

Mr. William Spencer
Mr. Albert Dickson



2015 Defense Health Information Technology Symposium

A Single Network to Support Healthcare
(WAN, LAN, Wireless and Directory Services)



“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



- Identify the services and products included in the planned single Defense Health Agency (DHA) network
- Describe the planned implementation approach for the network
- Describe the DHA approach to maintain and support the single network
- Explain the projected impacts and benefits of a single network supporting the Military Health System (MHS)

Agenda



- Stakeholder benefits
- Network and Security Management Service (NSMS)
- Medical Community of Interest (Med-COI)
- Network and security architectures 'As-Is' and 'To-Be' states
- Service transition to Med-COI
- Pacific Northwest (PNW) site network architecture 'As-Is' and 'To-Be' states
- Local area network (LAN)/wireless area network (WAN) system 'As-Is' and 'To-Be' states
- Summary

Stakeholder Benefits



| | Current State | Business Impact | Future State |
|------------------------------|--|---|---|
| Providers & Staff | <ul style="list-style-type: none"> ▪ Overlapping networks within MHS which do not support clinical workflow ▪ Fractionalize patient care | <ul style="list-style-type: none"> ▪ Reduces ability to move seamlessly with devices throughout the clinical workflow ▪ Restricts ability to access/share data across multi-service markets | Integrated network that allows access to systems and ability to move seamlessly within and between MTFs |
| Beneficiaries | Network access issues impact the timeliness and quality of healthcare delivered | Wasted time spent working around network challenges, causing delays in timely healthcare provisioning | Integrated network that allows patient information and medical records to be exchanged between MTFs |
| Technology | Duplicative and uniquely managed networks that constrain access to systems and information | <ul style="list-style-type: none"> ▪ Inconsistent performance, situational awareness and capabilities ▪ Difficult to effectively plan, efficiently deploy, and centrally manage enterprise IT solutions | Integrated, secure, and standardized network that is highly available, centrally managed and monitored |

Network and Security Management Service (NSMS)

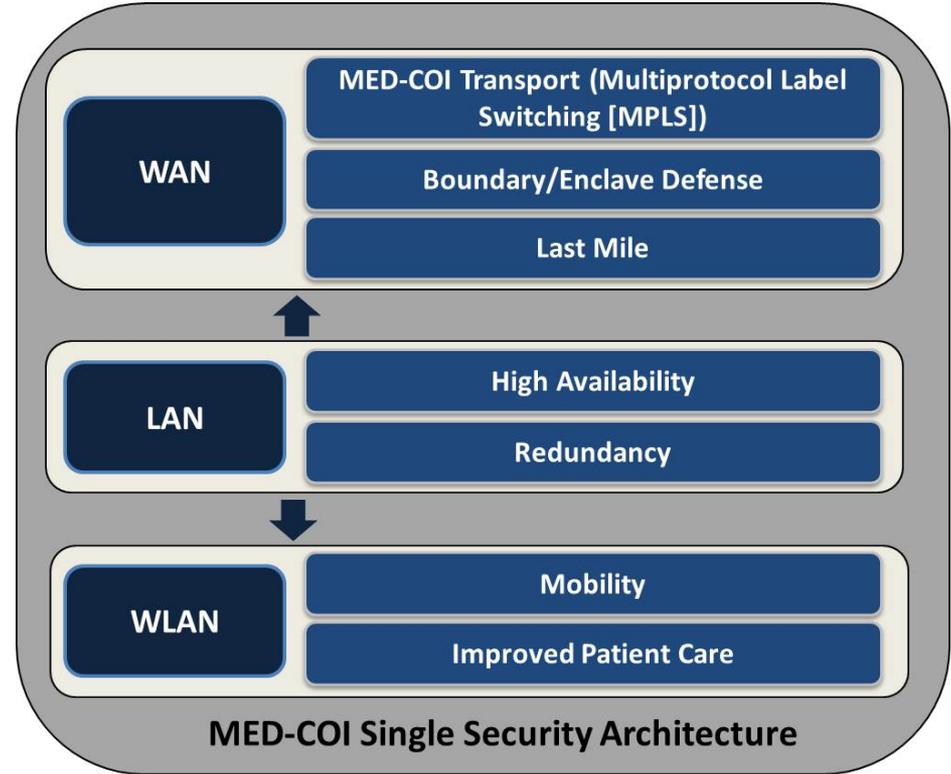


NSMS Capabilities:

Seamlessly integrated WAN, LAN, and Wireless Local Area Networks (WLAN) providing ease of access and integrated security for providers, beneficiaries, and business partners

NSMS capabilities include:

- Centralized and standardized management of the WAN, LAN, and WLAN
- WAN, LAN, WLAN behind a Single Security Architecture (SSA) under a single Designated Accreditation Authority (DAA)



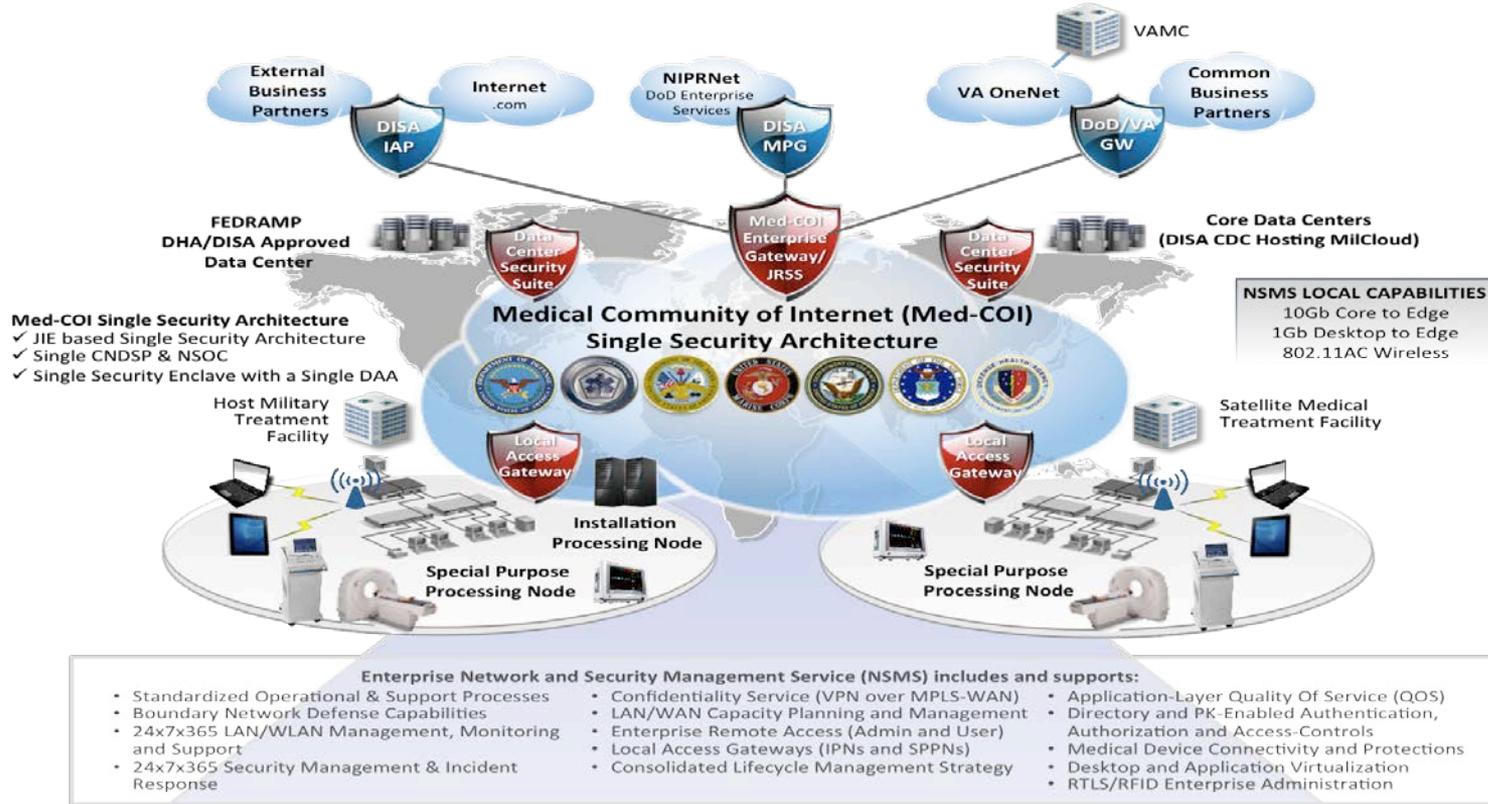
“Medically Ready Force...Ready Medical Force”

