Network Operations (NetOps)

COL Debbie Theall
Project Manager, PM I3C2
22 May 2013
Agenda

■ Context
■ NetOps Capabilities/Systems and Defensive Cyberspace Operations (DCO)
■ NetOps Operational Construct
■ Enterprise Service Management System as a Service (ESMSaaS)
■ Army Enterprise Service Desk (AESD)
■ Opportunities
U.S. Army NetOps capabilities have been generated, engineered, and procured in a decentralized manner across many commands and echelons.

Challenges:

- Disparate and non-interoperable systems/tools/configurations
- DOTMLPF – material solution is getting ahead of the other components
- Doctrinal Disconnects: NetOps, Defensive Cyberspace Operations, DoD Information Network Operations (DoDIN), Joint Information Environment (JIE) CONOPS
- Multiple NetOps and Cyber Working Groups/IPTs
- Maintaining “as is” while moving to the “to be” → Retrofitting the plane in flight

The Army needs a more centralized approach to defining, validating, procuring, and fielding NetOps capabilities.

Currently looking at 25 NetOps systems to buy as a service or as a library of tools.

Working closely with the NetOps Trail Boss (PEO C3T) for strategic/tactical integration of capabilities for LandWarNet 2020.
## NetOps Capabilities/Systems and Defensive Cyberspace Operations (DCO)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Network Management System (NetMan) (^{6+1})</td>
<td>Host Based Security System (HBSS) (^{6+1})</td>
<td>Network Access Control (NAC)</td>
<td>Database Element Manager</td>
<td>Enterprise Services Management System (ESMS) (^{6+1})</td>
</tr>
<tr>
<td>Network Intrusion Prevention System (NIPS)</td>
<td>Systems Management (SysMan) (^{6+1})</td>
<td>IAVM IP Network Vulnerability Scanner (^{6+1})</td>
<td>Domain Name Service (DNS) Management</td>
<td>Directory Services Management</td>
</tr>
<tr>
<td>Wireless Intrusion Prevention System (WIPS)</td>
<td>Storage Management System</td>
<td>Security Information Management System (SIMS) (^{6+1})</td>
<td>IP Capacity, Availability, &amp; Performance (CAP) Monitoring System</td>
<td></td>
</tr>
<tr>
<td>Firewall Element Management</td>
<td>Backup and Recovery Management</td>
<td>Identity Management System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy Management</td>
<td>Virtualization Management System (VSM)</td>
<td>Crypto Security Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router Element Management</td>
<td></td>
<td>IAVM Computing Platform Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Element Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Private Network (VPN) Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless IP Network Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* NDAA 2011 Section 933 stipulates the requirement to provide cyber quick reaction capabilities (QRC)\(^{6+1}\) 6+1 Component (AD not shown)

---

We must balance the value of best business practices that come with a managed service against cyber mission requirements.

Deliver as a library of tools
Deliver as a managed service
More analysis required

\(^{6+1}\) 6+1 Component (AD not shown)
One Global Workflow (Ticketing) System for the Army

ITSM as a managed service makes sense to keep up with technology changes, hardware lifecycles, and leverage best business practices from industry

18 RFI responses received and tracked last fall. Major outcomes:
- Establish and maintain a strong, aggressive project team
- The Army must define its CONOPS and requirements
- Start small and incrementally expand (phase)
- Use long-term contracts (7+ years)
- Establish a Single Award Indefinite Delivery / Indefinite Quantity (IDIQ)

“Out of the box” solution … with some constraints

Stakeholder will need training and business process reengineering assistance

IPT stood up by CIO/G-6 to pursue a disciplined approach to fielding ESMSaaS (and future NetOps tools/services)
- Hybrid of NDAA 2012 guidance with Business Capability Lifecycle (BCL)
Army Enterprise Service Desk (AESD) Current State

AESD → First Global Single-Point-of-Contact for IT Incidents
One Help Desk (People) with different Ticketing Tools and Processes

Enterprise Services Incident
- End User/IMO
- Tier 1
- Workflow Support System
- Tier 2 - 3

Enterprise Applications Incident

Functional Command Incident

CONUS Theater Incidents For 30-40 Installations

REPORTED BY
PHONE CALL VERIZON 866-335-ARMY
RIGHTNOWWEB SELF SERVICE TICKET
EMAIL

REPORTED BY
PHONE CALL VERIZON 866-335-ARMY
EMAIL

ENTERPRISE
ESM
Referral Ticket
Situational Awareness Notification

NETCOM ESMS
Incident Management -Call -Email

NETCOM ESMS Referral Ticket
Situational Awareness Notification

CONUS

Tier 2-3 Resolvers
EMAIL
Referral Ticket
Situation Awareness Notification
ACOIC/T-NOSC

Tier 1
- Triage agent
- Tier 1 Resolver agent

OR REFERRED TO TIER 2

DISA RightNowWeb
- Incident Management -Call -Web -Email

Service Request
Knowledge (Commercial RightAnswers, DISA Local Knowledge)
Problem Management

Tier 1
- HANDLED BY
ESD

Tier 1
- HANDLED BY
CSD

COMPUTER NETWORKS MODERNIZATION INITIATIVE | 6
The Army will continue to expand use of AESD to provide Tier 0 and Tier 1 support for all enterprise services while in parallel working replacement of current AESD contract:

- AESD Request for Information (RFI) issued to industry 20 MAY
  - Sources Sought announcement with FEDBIZOPS Solicitation Number: W52P1J-13-T-0414

- Seeking innovative input from Contractors
  - Experience operating Contact Centers supporting Government/multinational organizations
  - Core competencies in configuring and maintaining Call Center supporting technologies
  - Proven management and staffing approaches

Leverage ESMSaaS to provide one global workflow (ticketing) system for the entire Army
PROJECT MANAGER

I3C2

INSTALLATION INFORMATION INFRASTRUCTURE COMMUNICATIONS AND CAPABILITIES