

## 2016 Defense Health Information Technology Symposium

# Med-COI, LAN and WLAN Deployment, Sustainment and Lessons Learned



*“Medically Ready Force...Ready Medical Force”*

**“A joint, integrated, premier system of health, supporting those who serve in the defense of our country.”**



***“Medically Ready Force...Ready Medical Force”***

# Learning Objectives

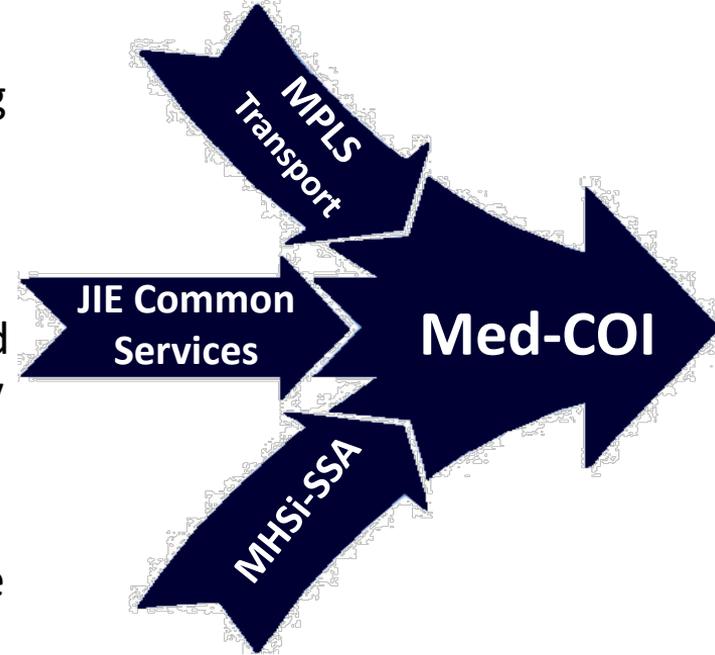
- Describe the scope of work associated with Med-COI
- Identify the activities downtimes associated with a Med-COI cutover to include implementation time lines
- Explain how the DHA Network Operations Center (DNOC) is structured and the services it provides
- Explain efficiencies gained through centralized LAN/WLAN monitoring and management
- Explain how the DNOC will coordinate efforts with the sites to achieve success

