AFCEA DISA CyberNetOps (CNO) Solutions

James Travis, PhD, CEH

Cyber SA/NetOps Directorate
14 June 17
CD4 Mission

Who We Are

CD4, a Cyber Directorate Division, provides Operational Support System Solutions for DISA’s command and control and information-sharing capabilities to DISA Operations & DISA’s Mission Partners

FOCUS

- Assuring DoDIN operations (transport, compute, apps)
- Optimize capabilities to enable software defined networking (SDN) and network function virtualization (NFV)

- CyberNetOps tools convergence
- Adopt open source and white box solutions
- CyberNetOps via mobile applications
ID4 CyberNetOps Leadership

Who We Are

CyberNetOps Division
James Travis, Division Chief
Alfrenetta Cooper, Deputy
Vacant, Chief Engineer

Robert Mauldin
Chief, NetOps PMO/Architecture Integration (ID41)

Scott King
Chief Engineer (Acting)
Chief, Network Element Systems (ID42)

Thomas Hines
Chief, Network/Service Management Systems (ID43)

Andrew Cape
Chief, Computing Management Systems (ID44)
CyberNetOps (OV-1)

What's the Operating Environment

Display Layer

Workflow Transactions

Alerts & Alarms

Workflow Data

ITSM

Request/Requirement & Demand

Change & Config

Design & Build

Capacity, Availability & Continuity

Event, Incident & Problem

Knowledge Centered Support

Service Level Management

Access, Security and CNDSP

Knowledge Management (KM), Business Intel (BI) & Analytics Queries

BI/KM/Analytics Engines

Knowledge Management (KM), Business Intel (BI) & Analytics Queries

BI/KM/Analytics Engines

Data Tagging Strategy

Data Warehousing

Translation Layer

The Data Layer

NIPR Data Warehouse

SIPR Data Warehouse

Cross Domain

Logs

EMS

PerfMS

CM

DODIN Security

CYBEROPS

DISA Workers

Mission Partners

Service Desk

Operations & DCO

DoD Senior Leaders

Command & Control

Service Managers & PMs

CyberNetOps (OV-1)
Baseline: Separate Tools & Architectures

DISA Telemetry & Control - Future

What’s the Telemetry Env
Baseline: Separate Tools & Architectures

End State: Standard Tools, OPS Views & Architecture

Cybersecurity Protect Functions

- DISN OSS
- Optical/IP/UC Legacy EMSSs Modeling
- Network Management
- Event Mgmt Perf. Mgmt Reporting Web Mon. Discovery Inventory
- Situational Awareness
- Portals Syslog Analytics Ticketing Dashboard

What's the Telemetry Env
CyberNetOps Enterprise Cloud Architecture

SECRET

PROD

MGMT

JMN-D (S) over JMN-D (U)