NSMS Scope



| | |
|--------------------------|---|
| Med-COI Transport | Leverages Defense Information Systems Network (DISN) Transport (MPLS, Joint Regional Security Stacks [JRSS], etc.) and Last Mile Solutions. Mission-based routing via Med-COI SSA in support of the DHA Mission. Single, consolidated, highly available and redundant network supporting the requirements of military healthcare. Scalable and agile to increase capability as requirements change. |
| Med-COI SSA | SSA is an Enclave Architecture aligned with the Joint Information Environment (JIE) Cybersecurity architecture, focused on medical system and access requirements. Single enterprise DAA/AO and aligned DHA Computer Network Defense Service Provider (CNDSP)/Network Security Operations Center (NSOC) functions to insure a consistent application of policy across the enterprise. Aligned with and leveraging Department of Defense (DoD) Enterprise Gateways (G/Ws). |
| LAN | High speed, highly available and redundant LAN infrastructure. Redundant core architecture providing 10gbps service at the network backbone and 1gbps service at the user desktop. Centrally managed to provide consistent service and access. |
| WLAN | High speed WLAN based on 802.11ac technology. Improved security and mobility to optimize provider capabilities at point of patient care. |

NSMS Operational View at FOC



“Medically Ready Force...Ready Medical Force”

Med-COI Background, Scope, & Benefits



- MHS Intranet (MHSi) was designed to conform with DoD Net-Centric principles through implementation of a SSA
- Med-COI is a Tier 1 Mission Partner Environment (MPE), that leverages MHSi investments and security architecture coupled with DISN MPLS transport to support consolidated Medical Community mission requirements and integrated service delivery
- The Med-COI MPE is engineered to support seamless interoperability with DHA business and mission partners, supports deployment of Defense Healthcare Management Systems Modernization (DHMSM), and is aligned with the JIE, and JRSS

“Medically Ready Force...Ready Medical Force”

Med-COI Enclave Node/Site Type Definitions; JIE Reference Architecture



- Core Data Centers (CDCs) – contain Enterprise Applications/Compute Capability/Data Services that can effectively and economically be delivered from a limited number of designated and approved CDC locations
 - All DISA DECCs are approved CDCs. Within Med-COI, CDCs are part of the MPE environment and share the same SSA. Med-COI CDCs may include any enterprise hosting environment that can meet Federal/DoD/DHA security requirements, including commercial hosting environments
- Installation Processing Nodes (IPNs) – Local data centers associated with the operation of stand-alone medical centers or hospitals, or such facilities which constitute an independent Base/Post/Camp (B/P/C), as well as hospitals whose networks are separated from the associated B/P/C
 - This definition would include most MTFs. Regional IPNs (like MHS Application Access Gateway [MAAG] sites) may support smaller IPNs and regional Special Purpose Processing Nodes (SPPNs)

“Medically Ready Force...Ready Medical Force”

Med-COI Enclave Node/Site Type Definitions; JIE Reference Architecture (cont'd)



- SPPNs – Applies to smaller compute capabilities in hospitals and clinics that support operation of Direct Care systems and Electronic Health Record (EHR) components on which these systems rely
 - ❑ In almost all cases, a Medical SPPN will be associated with a location with an IPN, but an SPPN can be stand-alone
 - ❑ Where these facilities are not collocated with an IPN, connections with other enclaves will be routed through an associated IPN and local access G/W.
 - ❑ Medical Device Enclave/Demilitarized Zone (DMZ) is a focused implementation of SPPN with specific interface requirements/limitations and special controls
- Installation/Network Services Nodes (ISN/NSNs) – Contain appliances such as domain/network/application delivery controllers, passive and or active scanners, monitoring equipment, or other devices intended to support secure, reliable, operations of the network
 - ❑ ISN/NSNs are typically collocated at an IPN or SPPN node site, and in some cases, at larger Geographically Separated Units (GSUs)

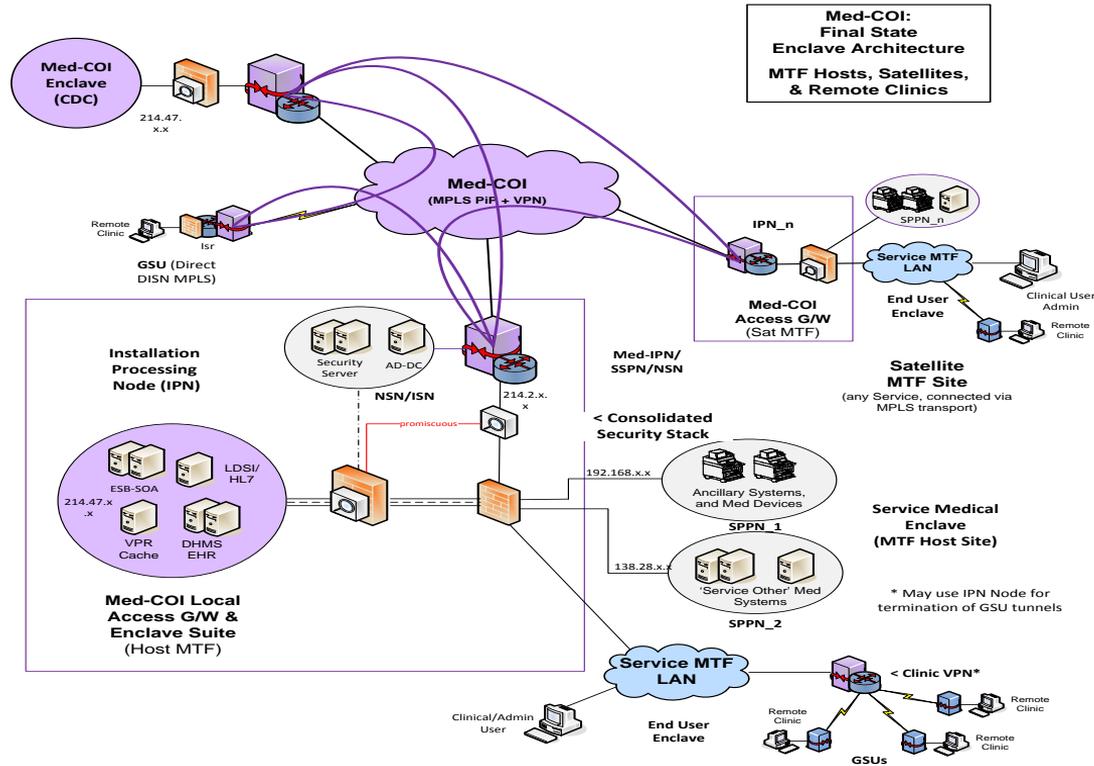
“Medically Ready Force...Ready Medical Force”

