Panelists

• LTC Sung In, Product Manager for Tactical Cyber and Network Operations (PdM TCNO), PM Tactical Network
• Mr. David Arty, Chief, Certification and Accreditation Branch, CCDC C5ISR Center Software Engineering Directorate
• Mr. Brian Lyttle, Chief Cybersecurity and Information Assurance Division, CCDC C5ISR
• Ms. Denee Lake, Cybersecurity Branch Chief, PM Mission Command
What is NetOps?

Joint Publication 6-0, Joint Communications Systems (June 2015), defines NetOps as the activities conducted to operate and defend the GIG. NetOps provide integrated network visibility and end-to-end management of networks, global applications, and information services.

FM 6-02 (Signal Support to Operations) – September 2019
The DODIN-A and automated information systems enhance the ability to plan and coordinate operations across staff sections, cells, command posts, and echelons. Signal Soldiers—
- Install, Operate, Maintain, and Secure the DODIN-A (DODIN operations and COMSEC).
- Formulate signal support plans as part of the military decision-making process.
- Conduct information management.

ATP 6-02.71 (Techniques for Department of Defense Information Network Operations) – April 2019
1-31 Department of Defense information network operations are operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network

1-34 DODIN enterprise management is the technology, processes, and policies necessary to execute the DODIN operations functions to install, operate, maintain, secure, and restore communications networks, information systems, and applications.
Simplifying Interfaces

Where UNO Fits into AFC Network Modernization Plan

Current  | UNO v1.1 & v1.2 / CS23 & CS25  | UNO CS27  
          | FY21-FY24                       | FY25-FY26  

Intuitive and simplifying NetOps tools

Common look and feel

UNCLASSIFIED/FOR PUBLIC RELEASE
Software Assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner.

**SERVICES**
- Static & Dynamic Code Analysis
- Finding Alignment to RMF control requirements
- Risk Assessments of findings

**PROGRAMS SUPPORTED**
- Tactical Systems (Government off the shelf, open source and Commercial off the shelf applications)
- SEC government developed applications
- Other programs as requested

**FUTURE PATH**
- Army Software Assurance Program
- Automation/Expedition of Assessment Process

**CHALLENGES**
- Measuring and establishing confidence for software assurance requirements for Army
- Personnel Training/Skillsets Programs
U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – C5ISR CENTER

Cyber Security and Information Assurance (CSIA) Division Services and Products Overview

Brian J. Lyttle
Chief, CSIA Division
C5ISR Center
CSIA MISSION & OBJECTIVES

Mission
Conduct applied research and development of cyber capabilities while operating and defending key cyber-terrain in order to increase the mission effectiveness of the US Army, JIIM and DIB partners.

In the News
- Radio Interoperability Capability-Universal (RIC-U)
- Tactical, Wearable PKI tokens (TIDAM)
- Cyber Situational Understanding
- Commercial Solutions for Classified (CSfC)

Contract Opportunities
(note: we don’t purchase many products)
- Broad Agency Announcement
- Request a TIM
• Potential Cooperative Research and Development Agreement (CRADA)
  – REprogrammable Single Chip Universal Encryptor (RESCUE)
  – AI/ML Defenses and usage in Defensive Cyber Operations (DCO)
  – Data Provenance
  – Commercial Solutions for TRANSEC (CSfT)
  – Hardening against Quantum based threats
  – Deterrence and Obscuration
  – Network Monitoring / Insider Threat

• Army laboratories authorized to provide testing support service to commercial partners IAW 10 USC § 2539b (eg Fee for Service)
  – Type 1 encryptors (HAIPE) assessments
  – Software Q/A IAW Risk Management Framework
  – Commercial Solutions for Classified (CSfC)
  – Cross Domain Solutions (CDS)
  – Tactical Secure Voice Interoperability (TSCVIS)
  – Lab based vulnerability assessment of devices
  – Cybersecurity Service Provider (CSSP)
• Technology demonstration opportunities
  – NETMOD-X
  – MDO-C (formerly CYBERBLITZ)
  – Technical Support & Operational Analysis (TSOA)

• Technology Transfer Opportunities
  – REprogrammable Single Chip Universal Encryptor (RESCUE)
  – Cyber Situational Understanding software (Cyber SU)
  – Radio Interoperability Capability (RIC-U)
• BLUF: Products originally produced for enterprise environments routinely fail to perform or overwhelm operators with complex work arounds and infrastructure.

Program Management Office (PMO) Priorities:
1. Integration into Opns
2. SWaP req’ts
3. Sustainment needs
4. Performance

Physical Environment:
•Disconnected / Intermittent / Low-bandwidth
•130F ← Temp → -30F
•Spectrum availability
•Moisture / Dust
•Expeditionary / Mobile

Organizational:
•Initial 72 hrs autonomous opns
•Always Coalition / Joint partners
•IT services provided by COCOM/DISA
•Multiple classifications / X-Domain needs
•No supporting infrastructure

Human:
•High OPTEMPO
•Capture / compromise
•Austere conditions
•Low density skill set
•Warfighter Age <=28
•SOFA & LOG limit SME support
### Project Manager Mission Command

#### Current Initiatives
- Product Manager, Tactical Mission Command
- Product Manager, Joint Battle Command – Platform
- Product Lead, Mission Command Cyber
- Product Lead, Mission Command Support Center

#### Ongoing Challenges
- Configuration Management
- CDS “Raise the Bar”
- Cloud
- Containerization

#### Where Industry Can Help
- Supply Chain Risk Management
- Automation for Cybersecurity Ease of Use
- Design for sustainability

UNCLASSIFIED/FOR PUBLIC RELEASE