

2015 Defense Health Information Technology Symposium

From Service DIACAP to DHA RMF:
What This Means to You



“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



- Discuss the changes to assessment and authorization process
- Describe DHA HIT's Assessment and Authorization vis-a-vis the Services
- Discuss the capabilities the RMF Knowledge Service provides in support of the RMF process, specifically for DHA IT
- Identify the role of eMASS in the assessment and authorization process

- Risk Management Framework (RMF) Overview
- DoD IT Assessment & Authorization
- DHA RMF Roles and Responsibilities
- DHA RMF Transition
- RMF Security Control Inheritance
- DHA RMF Implementation Strategy
- RMF Transition Summary

DHA Risk Management Framework



Continuous Monitoring:
DHA TTPs, ACAS, SPs,
CMRS, HBSS

Security Plans: R&R,
Arch Diagrams,
Description, Boundary

MONITOR

CATEGORIZE

SELECT

**DHA RISK
MANAGEMENT
WORKFLOW**

Security Plans: Controls,
Implementation and
Inheritance

**Authorization
Decision Document**

AUTHORIZE

IMPLEMENT

Self Assessment:
Assessment Plan, POA&M
Remediation & Mitigation

**Security Assessment
Report:** ACAS Findings,
POA&M, RAR

ASSESS

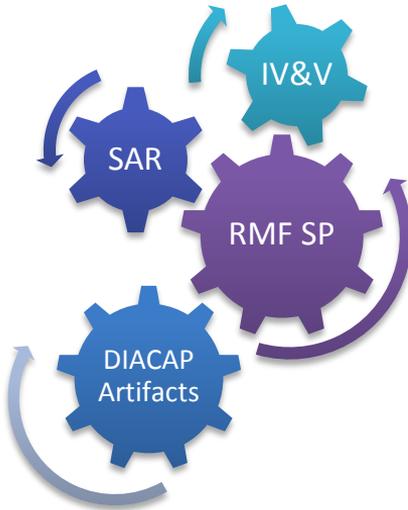
“Medically Ready Force...Ready Medical Force”

DHA RMF Transition Timeline

Current DoD Transition Guidance DoDI 8510.01

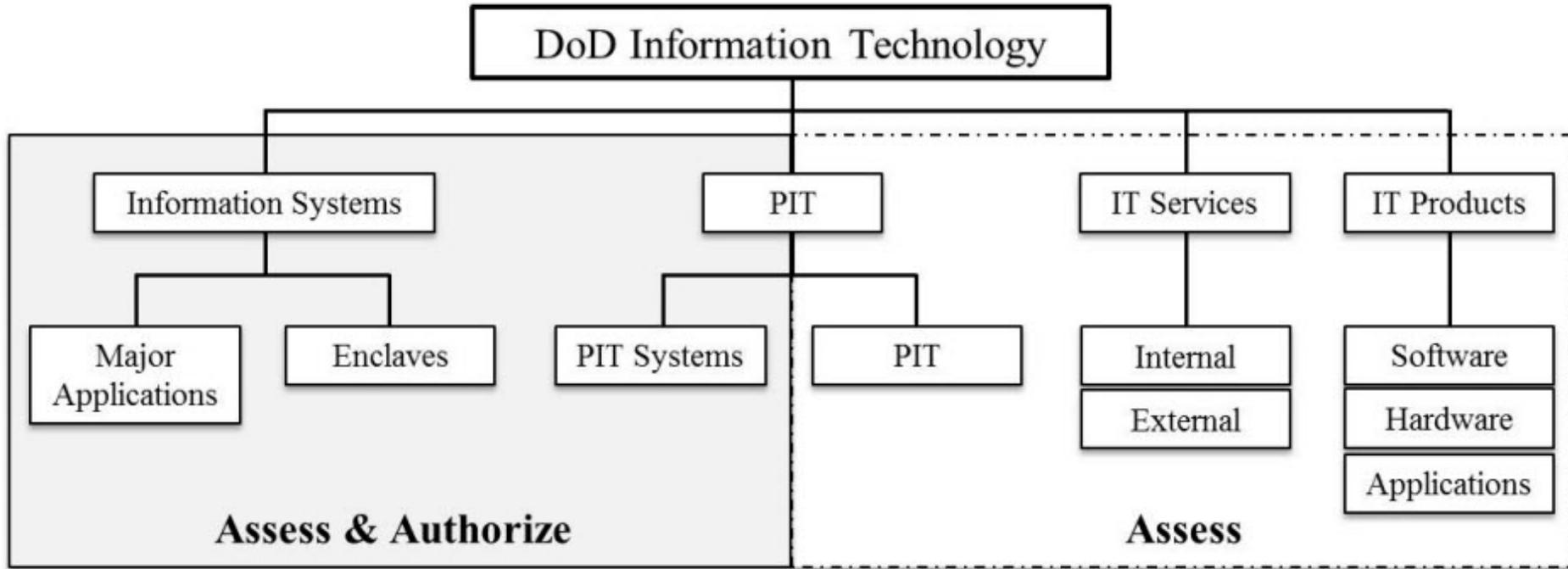
Transition to the RMF within 3 years and 6 months from the effective date of DoDI 8510.01 (12 March 2014)