# Agenda

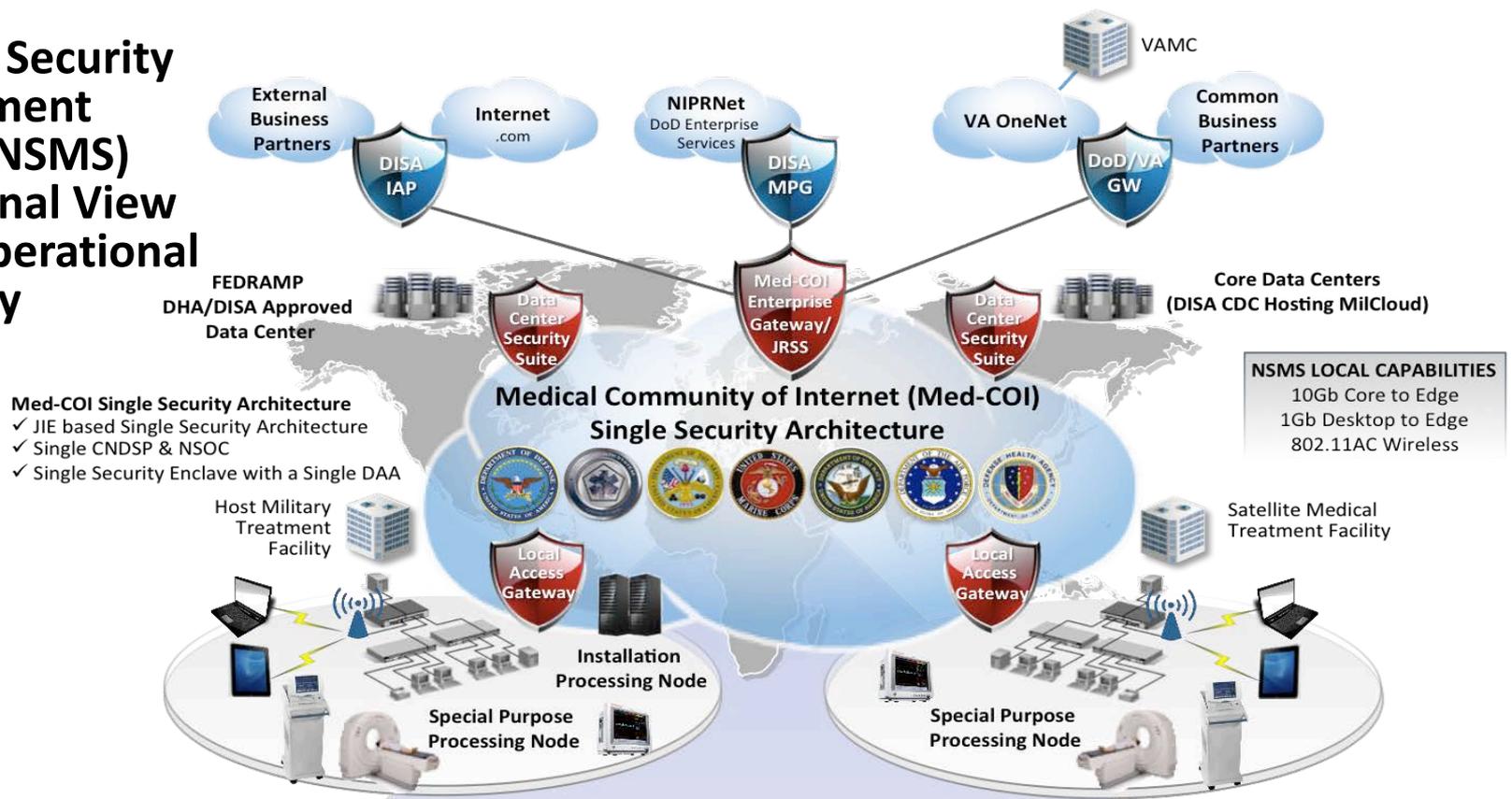
- Medical Community of Interest (Med-COI) site implementation and “Zone” transition plan
- Military Health System (MHS) Core Clinical Application Migration (Med-COI AM)
- Local Area Network (LAN) and Wireless Area Network (WLAN) monitoring and management
- DHA Network Operations Center (DNOC) overview

# Med-COI Background & Scope

- Med-COI leverages MHS Intranet (MHSi) security architecture coupled with Defense Information Systems Network (DISN) Multiprotocol Label Switching (MPLS) transport to implement a Single Security Architecture (SSA) consistent with DoD Joint Information Environment (JIE) net-centric principles
- As a Mission Partner Environment, must be segregated from the NIPRNet to support seamless interoperability with Medical mission/business partners
- Supports alignment with JIE Common Operating Environment, DHA IT consolidation objectives, and the deployment of the new electronic health record, MHS GENESIS



# Network Security Management Service (NSMS) Operational View at Full Operational Capability



## Enterprise Network and Security Management Service (NSMS) includes and supports:

- Standardized Operational & Support Processes
- Boundary Network Defense Capabilities
- 24x7x365 LAN/WLAN Management, Monitoring and Support
- 24x7x365 Security Management & Incident Response
- Confidentiality Service (VPN over MPLS-WAN)
- LAN/WAN Capacity Planning and Management
- Enterprise Remote Access (Admin and User)
- Local Access Gateways (IPNs and SPPNs)
- Consolidated Lifecycle Management Strategy
- Application-Layer Quality Of Service (QoS)
- Directory and PK-Enabled Authentication, Authorization and Access-Controls
- Medical Device Connectivity and Protections
- Desktop and Application Virtualization
- RTLS/RFID Enterprise Administration