Med-COI Enclave Node/Site Type Definitions; JIE Reference Architecture (cont'd - 2)



- End User Zones & GSUs – End user zones are enclaves containing end user devices (EUDs) and peripherals that are dependent on higher tier compute and network services hosted at CDCs, IPNs, SPPN, and ISN/NSNs
 - GSUs are End User Zones that are isolated from their parent IPN or SPPN site, generally with a small user population – the term ‘Remote Clinic’ is synonymous with this node type

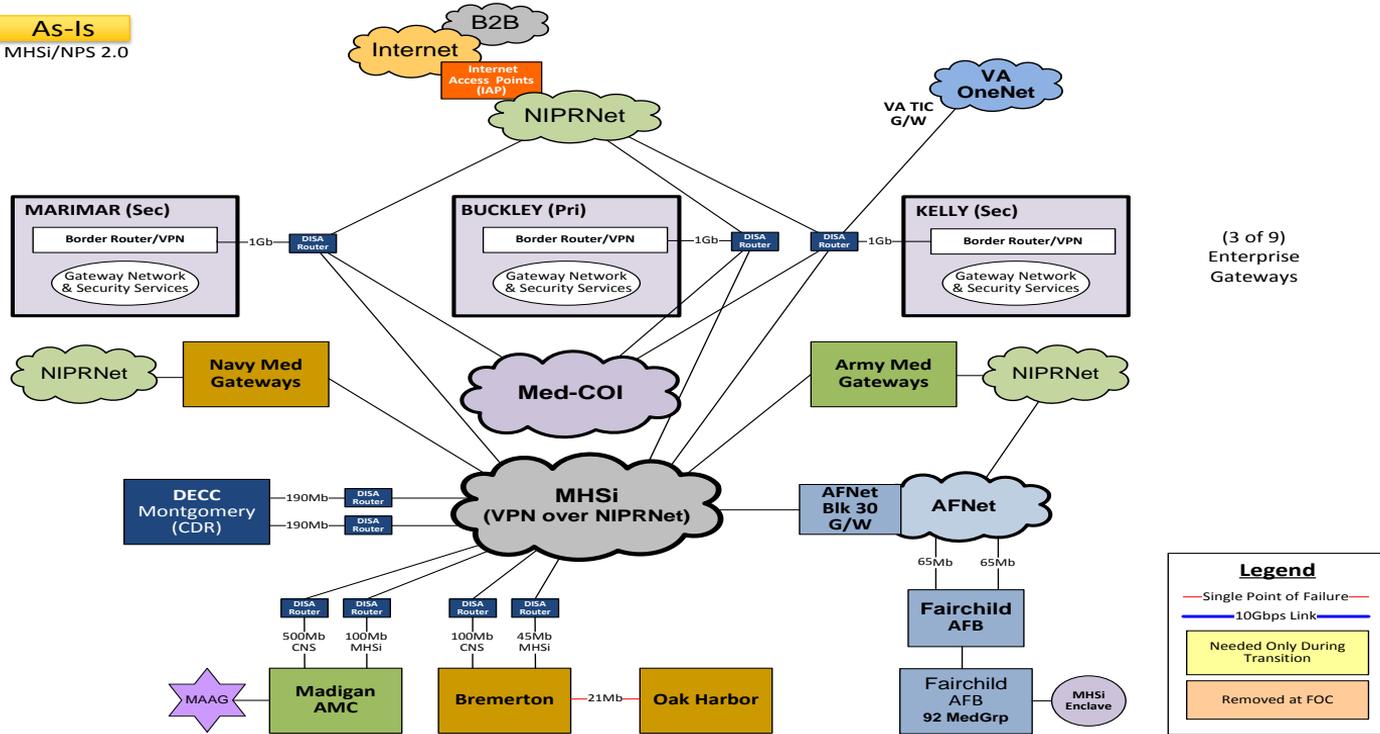
Med-COI Cyber Security Architecture IPN/SPPN Design Template (FOC)



“Medically Ready Force...Ready Medical Force”

MHSi & Service Medical Gateways - G/Ws 'As-Is' Architecture View

As-Is
MHSi/NPS 2.0

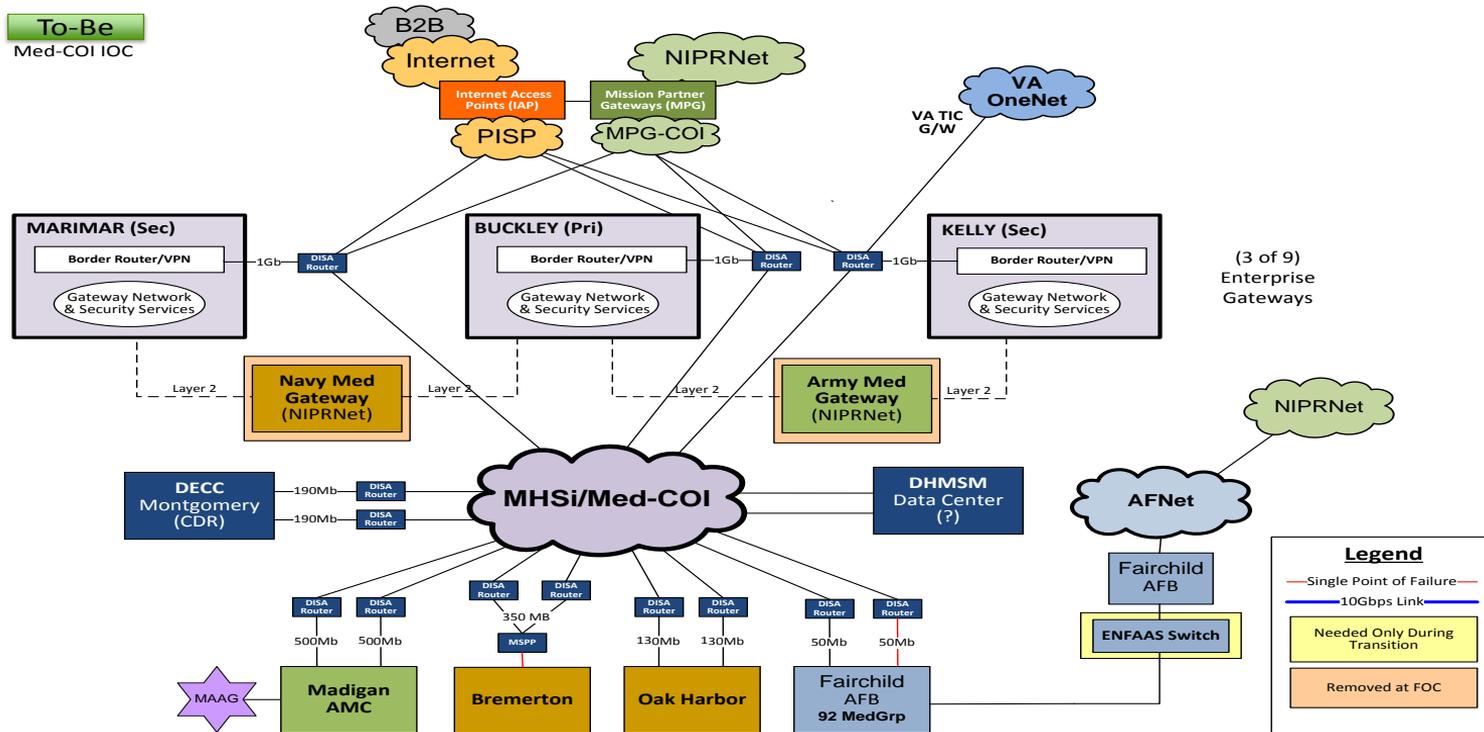


(3 of 9)
Enterprise Gateways

"Medically Ready Force...Ready Medical Force"

