

2016 Defense Health Information Technology Symposium

Everything You Wanted to Know about Med-COI Cybersecurity 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

- Describe Cybersecurity Service Delivery for Medical Community of Interest (Med-COI)
- Differentiate Cybersecurity Services provided with Med-COI and those provided by Military Service Cybersecurity Service Providers (CSSPs)
- Identify how Authorizing Official (AO) / Designated Accrediting Authority (DAA) transition is and is not related to CSSP transition

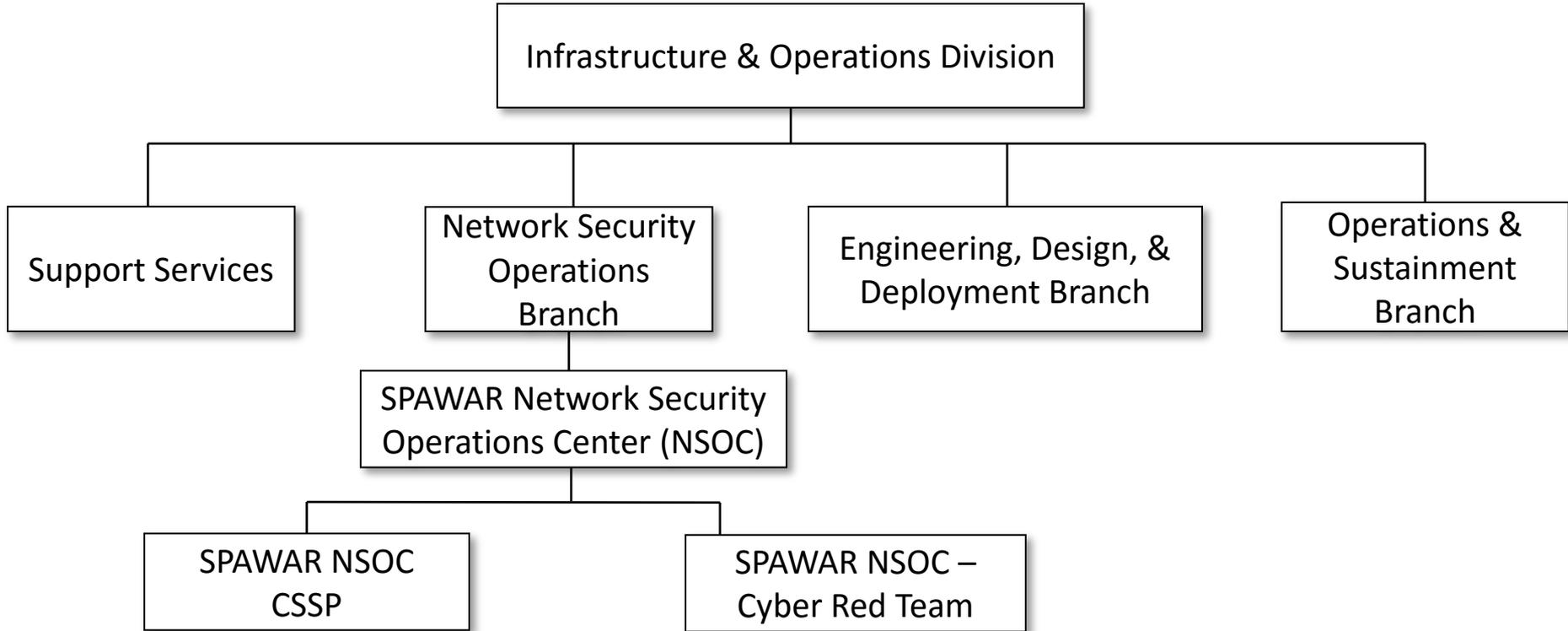
- Description of Cybersecurity Services
 - Protect, Detect, Respond, and Sustain
- Transition to Defense Health Agency's (DHA's) Cybersecurity Service Provider (CSSP)
 - Formerly Computer Network Defense Service Provider (CNDSP)
- Changes introduced upon migration to Med-COI

