

## 2015 Defense Health Information Technology Symposium

# DOD Medical Device Cybersecurity Considerations



*“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 processes a medical device user community must apply to protect confidentiality and integrity of electronic information
- Recognize how Information Technology, Cyber Security and Clinical Engineering/Medical Logistics collaboration is critical to maintain an organization's protection posture
- Recognize the various protection postures an organization may implement with regards to medical devices host security and in compliance with a DHA Single Security Architecture

# Agenda



- Background
- Directives for Securing Resources
- Three Part Problem
- Implementing a Different Approach
- Risk Assessment
- Threats
- High Level View – The Process
- Conclusion

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

# Background



- DHA Health Information Technology (HIT) Directorate in an effort to reduce variability by means of standardization
  - ❑ Established a cross functional Integrated Project Team (IPT) to meet multiple technical needs and process initiatives in support of standardization of cybersecurity classifications, criteria and mitigations for Medical Devices mapped to the DHA network architecture.
  - ❑ Developed a technical architecture available as part of the Medical Community of Interest (Med-COI) architecture Special Purpose Node (SSPN) delivering defense in depth protections
  - ❑ Supports the alignment of process and implementation, but does not “own” the Medical Device implementation.

# Directives for Securing Resources



## ■ Executive Orders, Directives and Guidance

- ❑ Healthcare and Public Health part of Critical Infrastructure Sector (Presidential Policy Directive/PPD-21)
- ❑ National Infrastructure Protection Plan Healthcare and Public Health Sector Specific Plan
- ❑ Health Information Technology (HITECH) Act of 2009 provisions
- ❑ Health and Human Services (HHS) directives
- ❑ Food and Drug Administration (FDA) and HHS guidance

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

# Department of Defense Instructions (DoDI) for Securing Resources



- DoDI 8510.01 Risk Management Framework (RMF), dated 12 March 2014
  - Platform Information Technology (PIT) / Industrial Control Systems (ICS) Cybersecurity Authorization Metrics
    - “Each ...system, and PIT must have Authorizing Official for authorizing the system’s operation...”
- DoDI 8500.01 Cybersecurity, dated 14 March 2014
  - Comply with DoDI 8500 Cybersecurity & DoDI 8510 RMF
    - “All IT that receives, processes, stores, displays or transmits DoD information will ....be consistent with applicable DoD cybersecurity policies, standards, and architectures.”
    - “Examples of platforms that may include PIT are: ... medical devices and health information technologies...”

# Three Part Problem

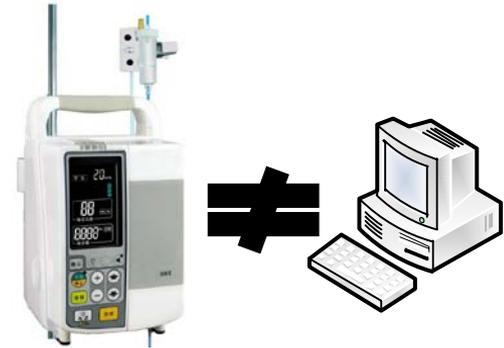
## ■ The need:

- ❑ Increased need to share electronic patient data has increased number of networked medical devices and applications
- ❑ Medical devices are key tools used to diagnose and treat DOD beneficiaries



## ■ The guidance:

- ❑ Public laws and DOD regulations provide general guidance on protection requirements, gaps remain for systems that cannot meet traditional cyber security measures
- ❑ FDA regulated devices for a specific purpose cannot be treated as regular information technology (IT) devices



# Three Part Problem (con't)



## ■ The challenge:

- ❑ Safety, effectiveness and data, and system security are key properties for connecting networked medical devices without compromising delivery of care and the organization
- ❑ Connecting a regulated medical device to an unregulated network results in a “medical IT network” with a new set of risks possibly affecting patient safety and medical efficacy
- ❑ Convergence of various medical devices built by multiple vendors on a single network increase
  - number of security vulnerabilities
  - likelihood of compromising data confidentiality, integrity, and availability