Med-COI Enterprise G/W – 'To-Be' Transition State Architecture

To-Be
Med-COI IOC



“Medically Ready Force...Ready Medical Force”

System View, Network and Security Architecture

PNW Sites, 'As-Is' State

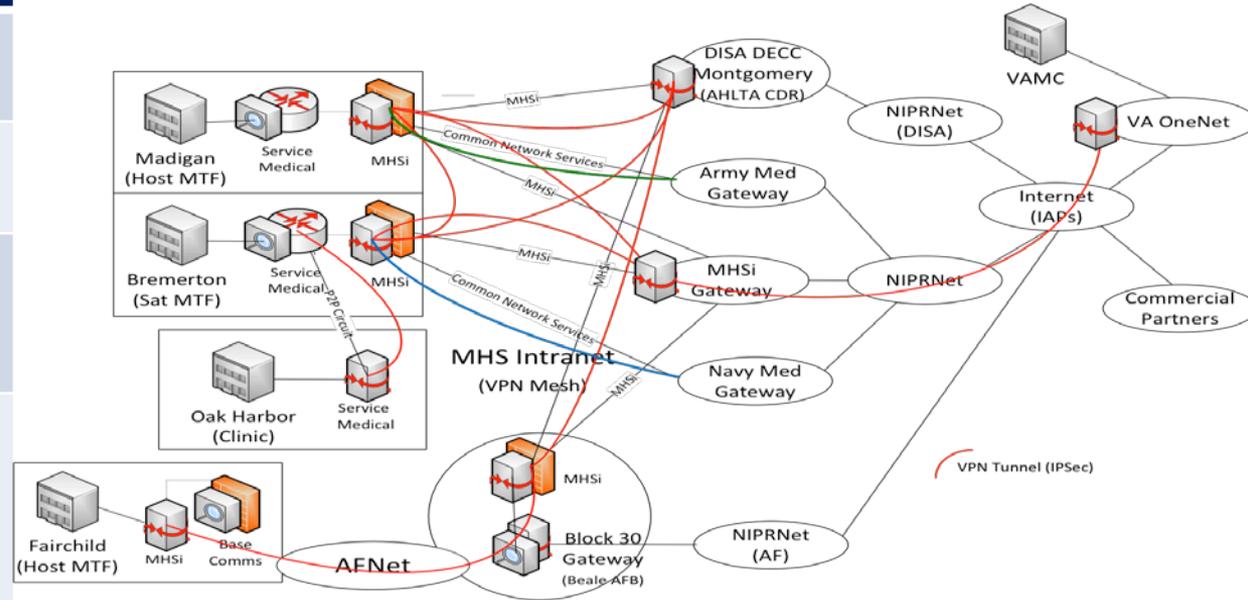
'As-Is' Highlights

Traffic flows segmented between MHS and Service Medical/Line

Separate Networks, Security Suites, policies and Management

IPSec over Non-classified Internet Protocol Router Network (NIPRNet) as WAN Transport (MHSi)

Boundary protection implemented at all enclave/site boundaries, multiple points of entry to the Global Information Grid (GIG) under separate Managers



“Medically Ready Force...Ready Medical Force”

System View, Network and Security Architecture

PNW Sites, 'To-Be' State

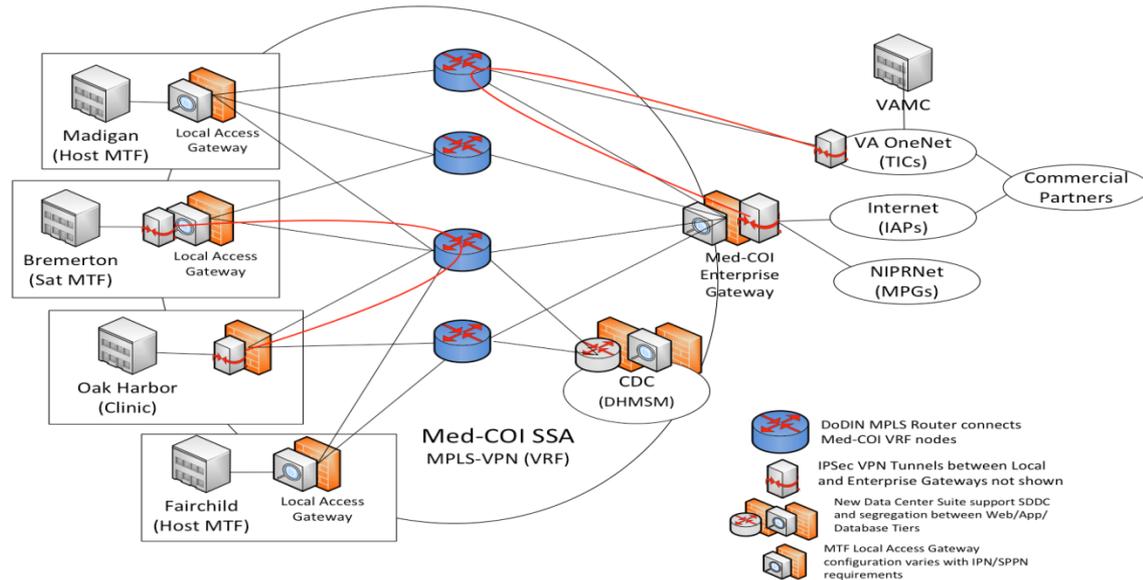
'To-Be' Highlights

Optimized transport over DoD Information Network(DoDIN) MPLS-VPN

Dynamic VPN supports confidentiality requirements and diverse path routing to enterprise G/Ws

Single security policy enforced across all nodes – standard interface to NIPRNet/External Networks

All WAN and Security Architecture components centrally managed (under DHA and DISA)



Transition to Med-COI, Army and Navy Sites



- MHSi G/Ws aligned with DISA managed Mission Partner G/Ws for Med-COI facing systems/enclaves
- DISN COI circuits extended to remaining VA Trusted Internet Connection (TIC) G/Ws and MHS/Med-COI Enterprise G/Ws; connections transitioned from Internet to Med-COI path thru 2014
- MHS CNDSP agreements established with DISA and Service CNDSPs
- Service Medical G/Ws consolidated behind MHS/Med-COI Enterprise G/Ws
- MHSi NIPRNet circuits migrated to MPLS COI
- MTF and MHS/Core Data Centers 'dual homed' with connections mediated via Enterprise G/Ws (will be maintained until transition is complete)
- MHS applications migrated from Service to MHS Enclaves with connections to the COI
- Service MTF security suites decommissioned

“Medically Ready Force...Ready Medical Force”

Transition to Med-COI, Air Force (AF) MTF Sites (Phase 2)



- Med-COI circuits and new Med-COI Access G/Ws deployed at AF MTFs*, residing behind MHS/Med-COI Enterprise G/Ws
- AF MTF enclave separated from local Base network. AF MTF/clinic uses existing fiber path to Base DISN demarcation point
- MHS application servers migrated to MHS address space concurrent with deployment of Access G/W*
- MHS enclave to remote MHS enclave or data center routes via Med-COI VPN
- Non-MHS/COI traffic default routes via VPN path to existing AF G/Ws to reach AF Base, AFNet, NIPRNet, or Internet based services/systems (pending A6 and Defense Information Assurance Security Accreditation Working Group approval of plans for Phases 2 and 3)

