

HIMSS[®]18

WHERE IT CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

Risk Management Framework for DoD Medical Devices

Session 136, March 7, 2018

Lt. Col. Alan Hardman, Chief Operations Officer, Cyber Security Division, Office of the DAD IO/J-6

William Martin, Deputy of Cybersecurity, Information Systems Security Manager, US ARMY Medical Materiel Agency (USAMMA), Integrated Clinical Systems Program Management Office (ICS PMO)

ENGAGED

www.himssconference.org



DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.

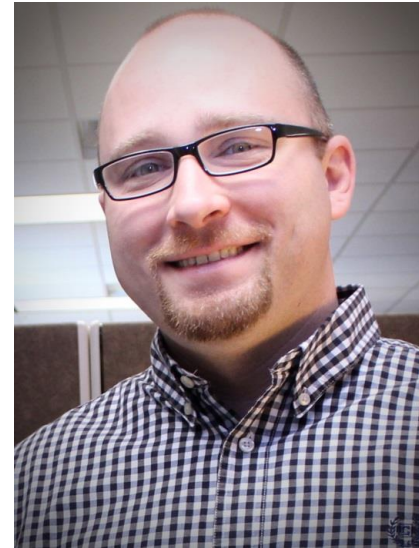
Speaker Introduction

Lt Col Alan C. Hardman
Chief Operations Officer
Cyber Security Division
Office of the Deputy Assistant
Director Information Operations
(DAD IO)/J-6
Defense Health Agency (DHA)



Speaker Introduction

William Martin, Deputy of
Cybersecurity, Information
Systems Security Manager
US Army Medical Materiel
Agency (USAMMA)
Integrated Clinical Systems
Program Management Office



Conflict of Interest

Alan Hardman, DHA, has no real or apparent conflicts of interest to report.

William Martin, USAMMA, Integrated Clinical Systems Program Management Office has no real or apparent conflicts of interest to report.

Agenda

- DHA's role in Risk Management Framework (RMF)
- DoD Cybersecurity Policy Requirements (USAMMA)
- Vendor Requirements RMF (USAMMA)
- Tri-Service/DLA Contracting Language

Learning Objectives

- Describe the DHA Cybersecurity role in RMF
- Identify DoD Cybersecurity policy requirements
- Outline vendor requirements for an RMF effort
- Discuss general workflow and timeframes for Department of Defense (DoD) RMF activities

DHA Focus Areas

- Broad overview
- DHA assigned RMF roles
- How we got here
- Single reliable network
- How it applies to Medical Devices-isolation architecture
- Bringing it together: Medical Device Integration

Describe DHA Role in the Military Health System (MHS) & RMF

- DHA: Joint Integrated Combat Support Agency
- Delivering Single Reliable Medical Network
- Operating under a single Chief Information Officer (CIO)/Authorizing Official
- Single authority for accepting risk and granting authorization decisions
- Develops, implements & enforces MHS Cybersecurity and RMF program