Cybersecurity Service Provider Background

- Solve Cybersecurity problems for the Department of Defense (DoD)
- Program established in 2001 by DoD Chief Information Officer (CIO)
- Certified by Defense Information Systems Agency (DISA) and accredited by U.S. Cyber Command
- Space and Naval Warfare Systems Command (SPAWAR) sponsored into program by Military Health System CIO in 2010



Organizational Alignment



“Medically Ready Force...Ready Medical Force”

DHA and Cybersecurity Services

- DHA subject to Triennial DoD Component Cybersecurity Service Alignment Validation Inspections by DISA
 - 2015 Results: *“DHA poses an overall LOW risk to the Department of Defense Information Network”*
- SPAWAR Network Security Operations Center (NSOC) subject to Triennial Accreditation Inspections by DISA and Defense Intelligence Agency
 - Designated Level 3 (Exemplary) Provider with 100% score
 - Credited with 10 “Best Practice” areas – *Highest in DoD*

GOOD JOB

Core Services

- Protect
 - Vulnerability assessment & analysis
 - Vulnerability management
 - Malware protection
 - INFOCON / CPCON
- Respond
 - Cybersecurity Incident Handling is Staffed 24x7x365
 - nsoc_cnd@nsoc.health.mil
Toll Free: 1-866-786-4432
DSN: 588-4432
- Detect
 - Information security continuous monitoring
 - Insider threat
 - Warning intelligence
 - Attack sensing and warning
- Sustain
 - Program management
 - Personnel
 - Security administration
 - Service provider information systems

Cybersecurity Services – Cyber Red Team

- Certified by National Security Agency and accredited by U.S. Strategic Command in 2014
 - Triennial accreditation inspections
- Blue Team assessment
- Red Team assessment
 - White Cell / Trusted Agent program
- Cooperative Vulnerability and Penetration Assessment
- Adversarial assessment
- “Playbook” assessments (aka Purple Team)



Cybersecurity Service Transition Phases

- Begins with transition from Service-provided Host Based Security Service (HBSS) & Vulnerability Scanning (VS) infrastructure (and related reporting chains) to the corresponding DHA-provisioned HBSS and VS capabilities
- Continues while agent-based capabilities are installed and configured on applicable end points
- Concludes with network migration configuration from Service to Med-COI gateways and System/Network Approval Process (SNAP) database update



Cybersecurity Service Delivery Approach

- Created *specifically for Military Medical Mission*
- Features Med-COI Single Security Architecture, Authority to Connect (ATC) Requirements, and DHA Cybersecurity Policy
 - Utilizes Network Protection Suite (NPS) and host-based capabilities
- Emphasis Upon *centralized, enterprise capabilities* reduces reliance upon military treatment facility (MTF) staff
- *Active participation* of MTF and program managed systems staff is still required
- Supplemental info (ATC capability and CONOPS documents, etc.):
<https://info.health.mil/hit/io/nso/nsm/SitePages/Cybersecurity%20Service%20Provider%20Tools%20CONOPs.aspx>



Changes Introduced

- Flat organizational structure
 - No tier structure (e.g., Enterprise Security Operations Center for Navy Medicine or Regional Cyber Center for Army Medicine)
- MTFs and program managed systems are provisioned with centrally managed infrastructure for performing cybersecurity / risk management / information assurance duties
 - Host Based Security Service (HBSS) and vulnerability scanning
 - End users complete DD Form 2875 for access as required