* Assumes consolidation of application servers to limited number of Host sites or RDCs in advance of the transition of smaller satellite clinics to the COI

Transition to Med-COI, FOC State Architecture

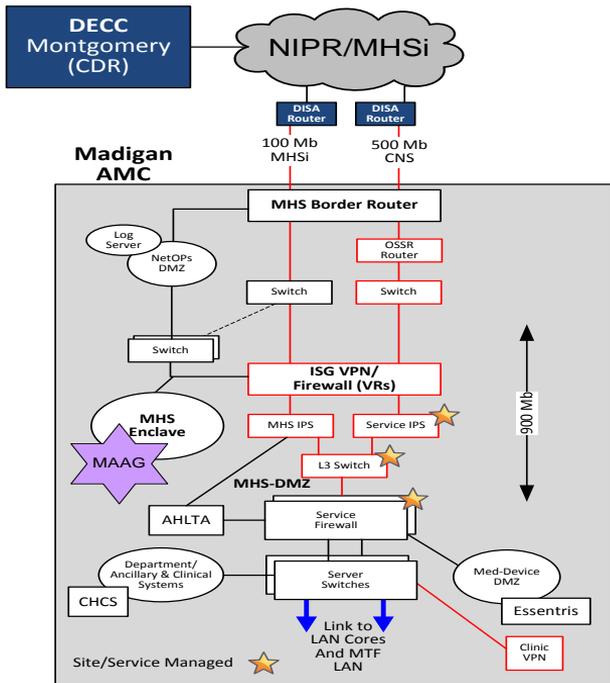


- All MHS apps at IPNs and SPPNs migrated to the COI
- All core medical services including services hosted in CDC's migrated to COI enclaves
- Reach-back to DISN/JIE core services via MPGs consistent with JIE-SSA
- Satellite MTFs direct connect to COI to access common services through consolidated security boundary
- VA/DoD primary communications path migrated to direct connect over DISN COI
- Migration of common external business partner connections to TIC G/Ws
- Possible integration of Med-COI Enterprise and Mission Partner G/Ws

PNW Network Architecture: Madigan NPS/IPN/SPPN Design

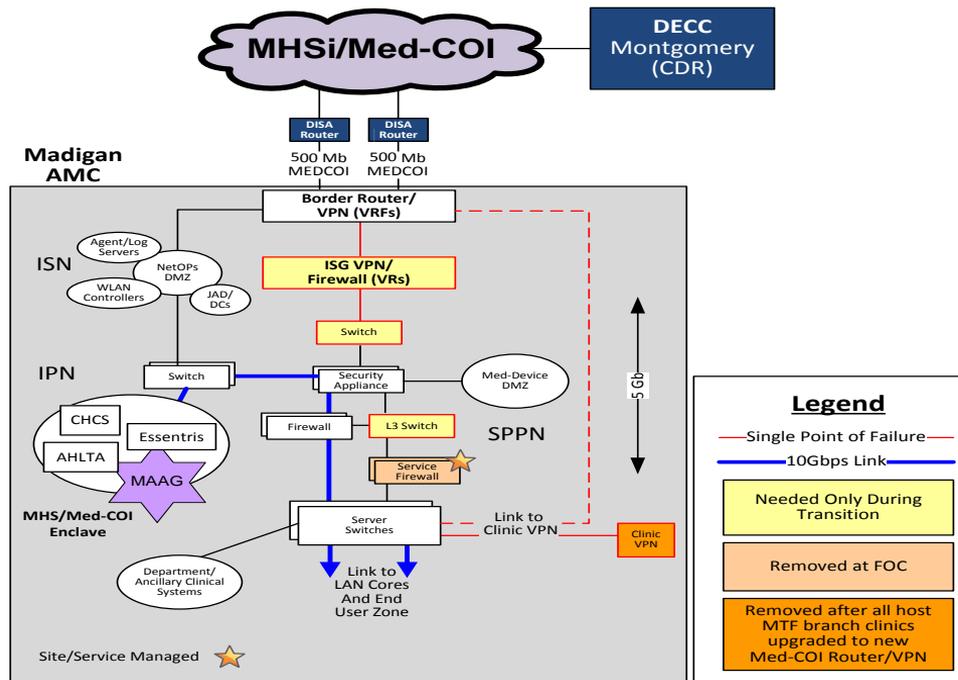
As-Is

MHSi/NPS 2.0



To-Be

Med-COI IOC



Legend

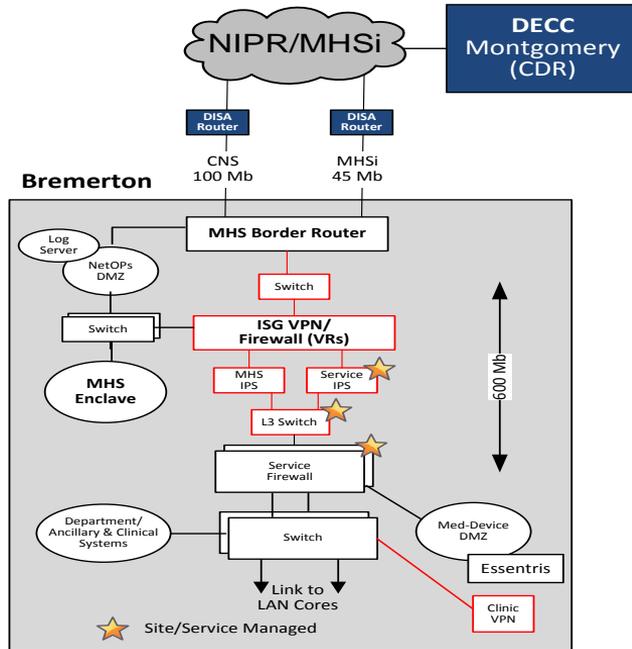
- Single Point of Failure —
- 10Gbps Link —
- Needed Only During Transition
- Removed at FOC
- Removed after all host MTF branch clinics upgraded to new Med-COI Router/VPN

“Medically Ready Force...Ready Medical Force”

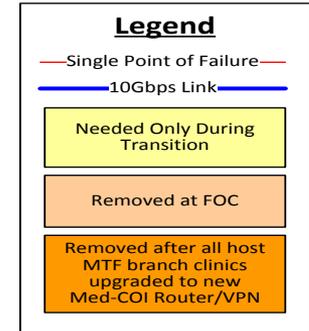
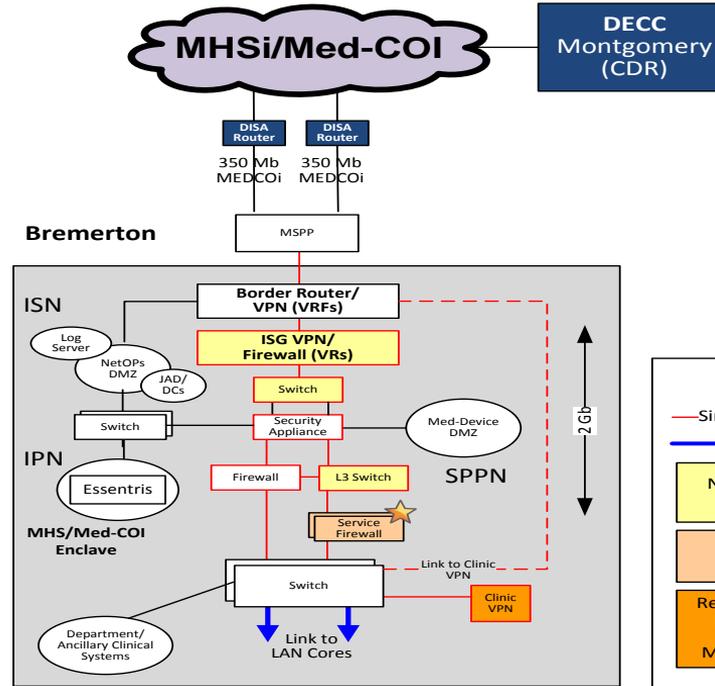
PNW Network Architecture: Bremerton NPS/IPN/SPPN Design