DHA Roles

- DHA Roles

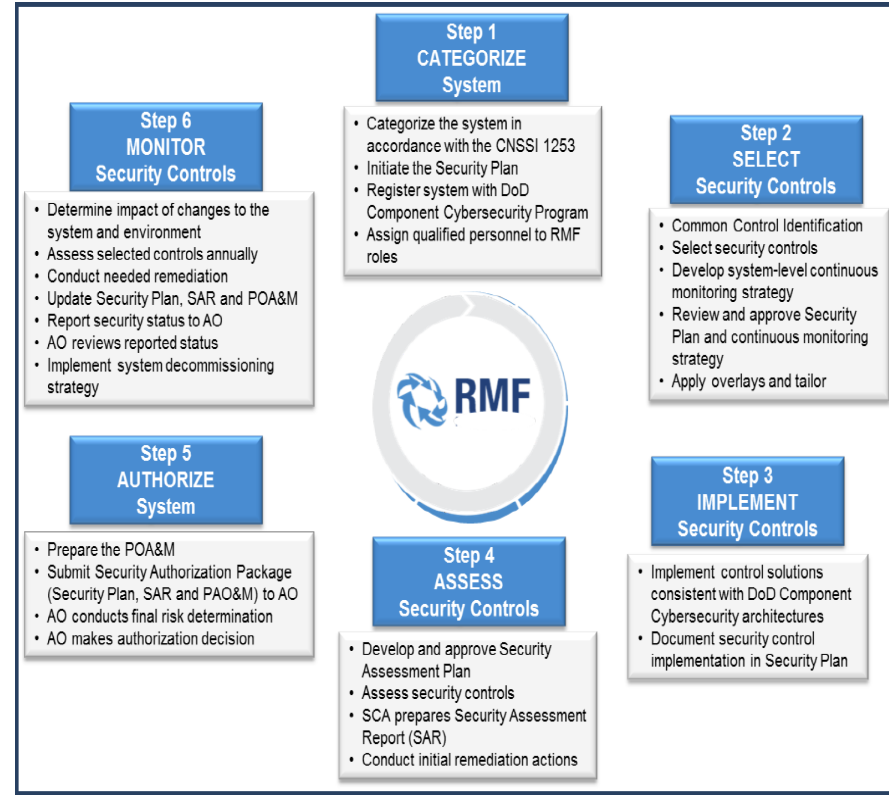
- CIO
- Authorizing Official

- DHA Cybersecurity Roles

- Senior Information Security Officer
- Security Control Assessor

- DHA Cybersecurity Responsibilities

- Assessments



MHS Information Technology (IT) Infrastructure Consolidation

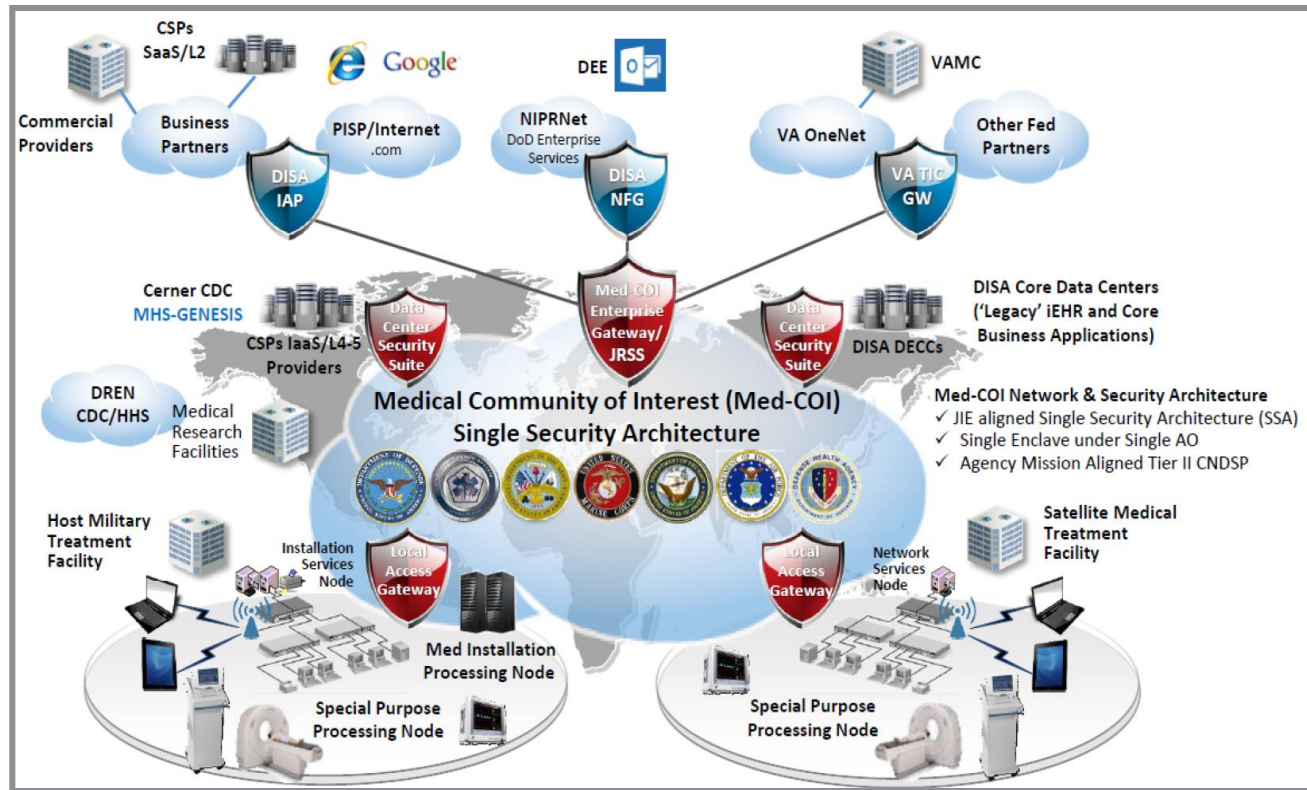
Desktop-to-Datacenter (D2D) achieves the MHS IT Infrastructure savings and consolidation mandated by Congress under the 2013 National Defense Authorization Act (NDAA), while simultaneously ensuring a robust, secure and highly available infrastructure capable of supporting MHS GENESIS mandated under the 2014 NDAA



