Delivering the Mission
Partner Environment Now
Mobile data anywhere, anytime, any device

Panel Discussion

Terry L. Carpenter, Jr.
Services Development Executive (acting)
15 June 2017
Panelist

Moderator:
- Mr. Terry Carpenter, Services Development Executive (Acting)

Panelist:
- Ms. Heidi Cotter, MNIS PM
- CW5 Bill Winkler, Technical Advisor to the Director
- Mr. Lenart Clark, DEC-TK Chief Engineer
- Dr. Brian Hermann, Enterprise Services Division Chief
Multi-National Information Sharing

Evolving to MPE-IS

Ms. Heidi Cotter
MNIS PM
Joint/Allied Coalition Information Sharing Capabilities

Mission Partner Environment Information Systems (MPE IS)
- Global Virtual Data Centers (VDC) - 2 Funded, 4 Unfunded
- Mission Partner Gateway
- Enterprise Cross Domain
- Virtual Desktop Infrastructure (VDI)/Multi-Enclave Client (MEC)
- MPE Test Environment
- Common Mission Transport (CMNT) w/Type 1 and Gray Core
- Enterprise-based Pegasus (ECVoIP, GVS, Enterprise Email, DCS)
- UISS APAN Cloud
- UISS-Controlled Unclassified Information (CUI)

Multinational Information Sharing
- Combined Enterprise Regional Information Exchange System (CENTRIXS)
- Combined Federated Battle Laboratories Network (CFBLNet)
- Common Mission Network Transport (CMNT)
- Pegasus
- Unclassified Information Sharing All Partners Access Network (UISS-APAN)

Legacy
Current
Immediate Target
FY17-FY24

✔ Deployed and Operational
☐ Under Development
MPE-IS Global Laydown Plan (FY16-22 Projected)

BICES-X Trusted Network Environment (TNE)
Intel Community

CONUS VDC1
(Tampa) In Progress

CONUS VDC2
(TBD)

OCONUS VDC2
NAVCENT/DISA
Operational

OCONUS VDC1
(Wiesbaden)

OCONUS VDC3
(Yokota AB)

OCONUS VDC4
(Wahiawa)

Transport: CMNT; SIPRNet; Internet

Mission Partners

Garrison Commands

Mission Partners
# Current DISA-Managed Coalition Information Sharing Systems

<table>
<thead>
<tr>
<th><strong>VDC (MPE IS)</strong></th>
<th><strong>Mission Partner Environment Information System (MPE IS) Virtual Data Center (VDC)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Provides a multi-enclave virtualization system that delivers the same functions as a physical data center and can host multiple discreet mission enclaves.</td>
</tr>
<tr>
<td></td>
<td>Currently supports AFRICOM’s AMNET.</td>
</tr>
<tr>
<td></td>
<td>13 standard COTS applications.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CFBLNet</strong></th>
<th><strong>Combined Federated Battle Laboratories Network (CFBLNet)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Provides network infrastructure to test technologies and training exercises with mission partners.</td>
</tr>
<tr>
<td></td>
<td>Partnership with 31 core mission partners and 4 guest mission partners.</td>
</tr>
<tr>
<td></td>
<td>11 network service tools.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Pegasus</strong></th>
<th><strong>Pegasus</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Provides the means for disseminating classified information between coalition partners.</td>
</tr>
<tr>
<td></td>
<td>Pegasus services (Web browsing, Emails, SharePoint, Unified Communications, Chat).</td>
</tr>
<tr>
<td></td>
<td>Pegasus National Network Operation Center (NNOC) and Coalition NOC.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CENTRIXS</strong></th>
<th><strong>Combined Enterprise Regional Information Exchange System (CENTRIXS)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allows the US and coalition nations and their forces to securely share operational and intelligence information in mission enclaves.</td>
</tr>
<tr>
<td></td>
<td>Bi-lateral and Multi-lateral enclaves connecting 200+ organizations 24/7/365.</td>
</tr>
<tr>
<td></td>
<td>Chat, Email and other COTS services.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CMNT</strong></th>
<th><strong>Common Mission Network Transport (CMNT)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Provides a transport for coalition information sharing (Replaces the use of SIPR).</td>
</tr>
<tr>
<td></td>
<td>CMNT is available at any Defense Security Service (DSS) location.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>UISS-APAN</strong></th>
<th><strong>Unclassified Information Sharing (UISS) All Partners Access Network (APAN)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Provides the single enterprise solution for sharing non-classified info supporting DOD Exercises and Humanitarian Assistance / Disaster Relief Mission.</td>
</tr>
<tr>
<td></td>
<td>&gt;150K+ users, 100+ nations and 4K+ COIs.</td>
</tr>
<tr>
<td></td>
<td>Services (Blogs, Wikis, Conferencing, language translation, chat, email).</td>
</tr>
</tbody>
</table>
Virtual Data Center Overview