# Med-COI Site Implementation (Army & Navy MTFs)



2016 Defense Health Information Technology Symposium

- Conduct surveys, develop circuit with Multipurpose Label Switching (MPLS) upgrade and last-mile implementation requirements
- Complete circuit and last mile installation
  - Parent/Host sites include primary and diverse secondary path
- Complete installation of Med-COI Single Security Architecture (SSA) replacing legacy Network Protection Suite (NPS) with enclave transition architecture
  - Implement the standard JIE Security Zone architecture supporting:
    - Standardized delivery of enterprise infrastructure services
    - Migration of Military Health System (MHS) Programs of Record (POR)
    - Transition of MTF enclaves and systems from NIPRNet/MHSi to Med-COI
- Initiate enclave transition beginning with current MHS Enclave and MHS Legacy Core Applications on MTF/Service networks
- Begin use of Med-COI MPLS VPN between regional sites, data centers, and enterprise gateways

# Med-COI Site Implementation (Army & Navy MTFs) – continued

- Proceed with MTF enclave transition by "Zone"/Network/Virtual LAN (VLAN)
  - For most Army/Navy sites, systems/networks will retain current addressing schema provided current VLAN structure does not violate security "best practices"
- Complete implementation of security controls and installation of Information Assurance (IA)/Computer Defense Service Provider (CDSP) compliance, monitoring, and forensics tools
  - Implementation by Zone following IA risk acceptance process
- Complete cutover to Med-COI network and protections following issuance of "final" Authority to Connect (ATC) or interim ATC (iATC)
  - Remove remaining Service or MTF managed security infrastructure\*

*\* Requires remaining Service/Site managed Business-to-Business connections to be migrated to Med-COI, and closure of any external connections to NIPRNet, Internet, or Base/Post/Camp if not mediated through the Med-COI Enterprise Gateways*

# Med-COI SSA: “Zone”/Demilitarized Zone (DMZ) and Virtual LAN (VLAN) Assignment Template



2016 Defense Health Information Technology Symposium

Zone	Name/Short Descriptor	Description/Zone-VLAN-DMZ Characteristics
1	NetOps DMZ	DMZ containing management interfaces for CND, ISN and NSN infrastructure
2	SecOps/CND DMZ	DMZ Security Server/Services for DHA/MHS/Local Service Systems Hosting Environment
3	Installation Services Node (ISN)	Installation Services Node, supporting Local IPN/SPPNs (Domain Controllers (DCs), Triple A, DHCP, other protected enterprise network services)
4	MHS Enclave - Regional IPN/MAAG Site	Web/App/DataBase VLANs related Regional IPN/MAAG Sites (current MHS enclave virtualized hosting environment)
4a	MHS Enclave - IPN (Local MTF)	Web/App/DataBase VLANs related Other MHS systems/PORs (stand-alone servers)
4b	MHS Enclave - OOB/Mgmt VLAN	Out-of-Band (OOB)/Management VLAN for MHS systems, Private Addressed - restricted access
4c	Legacy MHS Clinical Systems - CHCS	Legacy CHCS Core Infrastructure, MAAG sites to host multiple MTF application servers
4d	Legacy MHS Clinical Systems - AHLTA	AHLTA Network (former MHS-DMZ), including CHAS (former ICDB), MAAG Sites to Host multiple MTF application servers
4e	Essentris Servers	VLAN containing Essentris Servers (Layer 3 host network)
4f	Essentris Med-Device VLAN	Essentris Med Device VLAN (Layer 2 network sharing Essentris Server address space)
4w	Web DMZ (Local and Extended)	Local Web DMZ (extended from G/W), also contain local NetScaler (at MAAG site)