<p>2013 NDAA mandated:</p> <ul style="list-style-type: none"> • MHS Reform • Establishment of the DHA • A shared service model for the MHS with the goal of improving clinical and business practices, cost reductions, infrastructure reductions, and personnel reductions 	<p>Resulting from the 2013 NDAA, three Business Case Analyses (BCAs) were conducted for HIT:</p> <ol style="list-style-type: none"> 1. Reengineering IT Management (BCA#1) 2. Infrastructure Consolidation (BCA#2) 3. Portfolio Rationalization (BCA#3) <p>BCA#2 concluded significant and tangible savings could be derived from MHS IT infrastructure consolidation</p>	<p>The 2014 NDAA mandated:</p> <ul style="list-style-type: none"> • DHA to ensure the required medical IT infrastructure is in place and capable of supporting Department of Defense (DoD) Healthcare Management System Modernization (DHMSM) requirements for the DoD Electronic Health Record (EHR)—MHS Genesis • MHS Genesis requirements include high availability, short recovery times, and greater bandwidth 	<p>The 2017 NDAA mandated:</p> <ul style="list-style-type: none"> • Directed implementation of broader responsibilities • Reform of administration of the DHA and military treatment facilities (MTFs) 	<p>DHA’s IT infrastructure readiness plan brings together multiple IT components to create a more effective and efficient technical environment for the MHS; this plan was branded as D2D</p> <p>D2D allows DHA to deliver the mandated dual requirements of a single, consolidated medical IT infrastructure that is robust, secure and highly available while absorbing baseline funding cuts</p>
--	--	---	--	---