FW

Cross Domain

Privilege MGMT (AAM) Tools

JMS MGMT Tools

MNIS MGMT Tools

IAP MGMT Tools

Cmcl Cloud MGMT Tools

Cross Domain

SDN Orchestrator

SDN Controller

EOC/VNOC

M

G

M

T

P

R

O

D

SBU

PROD

MGMT

CNO JMN-D Edge

CNO JMN-D Core Router

JMN-D (U) OOB Transport
Optical, IP MPLS & SATCOM

CyberNetOps Enterprise Cloud

Army

Navy

USAF

USMC

VNOC

DISA

DISN OSS MGMT Tools

DIS N MGMT Tools

Coalition

Service

Agency

Joint

DISA

UNITED IN SERVICE TO OUR NATION
DISA Cyberspace Operations SV-1

What’s the CNO Architecture

This is where integration happens
Complexity makes pure fleet hard

UNCLASSIFIED
Future CNO Environment

What’s the target CNO Env

IP MPLS / Optical

10/100 Gbps Black Telemetry Core
W/multiple VRFs per separate management boundary
rate us
visit us
follow us
take the 3-question survey available on the AFCEA 365 app
DISA Booth # 443
Facebook/USDISA
Twitter/USDISA
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, authorization, and accounting (Advanced Defense Switched Network Integrated)</td>
</tr>
<tr>
<td>ATN</td>
<td>Mgmt Spt Sys Transport Network</td>
</tr>
<tr>
<td>BAS-G</td>
<td>Building Automation System-Global</td>
</tr>
<tr>
<td>BDP</td>
<td>Big Data Platform</td>
</tr>
<tr>
<td>CCV</td>
<td>Common Communications Vehicle</td>
</tr>
<tr>
<td>CEMS</td>
<td>Converged Element Management System</td>
</tr>
<tr>
<td>CNO</td>
<td>CyberNetOps</td>
</tr>
<tr>
<td>CSAAC</td>
<td>Cyber Situational Awareness Analytical Capabilities</td>
</tr>
<tr>
<td>DCN</td>
<td>Data Communications Network</td>
</tr>
<tr>
<td>DCO</td>
<td>Defensive Cyber Operations</td>
</tr>
<tr>
<td>DDOS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DECTK</td>
<td>DISN Enterprise Classified Travel Kit</td>
</tr>
<tr>
<td>DEPS</td>
<td>DOD Enterprise Portal Service</td>
</tr>
<tr>
<td>DMCC</td>
<td>Defense Mobility Classified Capability</td>
</tr>
<tr>
<td>DNG</td>
<td>DISN NetOps Center</td>
</tr>
<tr>
<td>DRSN</td>
<td>Defense Red Switch Network</td>
</tr>
<tr>
<td>DSN</td>
<td>Defense Switch Network</td>
</tr>
<tr>
<td>DWDM</td>
<td>Dense Wave Division Multiplex</td>
</tr>
<tr>
<td>ECVoIP</td>
<td>Enterprise Classified Voice over IP</td>
</tr>
<tr>
<td>EMS</td>
<td>Element Management System</td>
</tr>
<tr>
<td>EOC</td>
<td>Enterprise Operations Center</td>
</tr>
<tr>
<td>ESM</td>
<td>Enterprise Service Management</td>
</tr>
<tr>
<td>EVoIP</td>
<td>Enterprise Voice over IP</td>
</tr>
<tr>
<td>FOC</td>
<td>Final Operational Capability</td>
</tr>
<tr>
<td>FW</td>
<td>Firewall</td>
</tr>
<tr>
<td>GVS</td>
<td>Global Video Service</td>
</tr>
<tr>
<td>GVS-C</td>
<td>Global Video Service – Classified</td>
</tr>
<tr>
<td>IAP</td>
<td>Internet Access Point</td>
</tr>
<tr>
<td>IAPNet</td>
<td>Internet Access Point Network</td>
</tr>
<tr>
<td>IdAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>ISS</td>
<td>Information Sharing System</td>
</tr>
<tr>
<td>ISZ</td>
<td>Information Sharing Zone</td>
</tr>
<tr>
<td>ITSME</td>
<td>Information Technology Service Management Enterprise</td>
</tr>
<tr>
<td>JMN-D</td>
<td>Joint Management Network-DoDIN</td>
</tr>
<tr>
<td>JMS</td>
<td>Joint Management System</td>
</tr>
<tr>
<td>KM</td>
<td>Knowledge Management</td>
</tr>
<tr>
<td>LOB</td>
<td>Line of Business</td>
</tr>
<tr>
<td>LS-TDM</td>
<td>Low Speed – Time Division Multiplexer</td>
</tr>
<tr>
<td>ME</td>
<td>Managed Element</td>
</tr>
<tr>
<td>MNIS</td>
<td>Multinational Information Sharing</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi-protocol Label Switching</td>
</tr>
<tr>
<td>NCCM-R</td>
<td>Network Configuration and Change Management- Replacement</td>
</tr>
<tr>
<td>NMS</td>
<td>Network Management System</td>
</tr>
<tr>
<td>OOB</td>
<td>Out of Band</td>
</tr>
<tr>
<td>OSS</td>
<td>Operational Support System</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OTS</td>
<td>Optical Transport System</td>
</tr>
<tr>
<td>PCAP</td>
<td>Packet Capture</td>
</tr>
<tr>
<td>PDR</td>
<td>Preliminary Design Review</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PROD</td>
<td>Production</td>
</tr>
<tr>
<td>PSC</td>
<td>Production Support Review</td>
</tr>
<tr>
<td>SA</td>
<td>Situation Awareness</td>
</tr>
<tr>
<td>SDN</td>
<td>Software Defined Networking</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security information and event management</td>
</tr>
<tr>
<td>UC</td>
<td>Unified Capabilities</td>
</tr>
<tr>
<td>VNOC</td>
<td>Virtual Network Operations Center</td>
</tr>
<tr>
<td>VRF</td>
<td>Virtual routing and forwarding</td>
</tr>
<tr>
<td>WWOLS</td>
<td>Worldwide Online System</td>
</tr>
</tbody>
</table>