VDC provides a multi-mission enclave virtualization system that delivers the same computing, networking, and data storage functions of a physical data center

- Enduring computing infrastructure
- Episodically ready
- Rapid stand up mission enclave in days vs months (Meet “Fight Tonight” Rapid Response)
- Reduces hardware
- Centrally managed, de-centrally executed
- Standard set of services

Current Deployment:
- 1 node deployed
  - 3 Mission Enclaves
- 1 node funded and under development

Data Center Virtualization:
Multiple discrete MEs are converged on a single platform while maintaining distinct network separation.
Operational Use Cases
Mobile data anywhere, anytime, any device

CW5 Bill Winkler
Technical Advisor to the Director
Priority Use Cases

Use Case 1:
Headquarters user with a single workstation with access to multiple enclaves.

Use Case 2:
In theatre ability for tactical service component travel teams to provide the warfighter unified capabilities by working through multi-network enclaves when connected, as if in HQ, and working on single enclave in disconnected environment.

Use Case 3:
Privileged executive in theatre/on travel with ability to work on multi-network enclaves when connected, as if in HQ, and ability to work on single enclave in disconnected environment on a mobile device at classified level, to be treated as FOUO when off.
Use Case #3: Privileged executive in theatre/on travel with ability to work on multi-network enclaves when connected, as if in HQ, and ability to work on single enclave in disconnected environment on a mobile device at classified level, to be treated as FOUO when off.
Global Gray Core Service
Scaling DEC-TK Gateways

Mr. Lenart Clark
DEC-TK Chief Engineer
Global Gray Core (GGC) Service Concept

Enabling the Joint Information Environment
Enterprise Voice & Video
Cross Domain Service

Dr. Brian Hermann
Enterprise Services Division Chief
Enterprise Voice and Video Cross Domain Service

- Current environment increases costs, creates conferencing challenges, and impedes internal/external collaboration.
- Existing telephone infrastructures provide limited cross-domain interoperability, resulting in multiple independent devices at each workstation (i.e., MANY phones to MANY networks).
- ISDN/PSTN technology is ending.
- Legacy STEs need to be collapsed and tech refreshed into a common voice/video environment.
We need to coordinate across voice/video cross domain owners and relevant infrastructure service providers to create a global *enterprise* voice and VTC cross domain capability.

N! proliferation of individually managed CDSs for each security domain pair

Cost
Complexity
Redundancy
Lack of interoperability
Plan is to establish a core interconnected set of voice and video networks and expand as capability matures.

Enterprise Voice and Video Coalition Network (EVCNet) [Common Coalition Security Level]

Security Domain/Mission Enclave 1 (e.g., CENTRIXS)

Security Domain/Mission Enclave 2 (e.g., CENTRIXS)

Security Domain/Mission Enclave 3 (e.g., US BICES)

Security Domain/Mission Enclave 4 (e.g., REL/NATO)

Security Domain 5 (e.g., SIPRNet)

KEY
- ECVOIP Call manager
- Coalition ECVOIP Call manager (C-ECVOIP)
- SIP Trunk
- Cross Domain Gateway
- Phone
- VTC Workstation
- EVCNet Conference Bridge
- Call manager redundancy
Information Data Encryption Service (IDES)

Terry L. Carpenter, Jr.
Services Development Executive (acting)
Information Data Encryption Service (IDES)

Information Protection Evolution

- NOT just at the network level
- NOT just at the host level
- NOT just at the application level
- At the Data-Element Level

Data-Centric Protection
- Protection in transit
- Protection at rest
- Protection in use
- Traceability of information
This Incident Report details the Network Outage Reported in Ft. Bragg, NC. The affected nodes and users are depicted in the table below. This event was collected by the SolarWinds NNM, and has been confirmed by the Network Operations Team.

<table>
<thead>
<tr>
<th>Location</th>
<th>Ft. Bragg, NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident#</td>
<td>153512</td>
</tr>
<tr>
<td>REPORTING OFFICER</td>
<td>LT. JOHN DOE</td>
</tr>
</tbody>
</table>

This Incident Report details the Network Outage Reported in Ft. Bragg, NC. The affected nodes and users are depicted in the table below. This event was collected by the SolarWinds NNM, and has been confirmed by the Network Operations Team.