Medical Community of Interest (Med-COI): A Single Reliable Medical Network

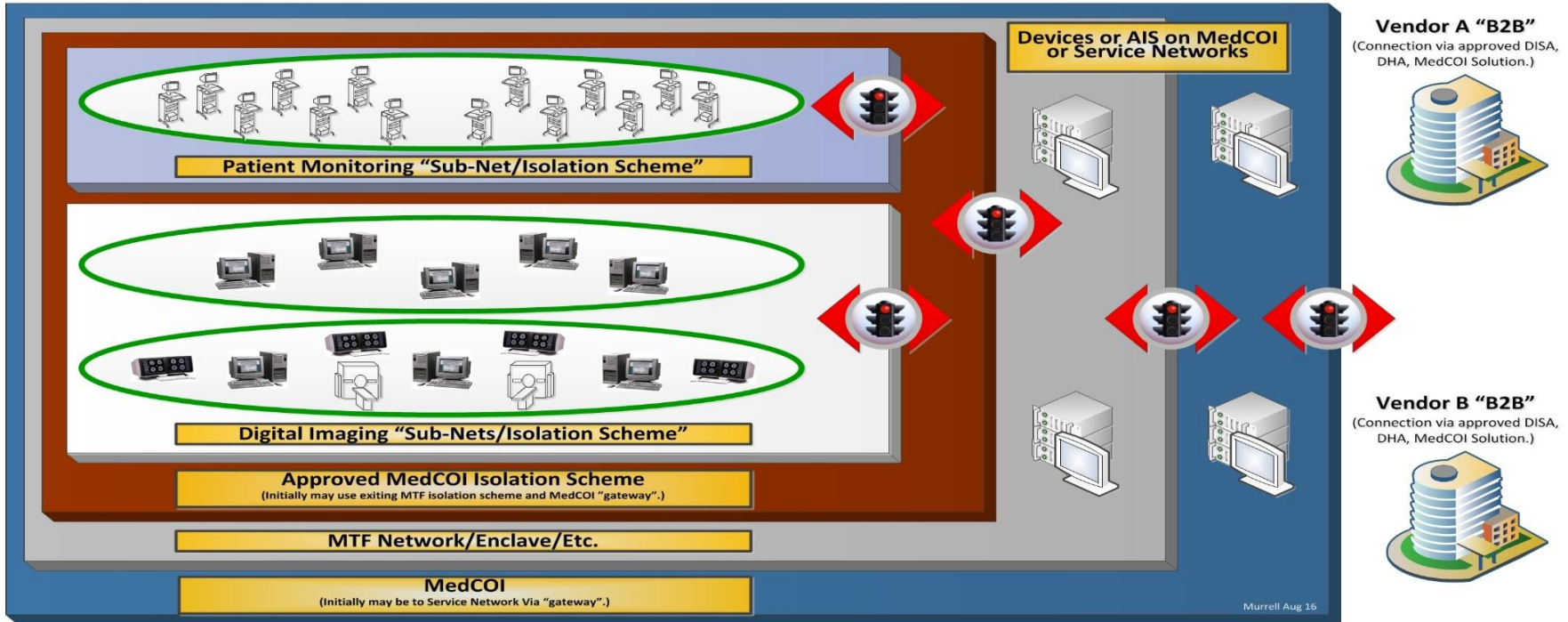
Med-COI provides a seamless, integrated network across the Enterprise, on which information, systems and applications will be accessible to users across the DoD healthcare environment. It is a “hard” requirement for MHS GENESIS



Generic Use Case Leveraging Infrastructure Protections

Medical Device Isolation/Network Protection Scheme

Example: Two "subnets" with all connectivity outside "Subnets" blocked.



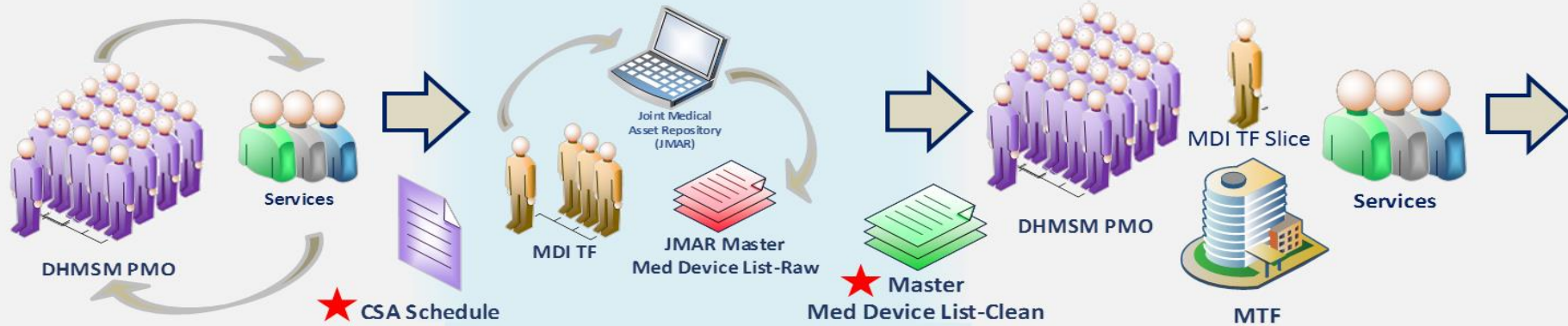
"Lights/Arrows" used in graphic indicate "rule sets" in place at firewalls/gateways/routers/switches/etc. to manage device connectivity between major network layers. For simplicity, only one set of "arrows/lights" are used to depict allowable connections. In reality, "rule sets" are cumulative based on each device's approved communications. Often, there will be requirements for connectivity to multiple "external" devices/systems. (EX: Digital Imaging will have rules for connecting to EHR, B2B, archives, etc.)