***“Medically Ready Force...Ready Medical Force”***

# Med-COI SSA: “Zone”/DMZ and VLAN Assignment Template (continued)



Zone	Name/Short Descriptor	Description/Zone-VLAN-DMZ Characteristics
5a	Service Other IT-Business Systems	Web/App/DataBase VLANs related to Service Other IT/Business Systems
5b	Service Other IT-Clinical Systems	Web/App/DataBase VLANs related to Service Other IT/Clinical Systems
5c	Service Other - OOB/Mgmt VLAN	Out-of-Band (OOB)/Management VLAN for Service other systems, private addressed - restricted
6	Departmental/Med Device VLAN	Medical Device/Departmental, Modality-based VLANs, Layer 2 Segregation Architecture
7	End User Zone	End User Zone (Workstations and related Devices), included GSUs
8	Guest Wireless, Guest Wired/Kiosks	Guest Wireless (SSID/VLAN), Guest Wired (e.g. Kiosks), Private addressed - no Local Access
9	Purgatory/Quaranteed Systems	VLAN containing non-accredited, or very high-risk systems, restricted access
10	Network Services Node (NSN)	Local Network Services 'DMZ', Core connected subnet, spanned/screened, (WLAN Controllers, ACAS, CIFS, SCCM DP's, etc.)
11	Wired/Wireless Network Electronics	LAN/WLAN network electronics (private addressed)
12	Voice/Unified Communications	IP Voice or Video Network Gateway
*	Other/TBD	TBD based on unique site requirements/application or infrastructure services

# Med-COI Site Implementation

## Air Force MTFs (per MOA/AF I-Plan)

- Procedure similar to Army/Navy MTF Sites
- New DHA Med-COI enclave is stood-up in parallel to existing AF network following the sequence defined in I-Plan
  - Subsumes/replaces existing MHS enclave/infrastructure
  - Bypasses existing VPN path through AF Block 30 Gateways
  - Provides network and security services replacing AF line infrastructure services
- Execute "Zone" transition following new MTF network address plan
  - All assets on AF MTF and clinic LANs will receive DHA addresses
  - All systems will be migrated to the MHS Joint Active Directory (mJAD)
- Non-Essentris sites (outpatient facilities), MHS Programs of Record (PORs) will migrate to regional MHS Application Access Gateway (MAAG) site
  - Affects AHLTA, CHCS, CHAS (formerly ICDB)
- At inpatient sites, MHS PORs will migrate to the local Site Med-COI enclave
  - Migration occurs after all other systems, services and end users are moved to minimize performance impacts during migration

# MHS Core Clinical Application Migration (AM) Plan



2016 Defense Health Information Technology Symposium

## No Re-IP – 48 sites

Data network addresses will not be changed

- Fully Qualified Domain Names (FQDNs) will change at all sites, only change at four Army/Navy sites
- Management network addresses will change at 44 Army/Navy sites

## Re-IP – 18 sites

All network addresses will change

- Essentris only at three Army/Navy sites, all EHR Core applications at 15 Air Force sites
- Data network addresses will change including all “No Re-IP” tasks

## Preposition – 31 sites

Hardware will be preconfigured at a MAAG site before migration

- Only data will be physically transported to the MAAG site
- Includes all “Re-IP” tasks (after transport)

## Forklift – 10 sites

Hardware will be moved to a MAAG site during migration

- All application hardware will be physically transported to the MAAG site
- Includes all “Re-IP” tasks (after transport)

# Med-COI and Med-COI AM Integrated Planning & Site Coordination

*Sites are requested to participate in a series of meetings to ensure all activities are reviewed and executed within schedule parameters and to address risks and issues.*

## Site Implementation Plan (SIP) & Pre-Implementation Meeting (PIM) Meetings

-120d

- Provide a brief overview of the Med-COI project
- Coordinate additional meetings to gather site data

## Continued Coordination

-90d, -60d, -30d

- -90d: Review status of network and PPS info
- -60d: Present updated SIP and PIM
- -30d: Finalize SIP and PIM
- Review Last Mile issues

