview
- NIE Limitations
- NIE Recommendations

About AEC

Army Evaluation Center (AEC) plans, supports, conducts and provides independent evaluations of Army acquisition programs.

AEC Survivability ensures that Soldiers can complete tasks and accomplish missions in threat environments using Army materiel.

.

What is NIE?

The **Network Integration Evaluation (NIE)** is the Army's series of semi-annual, Soldier-led evaluations designed to further integrate and rapidly progress the Army's tactical network**.**

- Systems Under Test (SUT's) and Systems Under Evaluation (SUE's)
- Evaluate the Capability Set network architecture
- Led by "TRIAD" consisting of Army Test and Evaluation Command (**ATEC**), the Brigade Modernization Command (**BMC**) and the System of Systems Engineering & Integration (**SoSE&I**) Directorate

Systems evaluated at recent NIEs include WIN-T, JWARN, CPoF,JTRS, JBC-P, Net Warrior

Current NIE Cyber Testing Overview

- Vulnerability scans of SUEs prior to NIE record test (SoSE&I)

- STEP 4* testing of SUTs prior to NIE record test
- STEP 5* testing during NIE record test
  - Evaluation of Protection, Detection, Reaction, and Restoration capabilities during NIE record test

* DOT&E Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs

DOT&E Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs

Current Six-step Process steps 4-6

- Operational IA Vulnerability Evaluation (Step 4)
- Protection, Detection, Reaction, and Restoration Operational Evaluation (Step 5)
- Continuity of Operations Evaluation (Step 6)

DoD currently redesigning Six-Step process to examine earlier DT cyber security testing: "OSD Shift Left".

AEC Survivability reorganizing to support new process.

Current NIE Cyber Testing Limitations

- Cyber (Step 5) and Performance testing done simultaneously
- Systems not ready for cyber security testing
- Conducting two events per year creates overlap with planning and execution (14.1 execution same time as 14.2 planning)
- No true test of system Restoration capabilities

NIE Cyber Testing Recommendations

- Separate Performance and Cyber security testing into two distinct NIE events.
- Implement “shift left” test methodology
- Change to annual event
- Evaluate restore capabilities by simulating a disaster and observe unit’s ability to rebuild the network.

NIE Cyber Testing Advantages and Disadvantages

Advantages:

- Creates more realistic and thorough Cyber test and evaluation
- Shifting testing to the left will identify issues earlier in the program lifecycle
- Separating out the cyber testing will allow a true performance assessment of the network in a benign environment
- Enables evaluation of restoration capabilities

Disadvantages:

- Increases test length which will increase overall cost.
- Delays reporting timeline

QUESTIONS