MDI Task Force Integration Into Current State Assessment (CSA) Process (1 of 2)







1. CSA Schedule Coordination

2. Medical Device Inventory Analysis

3. CSA Site Visit

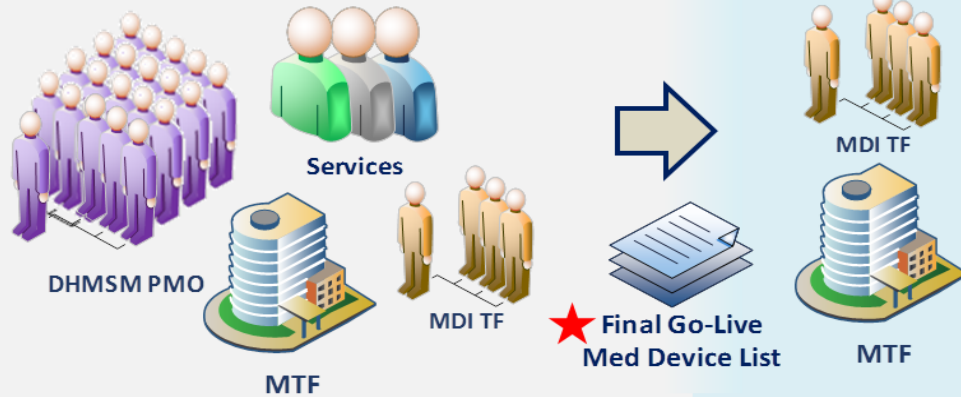


3. CSA Site Visit Details

	 Medical Device Inventory Review	 Functional Workflow	 Track RMF Status	 Medical Device Procurement
 PMO/LPDH Med Device Staff	What is currently connected to CHCS and Essentris	What is currently connected to CHCS and Essentris	Not In Scope	Not In Scope
 MDI TF Slice	What is NOT currently connected to CHCS and Essentris	What is NOT currently connected to CHCS and Essentris	Capture status for Med Devices connected to Essentris & CHCS and not Connected	Review current medical equipment replacement plans and priorities







MDI Task Force Integration Into Current State Assessment (CSA) Process (2 of 2)

4. Model System Review (MSR)



5. MDI Task Force Ongoing Engagement Activities

- Advocate for Governance prioritization of clinical capabilities not in MHS GENESIS Go-Live baseline (e.g. Ophthalmology, Dermatology)
- Propose workflows for devices that will not connect at Go-Live
- Aggregate RMF statuses, share best practices, elevate challenges
- Identify MTF, regional, and MHS standardization opportunities
- Support Biomed with Technical Documentation