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

# Implementing a Different Approach

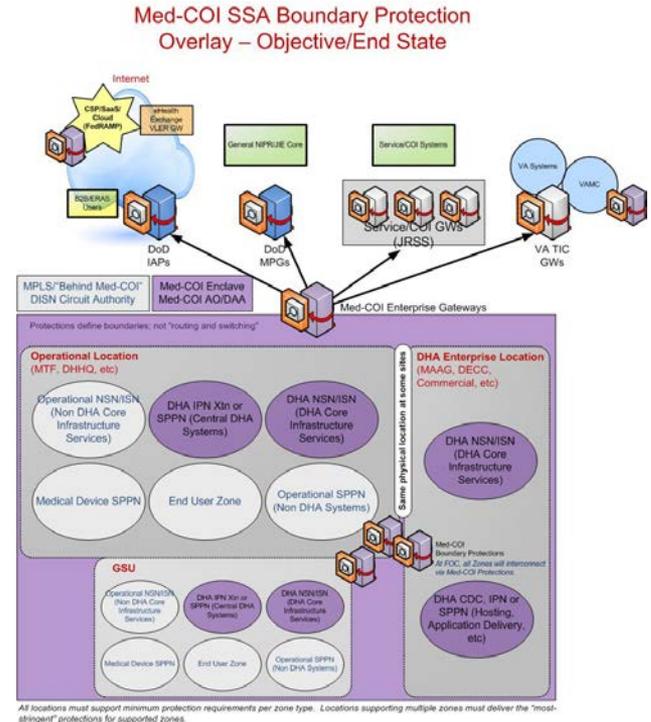
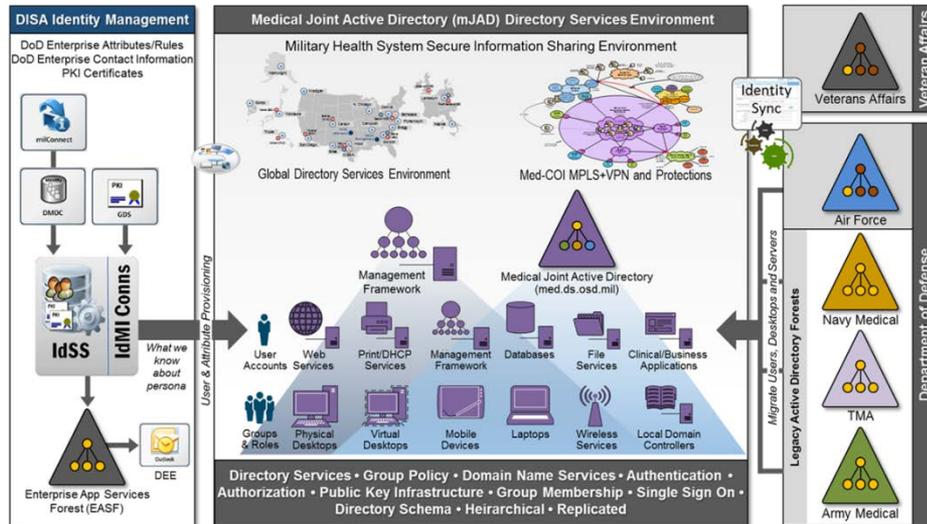


- DHA HIT sponsored a DHA Medical Device Information Assurance (IA) Architecture and Standards Integrated Project Team to:
  - Align and standardize cybersecurity architecture and mitigations for Medical Devices across DHA Stakeholders supporting:
    - Clinical Functions
    - DHA Consolidation, Med-COI Transition, and Defense Healthcare Management System Modernization (DHMSM) Delivery
  - Acknowledge resource limitations leading to trade-offs
  - Achieve dual goal: Improve patient outcomes and secure networks
  - Maximize medical device vendor vulnerability management controls
  - Leverage to maximum extent Med-COI Single Security Architecture (SSA) SSPN defense in-depth protections

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

# Implementing a Different Approach (con't)

- DHA delivers a single, centrally managed directory and cyber security services infrastructure providing authentication and authorization to simplify and optimize resource access.



***"Medically Ready Force...Ready Medical Force"***

- Traditional published IT guidance provides a general framework
- Med-COI SPPN approach recognizes that
  - Each healthcare activity is unique and must be evaluated as such
  - An overarching or “one size fits all” type of assessment does not take into consideration the diversity of systems found in one location

# Threats



## ■ Reported cases

- ❑ Malware on Healthcare.gov health insurance marketplace (PCWorld, Sep 14)
- ❑ Possible vulnerabilities in two computerized drug infusion pumps manufactured by Hospira (AHA News, May 15)
- ❑ Community Health Systems Inc. data exfiltration affecting about 4.5 million patients (CIO Website, Aug 14)