## Go-No-Go Meeting

-8d

- Issue MICCB information
- Confirm completion of all Site-Level Implementation activities prior to scheduled downtime

## Post-Implementation Meetings (PoIM)

0d, +7d, +30d

- Turnover Call
- +7d: Provide trap list, discuss COAs
- +30d: Add SNAP/ accreditation diagram

# Med-COI Schedule



2016 Defense Health Information Technology Symposium

	SIP kick-off (120)	SIP (90 day)	SIP (60 day)	Final SIP (30 day)	SIP Go/No-Go Call	Med-COI SSA	AHLTA/CHCS /CHAS	Essentris
Nellis	3/7/16	6/7/16	7/7/16	8/7/16	8/27/16	9/6/16	10/22/16	10/25/16
Bethesda, MD	5/18/16	6/14/16	7/12/16	8/11/16	8/31/16	9/10/16	9/17/16	9/20/16
Ft Belvoir	5/20/16	6/15/16	7/13/16	8/12/16	9/1/16	9/11/16		9/20/16
USAF Academy, CO	6/1/16	6/22/16	7/22/16	8/21/16	9/10/16	9/20/16	n/a	9/27/16
Los Angeles AFB	5/25/16	6/23/16	7/23/16	8/22/16	9/11/16	9/21/16	11/19/16	N/A
Eielson	6/1/16	6/29/16	7/30/16	8/29/16	9/18/16	9/28/16		N/A
Ft Wainwright	6/8/16	7/6/16	8/5/16	9/4/16	9/24/16	10/4/16	10/8/16	10/11/16
Cerner COOP	6/7/16	7/7/16	8/6/16	9/5/16	9/25/16	10/5/16		N/A
Ft Riley		4/27/16	5/27/16	6/27/16	7/16/16	7/26/16	12/10/16	12/13/16
Corpus Christi	6/20/16	7/15/16	8/14/16	9/13/16	10/3/16	10/13/16		N/A
Vandenberg	6/20/16	7/20/16	8/19/16	9/18/16	10/8/16	10/18/16	12/17/16	N/A
Tripler	6/25/16	7/25/16	8/24/16	9/23/16	10/13/16	10/23/16	1/7/17	1/10/17
Mountain Home	6/28/16	7/27/16	8/26/16	9/25/16	10/15/16	10/25/16	1/14/17	1/17/17
Pensacola, FL	7/4/16	8/3/16	9/2/16	10/2/16	10/22/16	11/1/16	11/5/16	11/8/16

***“Medically Ready Force...Ready Medical Force”***

# Med-COI Implementation

## Lessons Learned



2016 Defense Health Information Technology Symposium

- Ensure that new *health.mil* certificates are installed and contain (where appropriate) both old and new DNS names, and that these are resolving to the correct IP addresses
- Ensure site Government POC is on the pre-migration coordination call to concur with start of the downtime and affirm migration was successful
- Communicate with users about need to be off of systems prior to scheduled downtime, then remind them again just before start of the downtime
- Ensure availability of “subject matter testers” for functionality testing and confirm devices/printers in pharmacy, laboratory, radiology, etc., are functioning properly
  - Identify testers for remote sites and clinics as-required
- Ensure all system interfaces and functions are operational prior to start of the downtime – this will save time when testing and troubleshooting later
- For Essentris, verify Legacy Results Viewer and Early Warning Dashboard are working properly prior to migration

***“Medically Ready Force...Ready Medical Force”***

# LAN / WLAN Transition and Sustainment Update

# Network Monitoring

*If a site has HP NNMi (Network Node Manager), you can implement immediately*

## Rename Network Devices

## Configure NNMi

## Create Network Map

## Decommission Legacy Tools

- Re-name Network Devices IAW DHA naming convention
- Naming convention created with MTF input
- Exceptions, although rare, can be requested