 Deliverables	 Medical Device Inventory Review	 Functional Workflow	 Track RMF Status	 Medical Device Procurement
 MDI TF	<p>Med Device List Supplement</p> <ul style="list-style-type: none"> • Includes Lifecycle Management Factors, CareAware Compatibility, and Cerner Compatibility 	<p>MHS GENESIS Interoperability Roadmap</p> <ul style="list-style-type: none"> • Details workflows for systems that will not be connected at Go-Live • Identifies MTF specific critical clinical capabilities 	<p>RMF Status Tracker</p> <ul style="list-style-type: none"> • Details RMF status of all medical devices that will connect to MHS GENESIS and will be interoperable • Will aggregate for MHS and Service review 	<p>Medical Device Procurement Guidance Report</p> <ul style="list-style-type: none"> • Makes recommendations for upcoming medical device replacements and new systems • Shares standardization opportunities

ARMY USAMMA Focus Areas

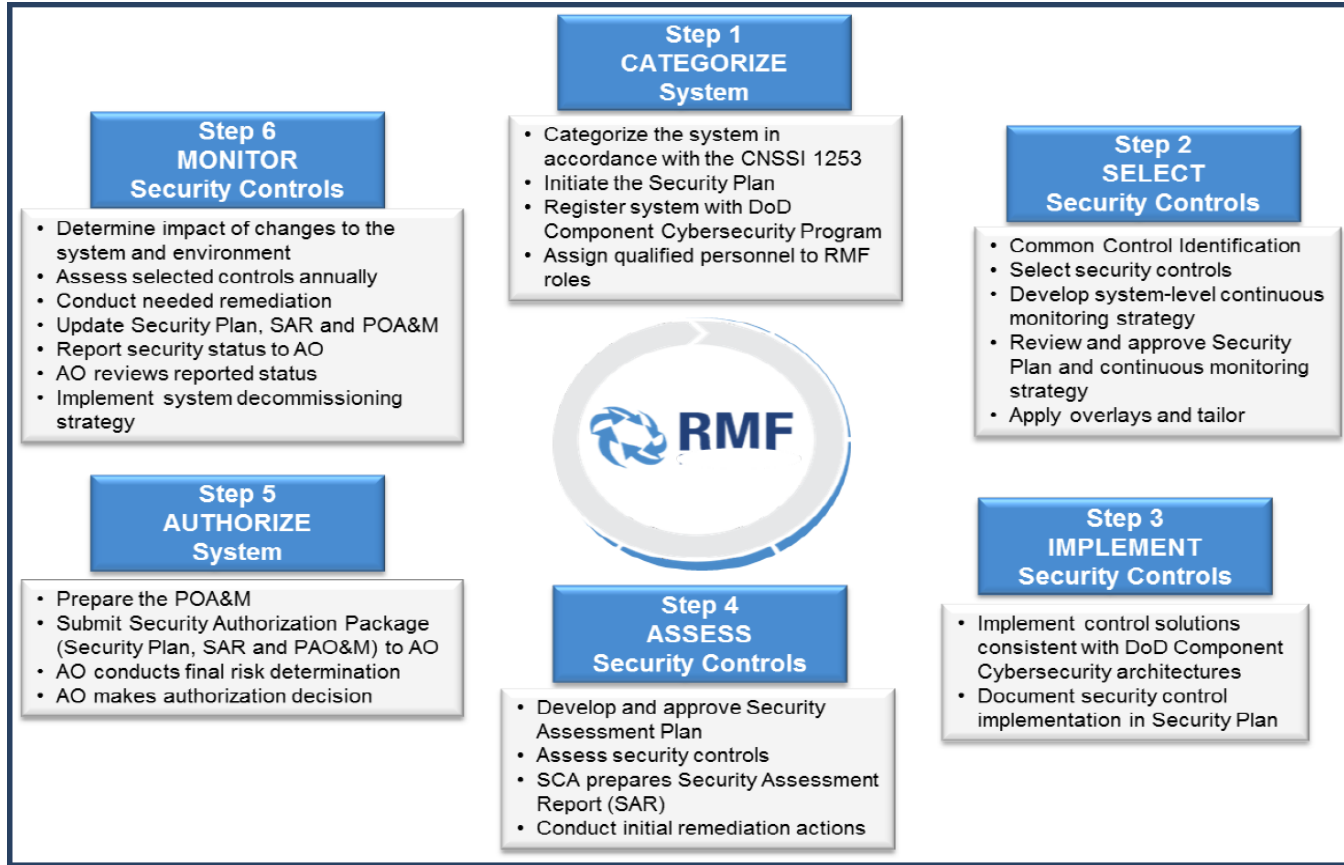
- Identify DoD Cybersecurity policy requirements
- Outline vendor requirements for an RMF effort
- Discuss general workflow and timeframes for DoD RMF activities
- Tri-Service/DLA Contracting Language