As-Is
MHSi/NPS 2.0

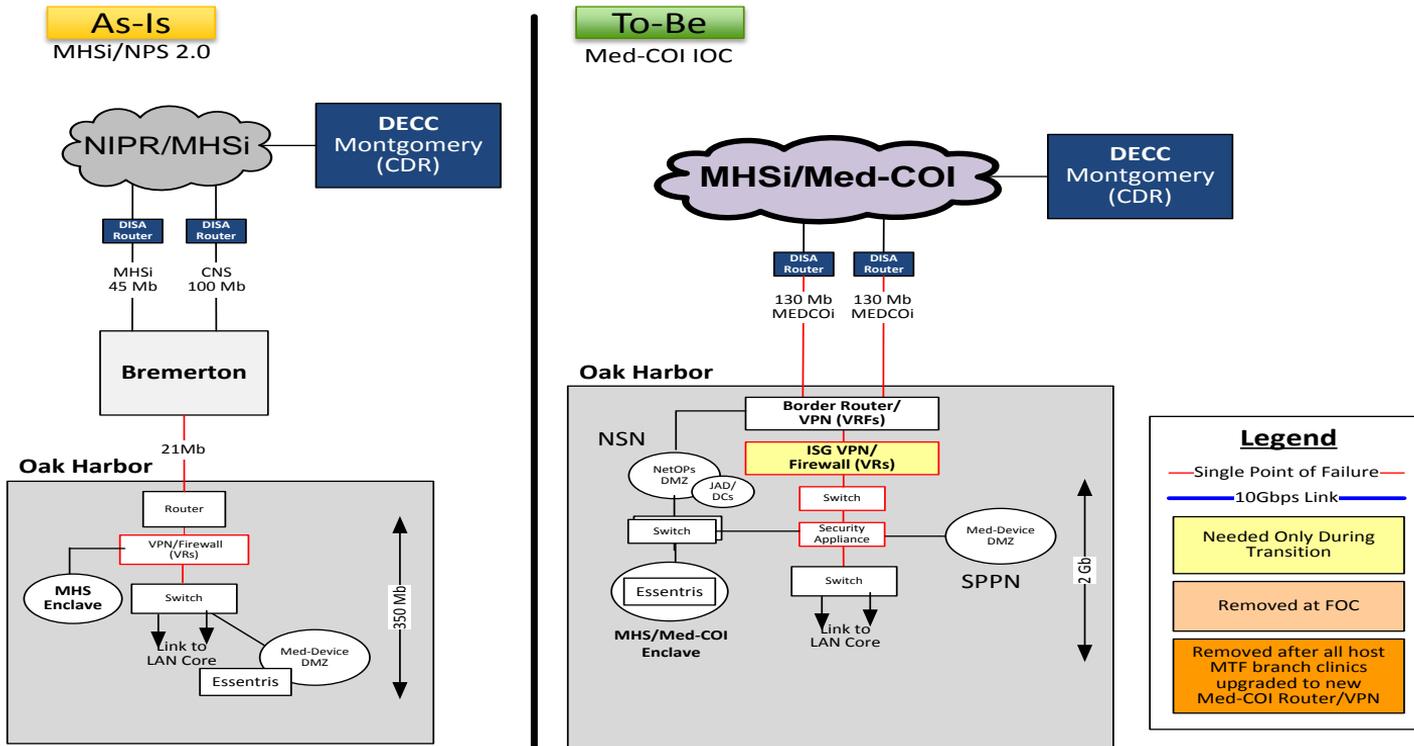


To-Be
Med-COI IOC



“Medically Ready Force...Ready Medical Force”

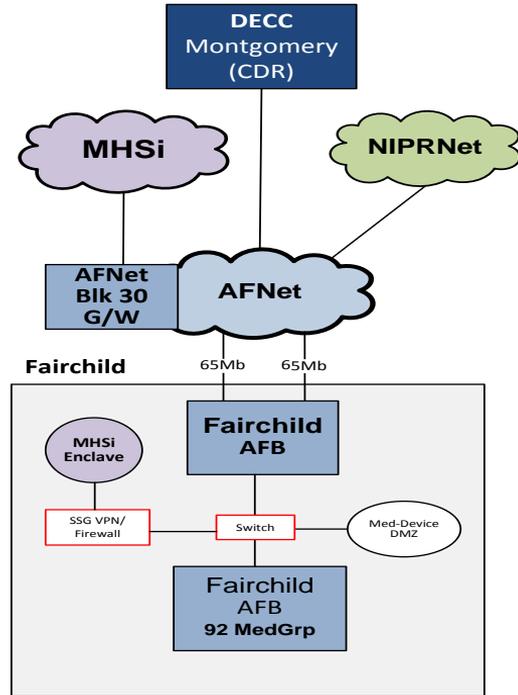
PNW Network Architecture: Oak Harbor NPS/IPN/SPPN Design



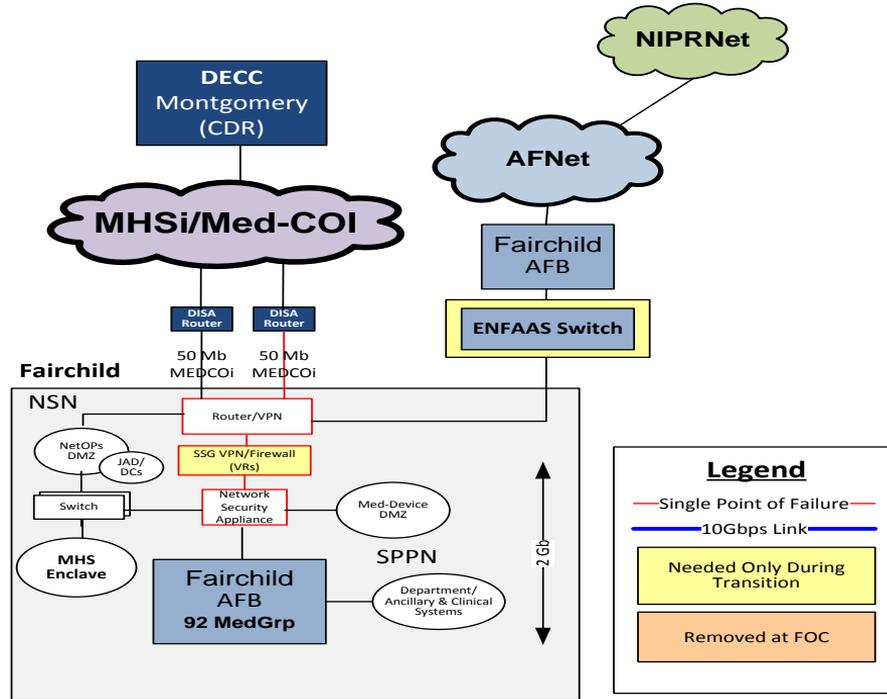
“Medically Ready Force...Ready Medical Force”