- NNMi is the enterprise tool of choice for network monitoring
- Working group convened to evaluate existing tools and select one tool

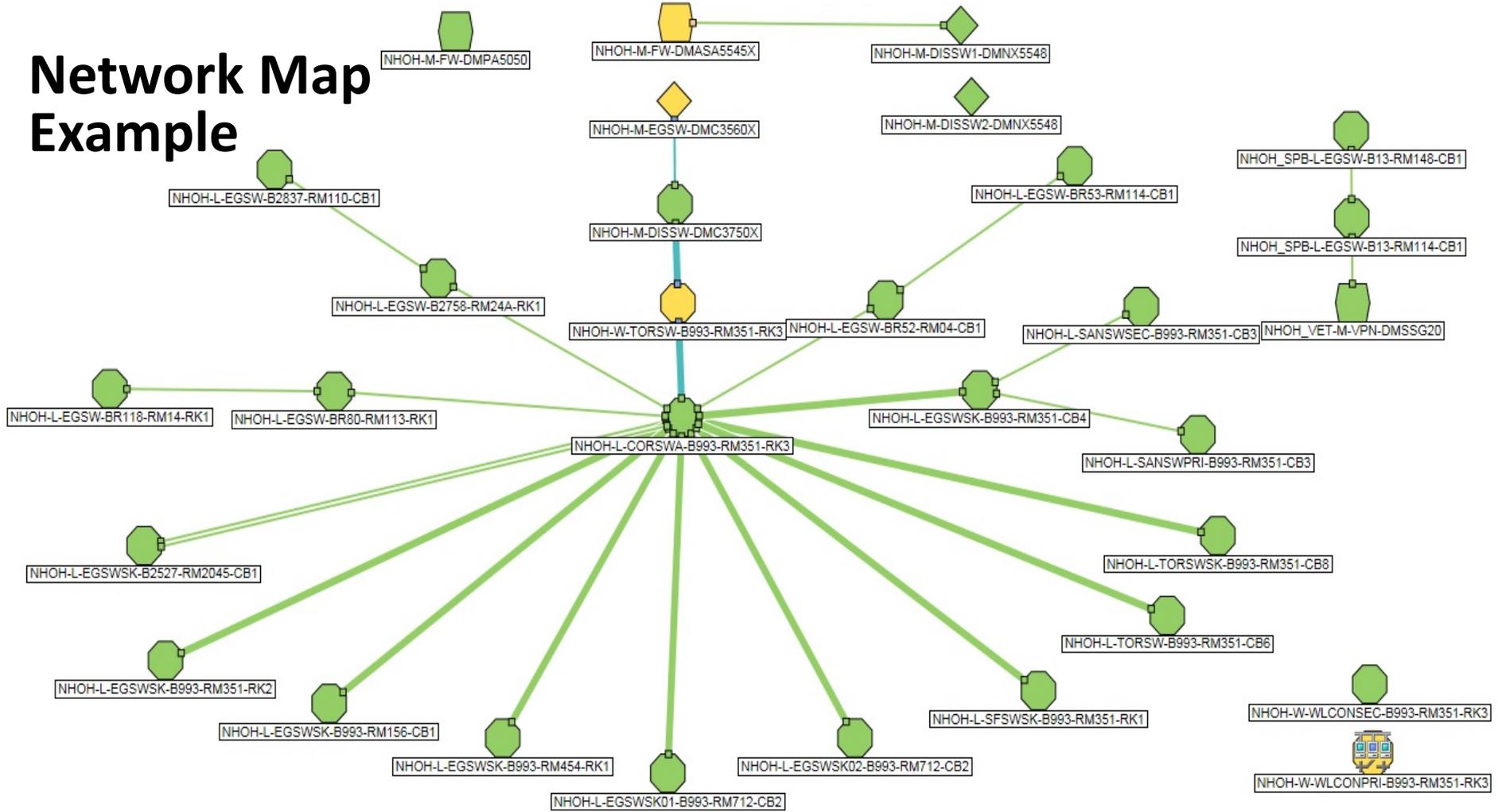
- Populate network map to include dependencies between devices
- Create critical and non-critical device list