Pending Changes to DoD RMF Transition Guidance



Completed DIACAP Package Submitted to AO for Signature	Maximum Duration of ATO under DIACAP
Prior to May 31, 2015	2.5 years from AO signature date
June 1, 2015 - February 1, 2016	2 years from AO signature date
February 2, 2016 - October 1, 2016	1.5 years from AO signature date

DHA IT Assessment and Authorization



“Medically Ready Force...Ready Medical Force”

DHA RMF Key Roles



Role	New To RMF	Appointee	Appointed By
CIO	No	Mr. Bowen, Director, HIT, CIO	DoD Component Head
Authorizing Official	Yes (DAA)	Mr. Bowen, CIO	Director, DHA
Senior Information Security Officer	Yes (SIAO)	Mr. Rowland, Chief CSD	CIO
Security Control Assessor	Yes (CA)	Lt. Col Hardman, COO CSD & others	SISO
Information System Owners	No	Various	Component Head, CIO, or Designated Representative

DHA RMF Key Roles (continued)



Role	New To RMF	Appointee	Appointed By
Program Manager(s) / System Manager(s)	No	Various	Component Head, CIO, or Designated Representative
Information Owner	Yes	Various	Component Head or Designated Representative
Information System Security Managers	Yes (IAM)	Various	PM or SM
Information System Security Officer	Yes (IAO)	Various	PM or SM

“Medically Ready Force...Ready Medical Force”

RMF Major Tasks Matrix Step 1



NAME	MAJOR TASKS	CIO	AO	Primary
Step 1 CATEGORIZE System	1-1 Security Categorization	Supporting	Supporting	ISO, IO, MOs
	1-2 Describe the DHA Information System	N/A	Supporting	ISO
	1-3 Register the DHA Information System	N/A	N/A	ISO, PM/SM

RMF Major Tasks Matrix Step 2



NAME	MAJOR TASKS	CIO	AO	Primary
Step 2 SELECT Controls	2-1 Common Control Identification	Primary	Supporting	CIO, SISO, CCP
	2-2 Security Control Selection	N/A	Supporting	ISO, PM/SM I
	2-3 Monitoring Strategy	Supporting	Supporting	SO, CCP, PM/SM
	2-4 Review and Approve the Security Plan	Supporting	Primary	AO/AODR