Changes Introduced

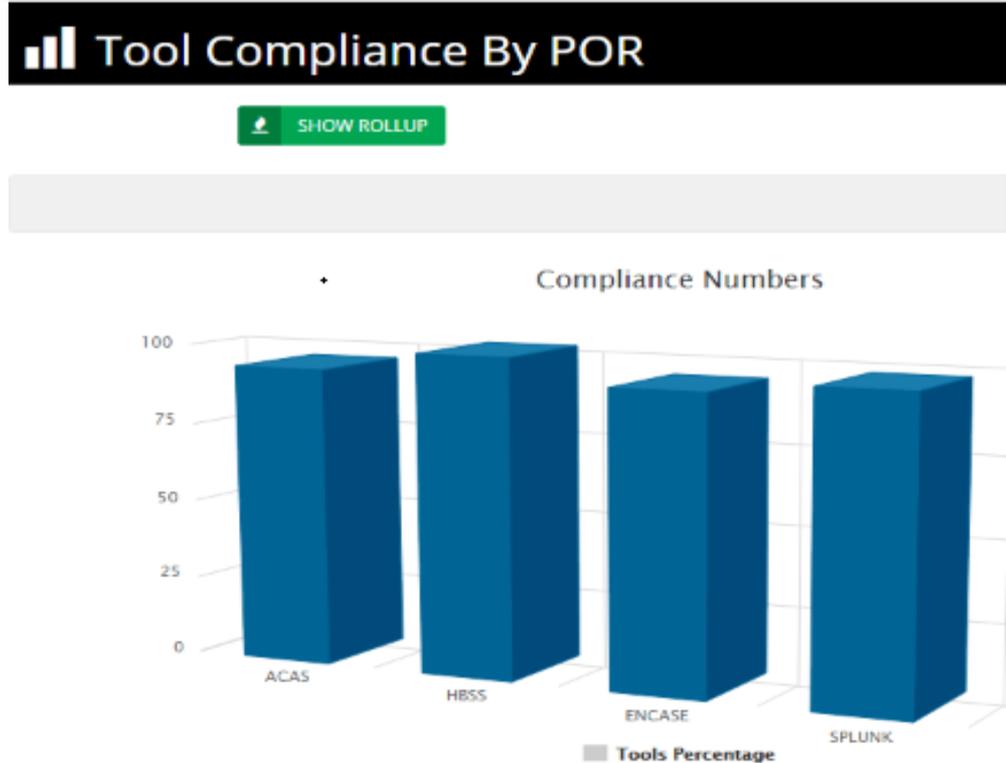
- Investigations and incident response is centralized
 - Med-COI enterprise forensic, audit logging, and host-based analysis capabilities require installation and configuration of agent software on applicable systems
 - Includes Desktop-as-a-Service (DaaS) coordination and integration
- ***Full deployment of cybersecurity capabilities requires direct participation from MTF & program management office staff, and others***
- Tight integration with Operations and Sustainment Branch for time sensitive, tactical adjustments to Med-COI Single Security Architecture

Changes Introduced

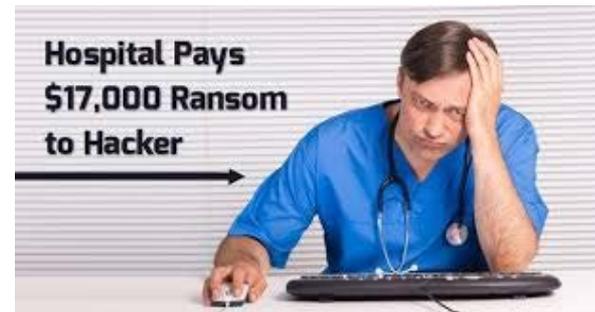
- Pre-coordinated Blue Team assessment upon successfully completed Med-COI migration
- Quarterly assessments of cyber threat landscape
- Cybersecurity mission readiness measurements performed at MTF and program managed system levels
 - Monitors successful operation & utilization rates of provisioned cybersecurity infrastructure when compared to number of fielded systems
- Supplemental information (daily status, threat reporting, capability readiness statistics, etc.):
 - <https://kbs.nsoc.med.osd.mil/CNDSubscriber/SitePages/Default.aspx>