- Legacy network monitoring tools should be decommissioned in favor of NNMi
- NNMi servers have been ordered to support those sites with no server

*x7 MTF completed a/o May 2016 & Leverage NP NNMi “How-TOs”*

*“Medically Ready Force...Ready Medical Force”*

# Network Map Example



# Interface Availability Report



2016 Defense Health Information Technology Symposium

## Weekly Device Interface Availability Report (BREM)

		5/11/16	5/12/16	5/13/16	5/14/16	5/15/16	5/16/16	5/17/16	Weekly Summary
		Availability (avg)							
BREM_BANG-M-VPN-DMSSG520	serial1/0	100.00%	100.00%	100.00%	42.71%	0.00%	35.42%	100.00%	68.30%
	<b>BREM_BANG-M-VPN-DMSSG520</b>	<b>100.00%</b>	<b>100.00%</b>	<b>100.00%</b>	<b>42.71%</b>	<b>0.00%</b>	<b>35.42%</b>	<b>100.00%</b>	<b>68.30%</b>
BREM_EVRT-M-VPN-DMSSG20	serial1/0	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
<b>Daily Summary</b>		<b>99.93%</b>	<b>99.85%</b>	<b>100.00%</b>	<b>98.15%</b>	<b>96.77%</b>	<b>97.91%</b>	<b>100.00%</b>	<b>98.94%</b>

**Reports on CPU, Memory, and Interface Utilization also available**

*“Medically Ready Force...Ready Medical Force”*

# Network Management

- Day-to-day support will reside with Network Engineering Specialist (NE&S) and MTF staff
  - Oversight provided by DHA
- Creating standard operating procedures / frequently asked questions outlining processes and procedures
  - Goal is to reduce variance across the enterprise; we need your feedback!
- Enterprise network management solution currently being evaluated by Engineering, Design, and Deployment Branch (EDD)
- DHA Global Service Center (DHAGSC) incidents must be submitted for all work orders
- Tier III and vendor escalation will be handled by Core Infrastructure Services (CIS)
  - Open ticket w/ DHAGSC and assign to CIS
- Local NE&S maintains network diagrams