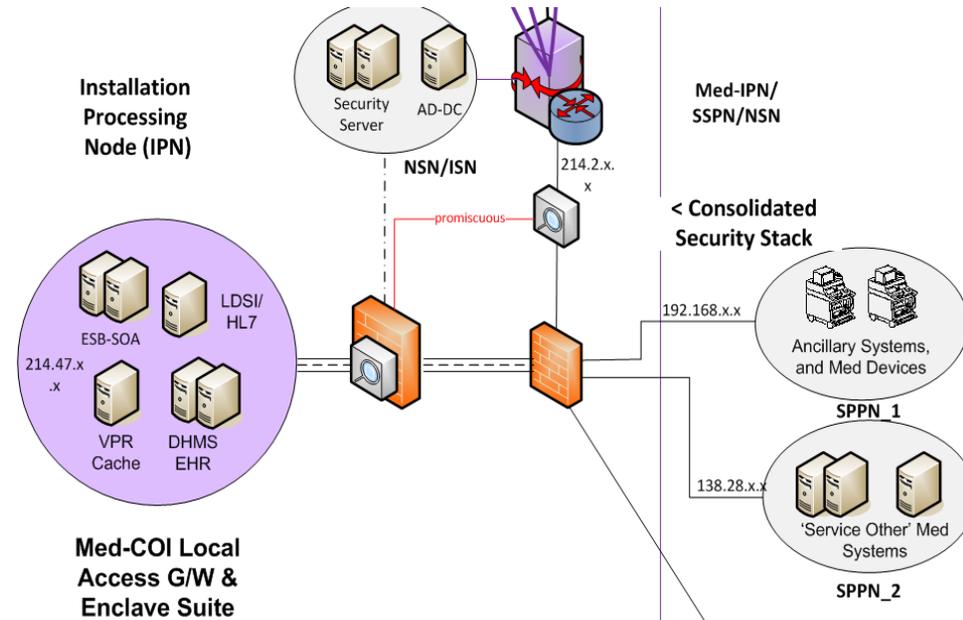
## ■ Healthcare and Public Health Sector Cyber Risk Framework

Category	Common Elements
Threats	Insider threat, hacking, and terrorism Botnets, malware, phishing, and distributed denial of service Natural disaster
Vulnerabilities	Inadequate patch management, configuration management, and password management Lack of antivirus protection and intrusion prevention and protection Software vulnerabilities and SQL injections Open USB ports, DVD, CD and R/W drives
Consequences	Loss of personally identifying information and identity theft Patient errors Inability to use patient data or deliver HPH services
Cascading Consequences	Forensic and system recovery service fees Blackmail and fraud (medical and financial) Loss of brand reputation Civil suits Financial theft and insolvency Loss of services Loss of life
Mitigation Strategies	Redundant and failover systems and warm backup sites Background investigations Identity management Multifactor authentication Intrusion prevention and detection Least privilege Data encryption Anti-virus software Auditing Hardware lockdown

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

# High Level View – The Process

- In collaboration with Cyber Security Division (CSD), DHA MEDLOG, and Medical Services
  - ❑ Identify medical device DOD RMF system and information type categorization
  - ❑ From categorization generate Request for Information/Query (RFI/RFQ) Vendor Cyber security questionnaire
  - ❑ Initiate Authorization or Risk Assessment process approved for Medical Devices deployed in a Med-COI SSPN



# High Level View – The Process (con't)



- Evaluation of aggregate system components increase impact of configuration changes
- Interconnection points and dependencies require evaluation to avoid outages
- Requires analysis beyond what is required in traditional networks
- Cybersecurity support for medical devices is the responsibility of
  - IT and Cybersecurity Staff
    - Support cybersecurity processes, IT patches and network resources
  - Clinical Engineering and BioMed staff
    - Management & scheduling of medical device maintenance
    - Oversight of safe use of all medical devices
  - Medical Device Vendor
    - Warranty and contract support for medical devices

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

# Conclusion

- Healthcare practitioners and business partners will rely on digital communications and shared data
- Policies, laws, and regulatory guidance provide a framework for security and privacy needs
- DHA desired end state for medical devices
  - ❑ Assured delivery of Medical Device data across devices and infrastructure
  - ❑ Standardized infrastructure protections
  - ❑ Standardized classification, controls criteria and mitigations
  - ❑ Standardized risk review, Authorization and Connection Approval process



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

# Contact Information



Enedina “Dina” Guerrero

Acting Chief, Incident Management/SOC Liaison Section  
Cyber Security Operations Branch, Cyber Security Division

[enedina.guerrero.civ@mail.mil](mailto:enedina.guerrero.civ@mail.mil)

# Questions?



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

# Evaluations



- Please complete your evaluations

# References



- AHA News Now (2015, May). FDA alerts health care facilities to infusion pump cybersecurity vulnerability. *AHA News Website*. Retrieved from AHA News website at <http://news.aha.org/article/fda-alerts-health-care-facilities-to-infusion-pump-cybersecurity-vulnerability>
- Eastwood, B. (2014, Aug). Community Health Breach Highlights Healthcare Security Vulnerabilities. *CIO Website* . Retrieved from CIO website at <http://www.cio.com/article/2597970/healthcare/community-health-breach-highlights-healthcare-security-vulnerabilities.html>
- Paul, I. (2014, Sep). Botnet malware discovered on Healthcare.gov server. *PCWorld Website*. Retrieved from PCWorld website at <http://www.pcworld.com/article/2603361/botnet-malware-discovered-on-healthcaregov-server.html>