PNW Network Architecture: Fairchild NPS/IPN/SPPN Design

As-Is
MHSi/NPS 2.0



To-Be
Med-COI IOC



Legend

- Single Point of Failure —
- 10Gbps Link —
- Needed Only During Transition
- Removed at FOC

“Medically Ready Force...Ready Medical Force”

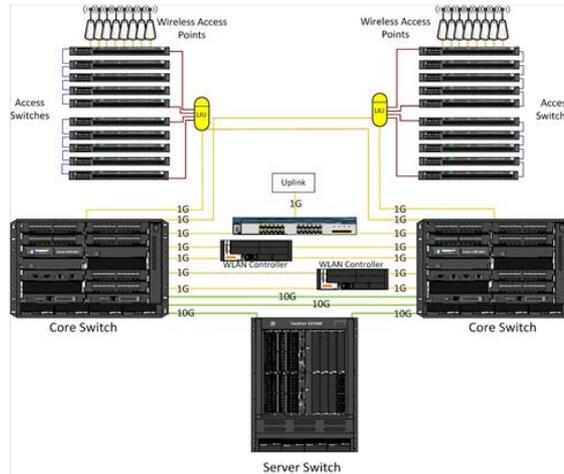
LAN/WLAN – System View ‘As-Is’ & ‘To-Be’

Madigan, Bremerton, Oak Harbor & Fairchild LAN/WLAN Capabilities

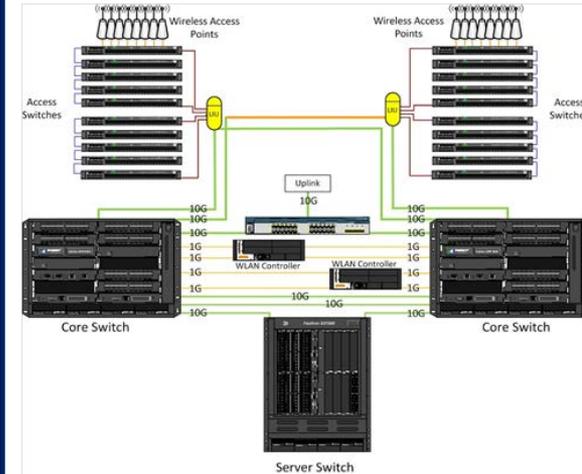


| | As-Is | To-Be |
|--|-----------------------------------|----------------------------|
| Wireless Access Points | 54 or 600mbps 802.11abg | 1.3gbps 802.11ac |
| To the Desktop | 1gbps | 1gbps |
| Interconnects – Main Computer Room | 10gbps | 10gbps |
| The Backbone – LAN Core to Access Layer | 1gbps | 10gbps |

As-Is



To-Be



“Medically Ready Force...Ready Medical Force”

Summary



- With the exception of current WAN bandwidth available to some sites, and earlier generation WLAN technology, the current network has sufficient capacity to support current and anticipated requirements for the new integrated EHR
- Planned upgrades are intended to address current performance/technology gaps and provide increased capacity
- New security architecture supports migration to ‘single enclave/single controlling authority’ supporting DHA IT service delivery, improves protections, and substantially reduces complexity, support requirements, and single-points-of failure

“Medically Ready Force...Ready Medical Force”

Please complete your evaluations

Contact Information



Mr. William Spencer

Chief, Engineering, Design & Deployment Branch
william.c.spencer61.civ@mail.mil

Mr. Albert Dickson

Acting Chief Operations Officer, Engineering, Design and
Deployment Branch
albert.n.dickson.civ@mail.mil

Back-Up Slides

Additional Notes



■ Guest Wireless

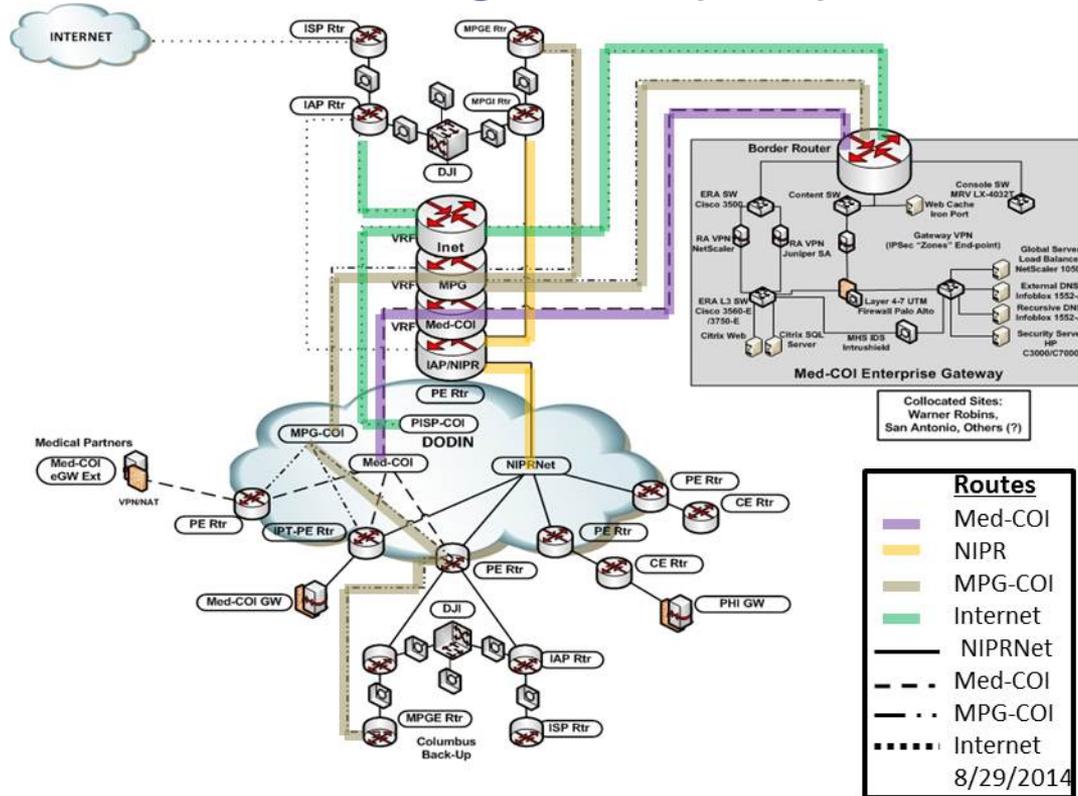
- ❑ Guest wireless has not been part of the baseline DHA offering in the past
- ❑ MAMC funded and maintains its own parallel wireless infrastructure for guest wireless (dedicated APs with a dedicated 25-50 Mbps circuit to the Internet)
- ❑ Guest wireless has been identified as a requirement and will be incorporated into the DHA baseline (not part of FY15 upgrades)
- ❑ Current plan is to install 802.11ac as part of FY15 upgrades, and then enable guest wireless when appropriate accreditations are in place

■ VoIP

- ❑ VoIP phones / call managers are not part of the current DHA baseline
- ❑ LAN infrastructure is capable of supporting IP telephony/unified communications
- ❑ Some sites have leveraged their own funding to acquire VoIP phones and operate them over the DHA network, other sites (e.g., Madigan) have elected to maintain parallel Plain Old Telephone Service (POTS) system for voice