Emphasis on Capabilities Readiness

- Heavy reliance upon enterprise capabilities necessitates cybersecurity capabilities “readiness” measurements
- Provides validation of Med-COI Authority to Connect (ATC) criteria
- Automatically measured and communicated on *per-site* and *per-program management office* basis



Threat Environment and Climate



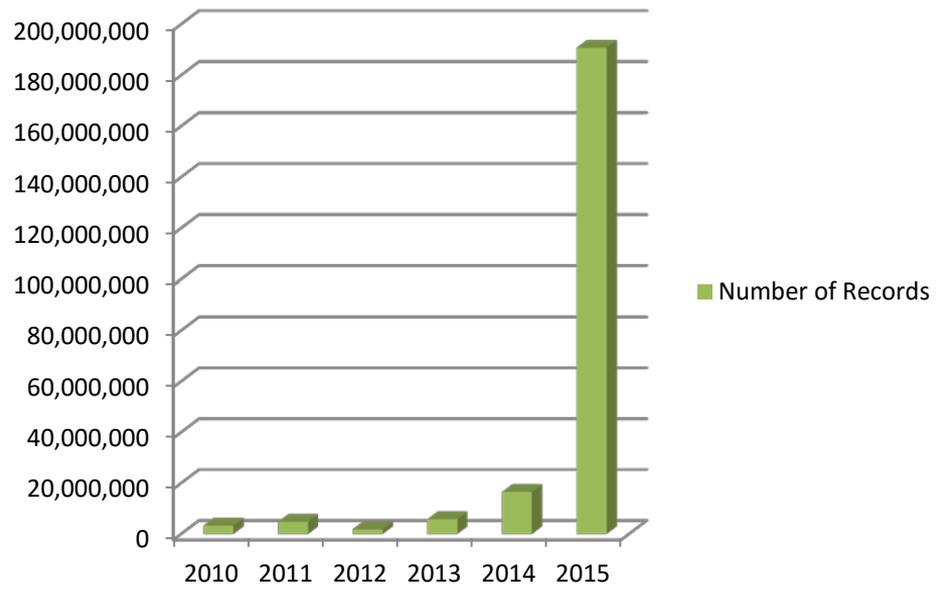
“Medically Ready Force...Ready Medical Force”

Threat Environment and Climate

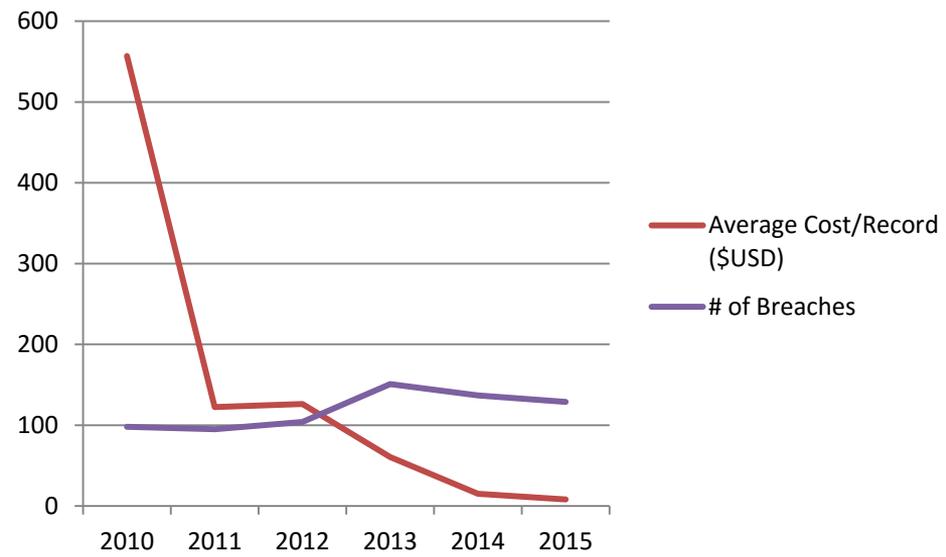


2016 Defense Health Information Technology Symposium

Healthcare Records Exposed via Network Breaches & Theft



Healthcare Records on the Black Market & Number of Breaches



“Medically Ready Force...Ready Medical Force”