RMF Major Tasks Matrix Steps 3 & 4

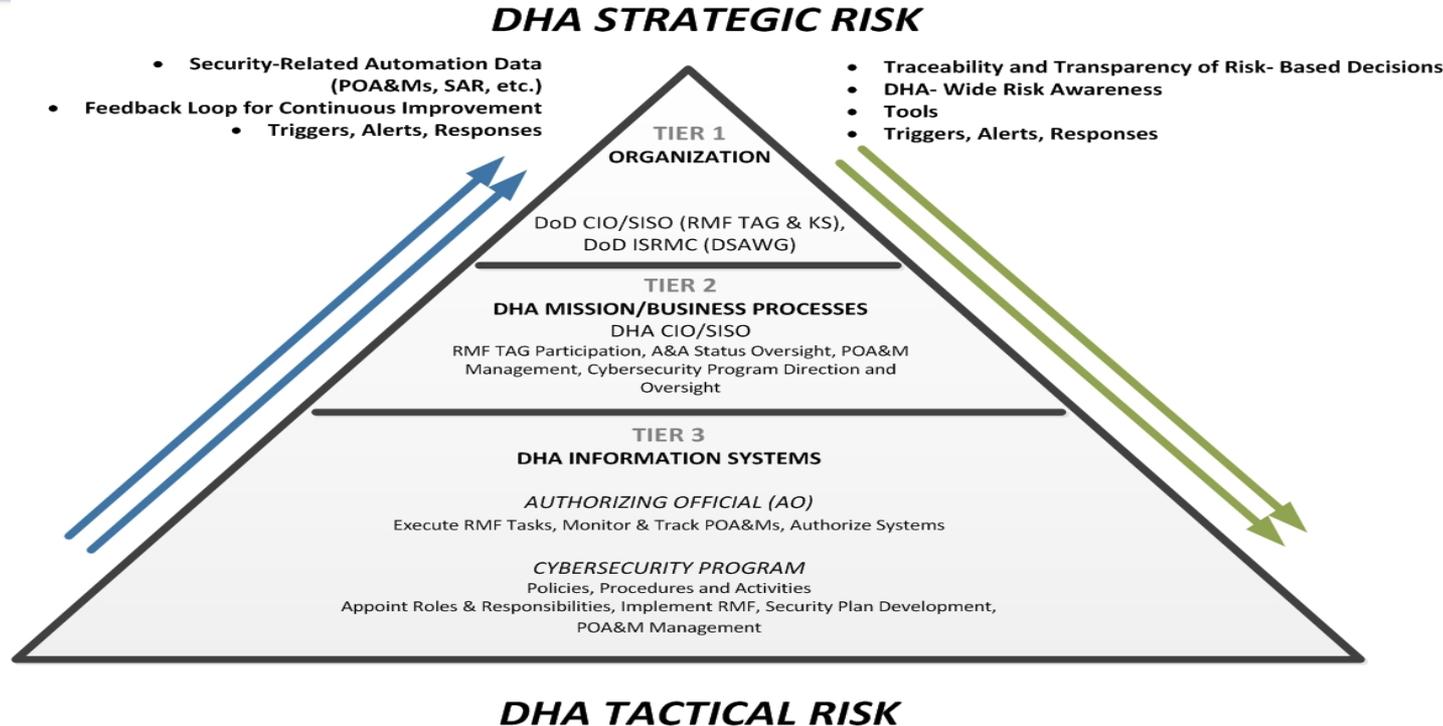


NAME	MAJOR TASKS	CIO	AO	Primary
Step 3 IMPLEMENT Controls	3-1 Implement Security Controls	N/A	N/A	ISO, CCP,PM/SM
	3-2 Document Security Controls	N/A	N/A	ISO. PM/SM
Step 4 ASSESS Controls	4-1 Develop, Review, and Approve Control Assessment Plan	Supporting	Primary	AO/AODR,SCA
	4-2 Assessment Security Controls	N/A	N/A	SCA
	4-3 Prepare Security Assessment Report	N/A	N/A	SCA
	4-4 Conduct Initial Remediation Actions	Supporting	N/A	ISO, PM/SM

RMF Major Tasks Matrix Steps 5 & 6



NAME	MAJOR TASKS	CIO	AO	Primary
Step 5 AUTHORIZE System	5-1 Prepare POA&Ms	N/A	N/A	ISO, PM/SM
	5-2 Assemble Security Authorization Package	N/A	N/A	ISO, ISSM
	5-3 Risk Determination	N/A	Primary	AO/AODR
	5-4 Risk Acceptance	N/A	Primary	AO
Step 6 MONITOR Controls	6-1 Determine Security Impact of System Changes	N/A	Supporting	ISO, ISSM
	6-2 Assess Subset of Security Controls	N/A	Supporting	ISSM
	6-3 Conduct Remediation Actions	N/A	Supporting	ISO, PM/SM
	6-4 Update SSP, SAR, and POA&Ms	N/A	N/A	ISO, PM?SM
	6-5 Report Security Status	N/A	N/A	ISSM
	6-6 Review Reported Security Status	N/A	Primary	AO
	6-7 Implement IS Decommissioning Strategy	N/A	N/A	ISO



