Association for Enterprise Information

Achieving Joint Force 2020
Through
Coalition Information Sharing

Mr. Stuart Whitehead
Deputy Director
Cyber and C4 Integration
Joint Staff J6
Defeat Aggression: …The United States will use military force in concert with allies and partners whenever possible, while reserving the right to act alone if necessary…

Capabilities - Our strategy, forged in war, is focused on fielding modular, adaptive, general purpose forces that can be employed in the full range of military operations. Joint Forces will improve their ability to surge on short notice, deploy agile command and control systems, and be increasingly interoperable with other U.S. government agencies…. 
The Afghan Mission Network Lessons Learned

• U.S. use of SIPRNET during mission partner operations generates strategic, operational and tactical limitations:

  – [Lack of] Flexibility to combine US and Allied forces (Afghanistan)
  – US norm of coordinating ops on SIPR (Afghanistan & Libya)
  – Unclassified capability to rapidly and seamlessly direct HA / DR operations with wide array of mission partners, i.e. non governmental organizations e.g. Red Cross (Haiti)
  – Different networks with inadequate cross-domain solutions resulted in poor ops, planning and intelligence information exchange between U.S. and NATO forces in ISAF

• Operational Requirements should be oriented to Coalition Data Sharing and enterprise mission based execution

• Need for human-to-human information exchange in a common language on same security level in real time
• On 26 Aug 2011 the Chairman Joint Chiefs of Staff (CJCS) directed the evolution of the Future Mission Network to enable more effective operations with mission partners.

• A 90 study was complete by November followed by a briefing to the tank at which time the term “FMN” was replaced by Mission Partner Environment (MPE)

• NATO issued similar guidance to Allied Command Transformation. US J6 assisted ACT in their assessment.

• The analysis yielded NATO Federated Mission Networking (FMN) which, by design, was identical to US MPE.
Way Ahead:

• Leverage the best of the Afghan Mission Network

• Evolve to a more agile and documented way forward

• Explore the ability for nations to “come as you are” and connect

• Ensure the FMN/MPE supports all types of missions, partner arrangements and security level (Unclass/Classifed)

• Focus on the non-material aspects of the challenge
Mission Partner Environment

Core Common Services

- Chat
- E-mail (with attachments)
- Voice Over IP (VOIP)
- Video Teleconferencing (VTC)
- GAL (Sharing Directories)
- Web-Browsing (Allowed)

Mission Threads define the authoritative data, where data is collected, where data needs to be accessed from, data classification, types of decision aids ...
Joining, Membership and Exit Instructions

- Afghan Mission Network (AMN) – Joining, Membership and Exit Instructions (JMEI) – Version 3.1

- Afghan Mission Network Steering Group transformed to support Resolute Support mission and Federated Mission Networking (FMN)

- Evolve to a more agile and documented way forward
  - NATO FMN Implementation Plan (NFIP) Instructions
  - US JMEI

- Ensure NATO and US efforts are synchronized
LEGEND

- FMN National Contribution (3rd Stack); Nat’l DOTMLPF, IA, Security
- National Classified Network (e.g. SIPRnet)
- National Unclassified Network (e.g. NIPRnet)
- NATO Federated Mission Network; Commander accepts risk, sets rules
- NATO Classified Extension
- National Network Extensions

**Presence of country flags does not imply an actual agreement or connection**
Coalition Interoperability Assurance and Validation (CIAV)

- Improve global interoperability

- **Implement and execute:**
  - Coalition focused, mission based process
  - Persistent Environment
    - Experimentation
    - Development and Operational Testing
Future information exchange solutions must:

• Respond to warfighter needs

• Be data standards driven

• Allow agile implementation

• Be easily composable

• Be easily scalable

• Accommodate a diverse user community

• Quickly integrate unanticipated users

• Incorporate a “trust but verify” approach
Key to Globally Integrated Operations is Interoperability

• The continual search for interoperability has been and continues to be defined by the communities which seeks it.

• What works for one community may not work for another; therefore, the interoperability standards for one community are usually not interoperable with another – yielding tailored solutions.

• Contemporary operations demand increased information sharing, often between un-forecasted entities.
Where do we go from here?

Paradigm Shift: Think inside, but start outside!

If everyone did it like me, we would be interoperable!

If I did it like you, I would have to change everything!

What would allow me to do what I want, but still communicate with everyone?

It's all about me!

It's all about us!
Standards-Based Approach for Information Exchanges

The National Information Exchange Model (NIEM) provides a potential way forward:

- Not a military “invention”
- Repeatable process for designing an information exchange
- Uses a collection of agreed, reusable data components
- XML-based
- Allows machine-to-machine data exchange to be implemented faster and at lower cost
- Approach already successfully demonstrated in a Mission Partner Environment
C2 / WMA Data Exchange Standards Management

Tactical Interoperability Standards Management

JS Representative/Warfighter advocate for Link 11, Link 16, VMF, IBS, USMTF, NATO STANAGs

National Information Exchange Model (NIEM)

Aligning US and NATO Data Strategy

US UCore and C2 Core (2009)
NATO Data Sharing CaT (JS J6 DSD Lead)

NATO Net-Enabled Data Strategy (2008?)
NATO XML Labeling (NXL) (2011)
NATO JC3IEDM Way Ahead (2012)
NATO Core Data Framework (2014?)

Data and Service Piloting Activities

MilOps-GML Interoperability Experiment (MOGIE)
Italian Mod & Sim Center of Excellence (M&S COE)

Geospatial Visualization Service Proof of Concept (GVS – MilOps)
TIES – Tactical Infrastructure Enterprise Services

Tactical Edge Data Solutions (TEDS)
TBD CCMD/Service/Agency NIEM Adoption Pilots
Software Encryption

NSA “Suite B” software encryption

Commercial off-the-shelf (COTS) security solution

- Public standards, protocols, algorithms and modes for protecting classified information
- Eliminate the need to transport bulky equipment
- Ease the burden of deployed forces

Prototype Assessment

Objective:
Ensure this new capability meets NSA requirements and needs of the Warfighter

Software encryption methods may finally address this long standing issue.
Are We Ready?
For Day 1 of
Mission Partner Ops

UNCLASSIFIED
Way Ahead - Train as We Partner

- CIWX
- Combined Endeavor
- Viking
- Pacific Endeavor / Talisman Saber
Questions ?