Identify DoD Cybersecurity Policy Requirements

A little background...

- Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002 (FISMA) and requires, among other things, that federal agencies develop/document/implement agency-wide information security program(s) for information systems that support the operations and assets of the agency
- DoD mandated RMF via DoDI 8500.01: March 14, 2014 and DoDI 8510.01: March 12, 2014
- DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation process is dead

Identify Cybersecurity Requirements (RMF lifecycle, NIST 800-37 Rev. 1)

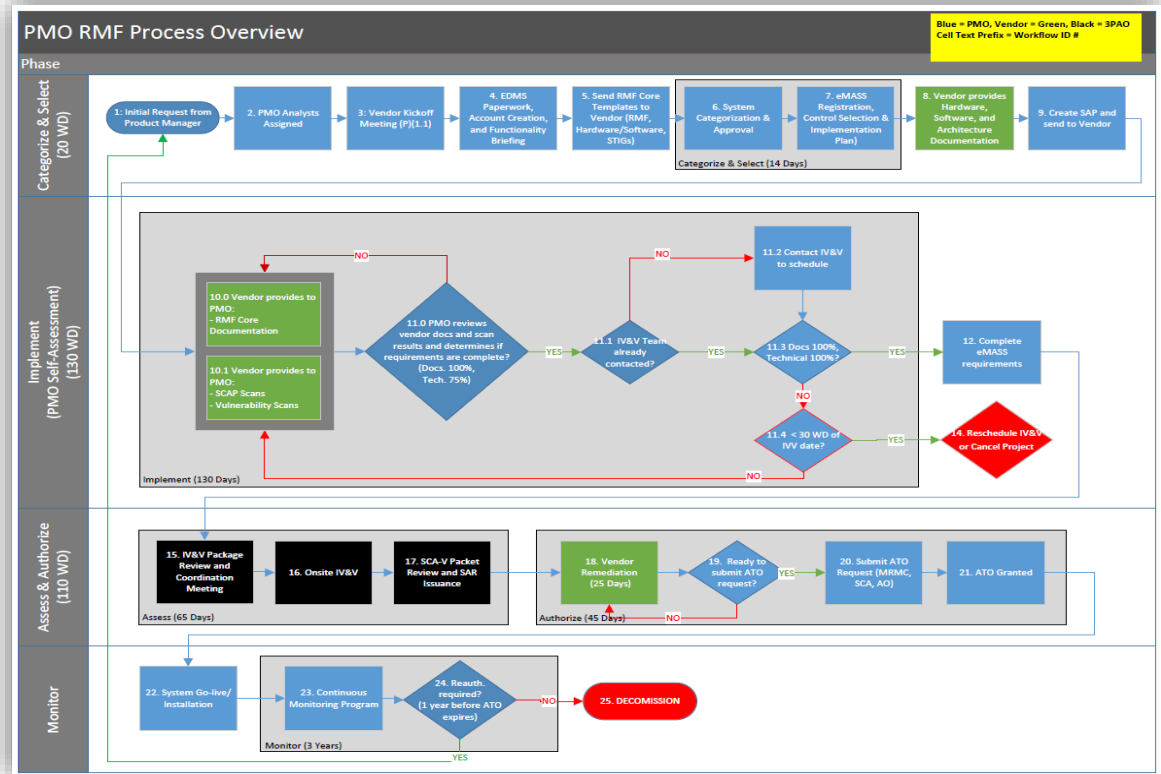


Discuss General Workflow and Timeframes for DoD RMF Activities

Approx. timeline for RMF activities (USAMMA specific)

- Categorize & Select : 20 WD
- Implement: 130 WD
- Assess & Authorize: 110 WD
- Monitor: 3 Yrs.