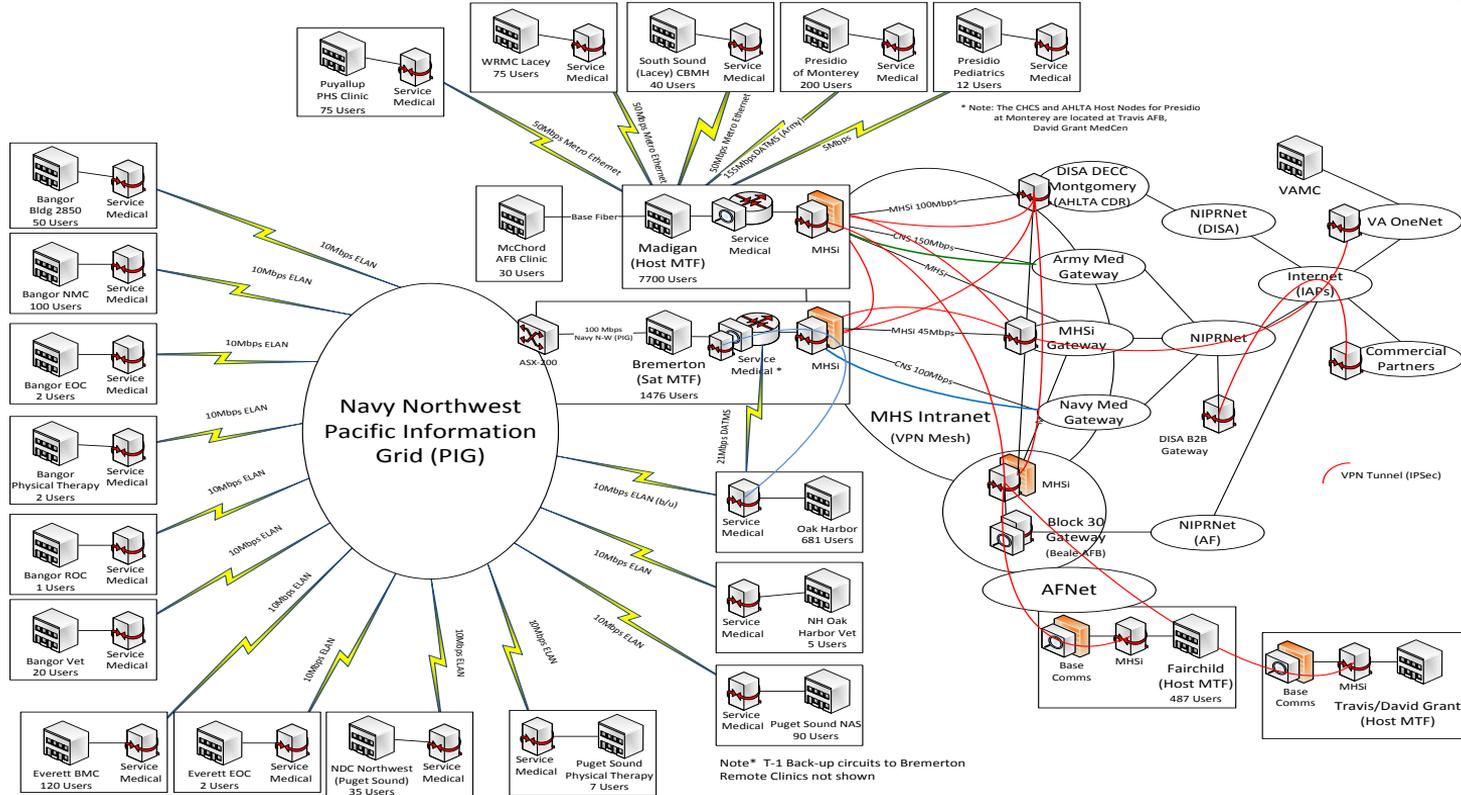
Med-COI Cyber Security Architecture

Med-COI/DISN NIPRNet/IAP Alignment (FOC)



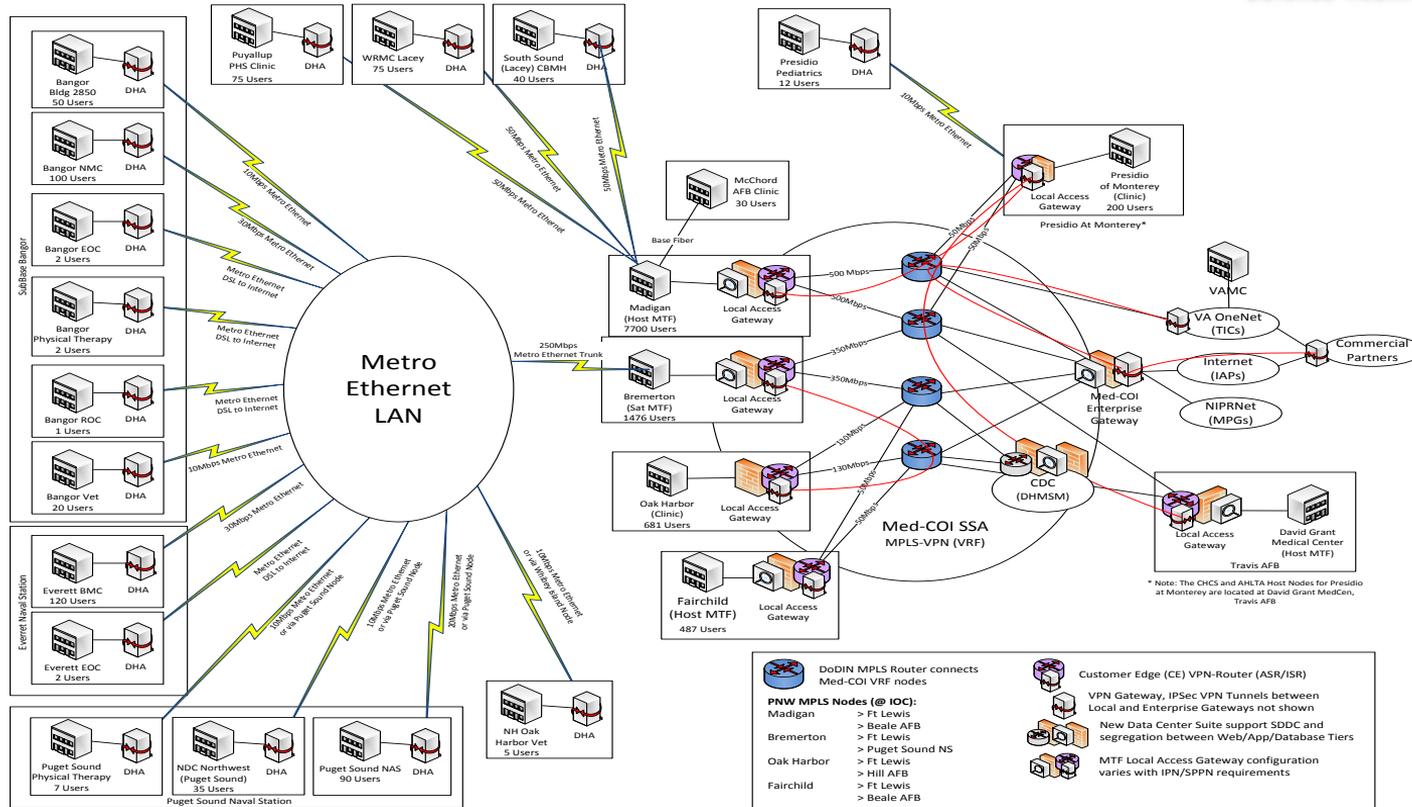
“Medically Ready Force...Ready Medical Force”

PNW Network Architecture 'As-Is'



"Medically Ready Force...Ready Medical Force"

PNW Network Architecture 'To-Be'



* Note: The CHCS and AHLTA Host Nodes for Presidio at Monterey are located at David Grant MedCen, Travis AFB

"Medically Ready Force...Ready Medical Force"