Security Control Inheritance



DoD Enterprise, Tier 1

DoD CIO
Policy

DHA Enterprise, Tier 2

DHA Policy

DHA IT, Tier 3

Enclaves

Major
Applications

PIT

“Medically Ready Force...Ready Medical Force”

More RMF Controls than DIACAP Controls



NIST SP 800-53 Rev 4 Baseline

Examples

800-53 controls are written at a more granular level

One DoD legacy control (IAIA-2) may satisfy multiple NIST SP 800-53 Controls + enhancements:

- IA-2 System authenticates users
- IA-4(2) Supervisor approval for password issuance
- IA-5 Password management
- IA-5(7) Password encryption....

800-53 controls implement existing DoD policies and guidance that were not captured within DoD legacy controls

These 800-53 Controls. implement parts of these policies:

- PL-2 System Security Plan
- MP-6 Media Access
- PS-4 Personnel Screening
- PE-6 Physical Access
- PM-4 POA&M Process
- AC-8 System Use Notification
- DoDI 8510 System Implementation Plan
- DoD 5200.1-R Information Security
- DoD 5200.2-R Personnel Security
- 5200.08-R Physical Security
- DoDI 8510 POA&M requirements
- DTM 08-060 Standard Consent and Use Banner

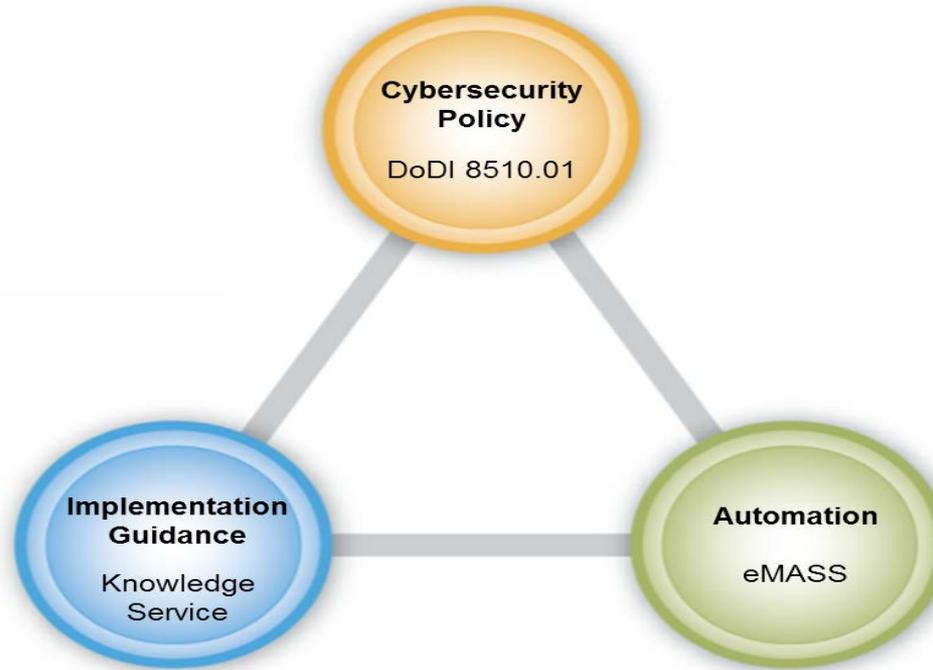
800-53 controls address emerging technologies

800-53 Controls expand upon the following areas:

- Remote Access
- Wireless Access
- Access Control for Mobile Devices
- Continuous Monitoring
- Supply Chain Protection
- Mobile Code

“Medically Ready Force...Ready Medical Force”