Authorizing Official / Designated Accrediting Authority Transition Impact



Defense Health Agency

2016 Defense Health Information Technology Symposium

- Med-COI falls under DHA Authorizing Official / Designated Accrediting Authority (DAA)
- Cybersecurity Service Provider (CSSP) assignment, designation, and scope of responsibilities defined by the DISA SNAP database
 - CSSPs assigned to individual DISN circuits and corresponding IP space
 - DHA's CSSP is assigned responsibility for Med-COI circuits and MHS Intranet enclaves only and will not service Army, Navy, or Air Force networks as defined by SNAP database
- Service transition of the AO / DAA role to DHA for systems and sites does not trigger CSSP transition

“Medically Ready Force...Ready Medical Force”

Cybersecurity Services Notional RACI Chart



Defense Health Agency

2016 Defense Health Information Technology Symposium

Tasks	MTF	HIT	POR	CSSP
DHA Cybersecurity Service Provider (CSSP) Alignment	I	A	I	R
Med-COI Connection Authority to Connect (ATC)	A R	R A	A R	I
Detect & Respond Services	I	C	I	A
Local Site Touch Labor Support (e.g. Selected Respond Actions)	R	C	I	A
Vulnerability Management (IAVAs)	R	A	R	C
Conduct Monthly Credentialed Vulnerability Scanning	R	A	R	R
HBSS Compliance	C	A	C	C
Red / Blue Team Assessments	- / C	C / C	- / C	A / A

R-Responsible; A-Accountable; C-Consult; I-Inform

MTF-Military Treatment Facility; HIT-DHA Health IT Directorate; POR-Program of Record

“Medically Ready Force...Ready Medical Force”

Summary

- Cybersecurity service delivery under Med-COI will be different
- Service transition requires active participation by MTF and program managed system staff
- Service delivery effectiveness and readiness will be measured
- Cybersecurity service transition requires integrated efforts and good communications

Key Takeaways



Defense Health Agency

2016 Defense Health Information Technology Symposium

- Med-COI cybersecurity service was built specifically to support the military medical mission
- Services and corresponding capabilities are assessed to perform at the highest possible level
- Cybersecurity is a DHA shared responsibility
- Med-COI transition and cybersecurity service provider transition require active participation and constant communication

“Medically Ready Force...Ready Medical Force”

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

Jason Jurand

Technical Lead, SPAWAR Network
Security Operations Center

jason.jurand@nsoc.health.mil

Backup

Acronyms

Acronym	Description
ACAS	Assured Compliance Assessment Solution
AO	Authorizing Official
ATC	Authority to Connect
CIO	Chief Information Officer
CNDSP	Computer Network Defense Service Provider
CONOPS	concept of operations
CPCON	
CSSP	Cybersecurity Service Provider
DAA	Designated Accrediting Authority
DaaS	Desktop-as-a-Service

Acronyms (continued)



Defense Health Agency

2016 Defense Health Information Technology Symposium

Acronym	Description
DHA	Defense Health Agency
DISA	Defense Information Systems Agency
DoD	Department of Defense
HBSS	Host Based Security Service
IAVA	Information Assurance Vulnerability Alert
INFOCON	Information Operations Condition
Med-COI	Medical Community of Interest
MHS	Military Health System
MTF	military treatment facility

“Medically Ready Force...Ready Medical Force”

Acronyms (continued)



Defense Health Agency

2016 Defense Health Information Technology Symposium

Acronym	Description
NPS	Network Protection Suite
NSOC	Network Security Operations Center
SNAP	System/Network Approval Process
SPAWAR	Space and Naval Warfare Systems Command
VS	vulnerability scanning