U.S.ARMY

PEO C3T

PROGRAM EXECUTIVE OFFICE COMMAND CONTROL COMMUNICATIONS-TACTICAL

International Test and Evaluation Association (ITEA) 2nd Cyber Security Workshop

25 February 2015

Mr. Jerry Cook

Program Executive Office for Command, Control and Communications-Tactical

Cyber Defense Against the Unknown Enemy

Cyber attacks threaten Army networks and information every day. PEO C3T is charged with protecting the systems that make up the tactical network and providing Soldiers the tools they need for an active defense.

Focus areas:

- *Lock down data that rides on the network, limiting damage caused by a breach*
- *Provide additional security and visibility but maintain simplicity*
- *Two-factor authentication*
- *Biometrics tailored to meet the unique demands of the tactical environment*

Establishing the Cyber Focal

- ASA(ALT) maintains the Cyber Focal to coordinate materiel programs across the Army
  - *Synchronization across Army acquisition is increasingly important in SoS environment*
  - *Acquisition process must enable quick proactive insertion of technology when it becomes available*
- ASA(ALT) defines cyber requirements and priorities, then funnels through appropriate Program Executive Offices (PEOs) who provide materiel solutions
- Integrates both offensive and defensive cyber efforts
- Three PEOs key to materiel solutions:
  - Program Executive Office for Command, Control and Communications-Tactical (PEO C3T): Defensive cyber operations
  - PEO Enterprise Information Systems (PEO EIS): DoD information network operations and enterprise
  - PEO Intelligence, Electronic Warfare & Sensors (PEO IEW&S): Offensive cyber operations

PEO C3T Cyber Operations & Defense

Mission: To provide a full-spectrum, system-of-systems approach to advancing and synchronizing cyber security, information assurance and information management across PEO C3T.

- New organization created in response to growing cyber mission across the Army
- Single synchronization point to enable information security and compliance across the PEO, PMs and tactical systems
- Responsible for implementing policies, standards and procedures to ensure a secure information-sharing environment for the PEO's daily operations and the Army's tactical network

PEO C3T Priorities

As ASA(ALT) defines requirements, PEO C3T will work materiel solutions focused on defense of the tactical network.

Priorities: Deny, Detect, React, Restore

PEO C3T Cyber Initiatives

- **AUTHENTICATION**
  - Simple ID and Password
  - Active Authentication
- **IMPROVED SITUATIONAL AWARENESS**
  - Tactical Insider Threat Detection
  - Adversarial Reasoning and Attack Prediction
  - Signature Based Detection
- **SIMPLIFICATION**
  - Reduce Footprint
  - Single Tactical Computing Environment
- **NETWORK/SYSTEM MANAGEMENT**
  - Configuration Management
  - Streamlined Patching
  - Self-healing

Army S&T Community

Academia and private industry

Smart Testing for Cyber

- Strengthen the acquisition-test partnerships that exist today
- Align testing approach to innovative and adaptable systems
- Advance requirements for smart, agile testing for cyber
- ATEC, ARCYBER, ASA(ALT) and the PEOs are contributing to test strategy to better examine cyber protection early and often at the system-of-systems level
- Cyber risk reduction and emerging technology evaluated at the Army's federated labs at APG
- Followed by "red" and "blue" cyber teaming at the Network Integration Evaluations (NIEs)

PEO C3T Path Ahead

- Empower Soldiers' defensive efforts through a network that is cyber-hardened, anticipates threats and is self-healing
- Work with PEOs IEW&S and EIS to map out technology goals
- Advance emerging capabilities:
  - Authentication: Simple ID/Password; Active Authentication
  - Improved Situational Awareness within the Cyber environment: Tactical Insider Threat Detection; Adversarial Reasoning and Attack Prediction; Signature Based Detection
  - Simplification: Reduce Footprint; Single Tactical Computing Environment
  - Network and System Management: Configuration Management; Streamlined Patching; Self-Healing Network