<table>
<thead>
<tr>
<th>Base 1</th>
<th>Base 2</th>
<th>Base 3</th>
<th>Base 4</th>
<th>Base 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lat.</td>
<td>Long.</td>
<td>Nodes</td>
<td>Users</td>
<td></td>
</tr>
<tr>
<td>30° 20’</td>
<td>40° 65’</td>
<td>10</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>30° 40’</td>
<td>40° 38’</td>
<td>2</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>30° 60’</td>
<td>40° 43’</td>
<td>15</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>30° 80’</td>
<td>40° 82’</td>
<td>4</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>40° 01’</td>
<td>45° 16’</td>
<td>2</td>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

*Not An Actual Event. For illustrative purposes only*
This Incident Report details the Network Outage Reported in Ft. Bragg, NC. The affected nodes and users are depicted in the table below. This event was collected by the SolarWinds NNM, and has been confirmed by the Network Operations Team.

<table>
<thead>
<tr>
<th>Base</th>
<th>Lat.</th>
<th>Long.</th>
<th>Nodes</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base 3</td>
<td>30° 60’</td>
<td>40° 43’</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base 4</td>
<td>30° 80’</td>
<td>40° 82’</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base 5</td>
<td>40° 01’</td>
<td>45° 16’</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Not An Actual Event. For illustrative purposes only*
This Incident Report details the Network Outage Reported in Ft. Bragg, NC. The affected nodes and users are depicted in the table below. This event was collected by the SolarWinds NNM, and has been confirmed by the Network Operations Team.

**Network Outage Report**

**Location**: Ft. Bragg, NC

**Incident #**: 153512

**REPORTING OFFICER**: LT. JOHN DOE

---

**Not An Actual Event. For illustrative purposes only**
Delivering the MPE-IS Now

- **Virtual Data Centers**
  - Multi-enclave virtualization system that delivers the same functions as a physical data center and can host multiple discreet mission enclaves

- **Global Gray Core (GGC) Service**
  - Commercial Solutions for Classified (CSfC) across public internet with multiple forms of encryption.

- **Information Data Encryption Service (IDES)**
  - Self-Protecting Data, and Differential Sharing while ensuring full data traceability.

- **Mobile C2**
  - Enterprise standards and solutions.
  - Access to various SIPR domains.
  - Access to secret releasable, coalition, and other non-DoD Mission Partners.

DISA currently standing up pilot for standard configuration of end point on Win10.
CAPE Program Decision Memorandum Action:
Executing an end-to-end pilot to assess the effectiveness, suitability and survivability/security of the MPE-IS

- **Development Test 1 (DT-1): Steadfast Cobalt 2017 Exercise (May 17)**
  - VDC mission enclave at Wiesbaden Global Node
  - Support building of JCSE enclaves
  - JITC validation of service

- **Development Test 2 (DT-2): TBD Exercise (Aug 2017)**
  - 3 VDC mission enclaves at Tampa Global Node
  - 1 VDC mission enclave at Wiesbaden Global Node
  - MEC solution
  - CSfC capability based on SOUTHCOM solution
  - JITC validation of service

Notional End-to-End Pilot Diagram
# IDES Policy Challenges

<table>
<thead>
<tr>
<th>Policy Document</th>
<th>Reference</th>
<th>Content</th>
<th>Challenges</th>
<th>Applies to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Software Extended Package for Redaction Tools (NIAP Version: 2.0)</td>
<td>RED_REM_EXT. 1 (Removal of Redacted Data) Page 17</td>
<td>Application Note: Selected content must be removed, not obscured by encryption, encoding, conversion to a proprietary format, or any other method</td>
<td>• The policy prevents the Information Data Encryption Service solution from using encryption software to redact information from a document &lt;br&gt;  • Current technology supports encryption for Top Secret data (e.g. AES-256) &lt;br&gt;  • Latest technology has not been tested by the DoD, due to policy limitations</td>
<td>DoDIN, All Coalition and Non-Coalition networks.</td>
</tr>
<tr>
<td>DoD Information Security Program: Controlled Unclassified Information (CUO) (Number 5200.01, Volume 4)</td>
<td>Page 7 #2 DODM 5200.01 vol. 1 - 4</td>
<td>UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall, in accordance with DoDD 5111.1 (Reference (g)), establish policies and procedures for disclosing DoD CUI to foreign governments and international organizations</td>
<td>• The policies prohibit the use of a single coalition enclave (flat network) &lt;br&gt;  • MPE-IS provides implementable efficiencies through network and computing virtualization, but does not reduce number of computing environments or network enclaves &lt;br&gt;  • Merging or collapsing of these bi-lateral and multi-lateral applications and enclaves is not practical without policy remediation</td>
<td>Controlled Unclassified Information (CUI)</td>
</tr>
</tbody>
</table>