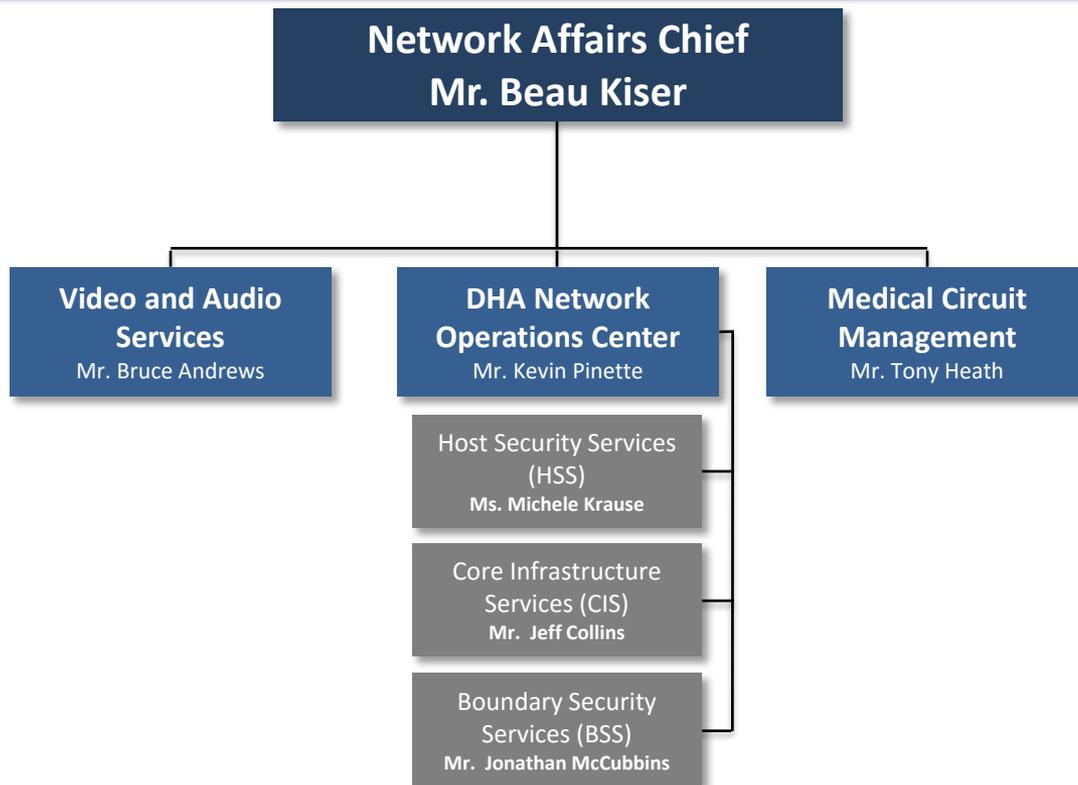
# Key Site Responsibilities

- Keep HP Network Node Manager (NNMi) updated
- Security Technical Implementation Guidelines (STIGs) and Information Assurance Vulnerability Alert (IAVA) compliance
- Adds, moves, changes
- Note: Network Engineers & Specialists (NE&S) assigned to DNOC/CIS Function will perform (quality control) tickets to ensure conformance with present and future DHA guidelines

# WLAN Management

- Service Set Identifier (SSID) changes or enterprise changes required on the master controller are a DHA responsibility
- Deviations from the standard enterprise architecture will be accomplished by the DNOC/CIS
  - Approved SSIDs are outlined in the DHA Wireless LAN (WLAN) accreditation documentation
- CIS will maintain WLAN configurations via Wireless Network Management System (NMS)
- CIS will manage public key infrastructure (PKI) certificates on LAN and WLAN infrastructure devices

# Network Affairs Org Chart



# Boundary Security Services (BSS)

- Devices above the core switch are managed by BSS
  - Read only access authorized for site network personnel
- Domain Name System (DNS) / Internet Protocol (IP) addresses managed by the DNOC and assigned to the MTF
  - Includes both public and private IP address
  - Private IP scopes MUST be assigned by the DNOC in order to adjudicate any conflicts within DHA
  - Domain name registration for health.mil are also managed by the DNOC

# Host Security Services (HSS)

- Service and local Programs of Record (PORs) will be incorporated into DHA Host Based Security System (HBSS) instance
- Local IT staff will have ability to disable Host Intrusion Prevention System (HIPS) temporarily if HIPS is suspected of interfering with application functionality
  - MTFs will coordinate with HSS team for signature tuning
  - If signature cannot be tuned, a waiver must be submitted
- Disabling HIPs is temporary for troubleshooting purposes
  - Waiver requests will be processed through Cyber Security Division

# Summary and Key Takeaways

- Familiarity with the Med-COI site implementation and “Zone” transition plan
- Understanding of MHS Core Clinical Application Migration (Med-COI AM) procedures and timeline
- Understanding of the DHA LAN and WLAN monitoring and management strategy
- Familiarity with the DNOC and the services it provides to DHA customers

# Questions?



Defense Health Agency

2016 Defense Health Information Technology Symposium

***“Medically Ready Force...Ready Medical Force”***

# Evaluations

---

Please complete your evaluations

# Contact Information



2016 Defense Health Information Technology Symposium

Kevin Pinette

Chief, DHA Network Operations Center (DNOC)

kevin.j.pinette.civ@mail.mil