Total = 260 WD (approx. 1 calendar year)



Outline Vendor Requirements for an RMF Effort

(U.S. Army Cybersecurity/RMF Requirements, June 6, 2017)

- **System Security**

- Cybersecurity Questionnaire
- Pre-validation Screening
- Mitigation of Category I&II / Mod, High, Very-High assessment findings
- Assigned Cyber Point of Contact (POC) & Subject Matter Experts (SME)
- Authority to Operate (ATO) within 12 months of award
- No delivery/payment until ATO
- Maintain ATO for warranty/SMA/contract lifetime
- Regulations Compliance

Outline Vendor Requirements for an RMF Effort (cont.)

- **Security Assessment & Authorization (SA&A)**
 - All RMF docs submitted within 4 months of request/kick-off
 - Any additional docs submitted within 30 days of request
 - Technical scans submitted within 1 month of kickoff
 - Technical scans submitted monthly until ATO
 - Support Defense Information Systems Agency (DISA) approved Intrusion Detection/Prevention Systems (IDS/IPS), Anti-virus (AV), Antimalware, and a correlating Plan of Action and Milestones (POAM)

Outline Vendor Requirements for an RMF Effort (cont.)

- **Training/Cert Req. (Business-to-Business [B2B], etc.) for Priv./Administrator accounts**
 - Cyber Certification
 - Background Investigation
 - Professional Baseline Cert.
 - Computer Environment (CE) Certification
 - Information Assurance (IA) Training (Cybersecurity Fundamentals, Cyber Awareness)
 - Two-Factor Authentication / Common Access Card (CAC)
 - Acceptable Use Policy (AUP)

Outline Vendor Requirements for an RMF Effort (cont.)

- **Warranty and Post-Warranty SMA**

- Maintain test lab
- Update ATO docs per system changes
- Maintain security boundary
- DoD Information Assurance Vulnerability Management (IAVM) compliance
- Update per Security Technical Implementation Guide (STIG) within three months
- Monthly vulnerability and Security Content Automation Protocol (SCAP) scans
- Remediate vulnerabilities/POAMs within 3 months
- Annual security policy/plan/procedure reviews
- DISA B2B compliance

Tri-Service/DLA Contracting Language

- Samples included in this presentation are ARMY USAMMA specific
- Other ARMY medical device acquisition groups (MEDCOM, MRMC), DoD medical device acquisition groups (AFMOA, NAVY), and DHA are targeting similar Cybersecurity requirements/contract language

Key Takeaways

- Awareness of Cybersecurity related laws and policies for DoD/DHA medical devices
- Emphasis on vendor participation and response to:
 - RMF requirements and efforts
 - General timelines for RMF activities
 - Understanding PMO/Vendor responsibilities
- Collaborative effort to secure modern medical devices

References/ Resources

- Transitioning from DIACAP to RMF (article)
 - <https://phoenixts.com/blog/diacap-vs-rmf/> (no endorsement site or author)
- NIST Risk Management Framework (RMF) Overview
 - [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(RMF\)-Overview](https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview)
- NIST SP 800-37 Rev.1 (Rev.2 forthcoming, introducing “Step 0”)
 - <https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final>
- NIST 800-53 Rev. 4 Security Controls
 - <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- DoD Policy Documents (8500.01, 8510.01)
 - www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf
 - www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf

Questions

Contact information:

- Lt. Col. Alan Hardman, alan.c.hardman.mil@mail.mil
- William B. Martin, william.b.martin82.civ@mail.mil

Lastly, please remember to complete the online session evaluation