Role of eMASS in RMF



“Medically Ready Force...Ready Medical Force”

eMASS Overview



- What is eMASS?
- Stands for Enterprise Mission Assurance Support Service
- Designed to develop, collect, and manage cybersecurity-related data across DoD Organizations focused on requirements of the DoDI 8500.01 and 8510.01
- Owned and centrally managed by DISA Mission Assurance
- Updated every six months
- Currently hosted at the DISA DECC, Columbus, OH
- Resides on both the NIPR and SIPR networks

eMASS RMF Enhancements



eMASS v4.8 & v5.0

- 1) RMF System Registration
- 2) Assess & Validate NIST SP 800-53 Revision 4 Controls (using DoD Rev 4 Assessment Procedures and Enterprise Assignment Values)
- 3) Upload Artifacts & Create POA&M Vulnerabilities
- 4) Generate RMF Package Reports (Security Plan, Security Assessment Report, POA&M, Authorization Decision Document)
- 5) DIACAP to RMF System Migration
- 6) Dual Policy Support (within a single system record)

eMASS Releases (v5.1 & Beyond)

- 1) Risk Assessment Process / Module
- 2) Organizational Assignment Values
- 3) Risk Assessment Report (RAR)
- 4) Digital Signature Process (SAR, ADD)
- 5) Overlays
- 6) DoD Common Controls

“Medically Ready Force...Ready Medical Force”

RMF Security Authorization Package



Component	Notes
1) Security Plan	Generated in eMASS Includes supporting appendices: <ul style="list-style-type: none">• Risk Assessment• Privacy Impact Assessment• System Interconnection Agreements• Contingency Plan• Security Configurations• Configuration Management Plan• Incident Response Plan• Continuous Monitoring Strategy
2) Security Assessment Report (SAR), POA&M, Authorization Decision Document, Risk Assessment Report	Generated in eMASS

“Medically Ready Force...Ready Medical Force”

RMF Transition Tasks



Step	Task
1	Establish RMF IPT Working Group and eMASS Transition Working Group
2	Establish DHA RMF Standard Operating Procedures, Policies, and Templates in alignment with DoD guidance
3	Issue RMF appointment letters
4	DoD CIO RMF briefing
5	Training and orientation for RMF
6	Identify Common Control Providers (CCPs)
7	Categorize systems in accordance with CNSI 1253 and DHA Administrative Instruction 77(draft)
8	Schedule RMF transition kickoff meetings
9	Convert existing DIACAP packages to RMF using eMASS and RMF Knowledge Service guidance
10	Authorize systems under RMF

“Medically Ready Force...Ready Medical Force”

RMF Summary PT 1



- The DoD established and uses an integrated enterprise-wide decision structure for cybersecurity risk management - the Risk Management Framework (RMF) implemented through DoDI 8510.01
- The RMF applies to all DoD/DHA IT that receive, processes, stores, displays, or transmits DoD/DHA information
- The RMF process parallels the system life cycle, with the RMF activities being initiated at program or system inception
- The cybersecurity requirements are managed through the RMF as defined by the RMF Knowledge Service
- All DoD/DHA IS and PIT systems are categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253
- All DoD IS and PIT systems implement a set of security controls as defined by the RMF Knowledge Service

RMF Summary PT 2



- The DoD RMF governance structure implements the three-tiered approach to cybersecurity risk management, and synchronizes and integrates RMF activities
- The system cybersecurity program consists of the policies, procedures, and activities of the ISO, AO/AODR, SCA, PM/SM, ISSM, ISSO at the system level
- Implementation of the RMF is supported and augmented by the RMF KS and eMASS
- The RMF KS provides policy, implementation and validation values, templates, security control selection tools and supporting guidance
- eMASS automates the A&A process, manages workflow among user roles, and generates reports required by the RMF while integrating other cybersecurity services
- Continuous monitoring capabilities will be implemented to the greatest extent possible

RMF Role Acronyms



- Authorizing Official (AO)
- Authorizing Official Designated Representative (AODR)
- Certification Authority (CA)
- Chief Information Officer (CIO)
- Common Control Provider (CCP)
- Designated Approval Authority (DAA)
- Information Owner (IO)
- Information System Owner (ISO)
- Information System Security Manager (ISSM)
- Information System Security Officers (ISSO)
- Mission Owner (MO)
- Program Manager/System Manager (PM/SM)
- Roles and Responsibility (R&R)
- Security Control Assessor (SCA)
- Senior Information Assurance Officer (SIAO)
- Component Senior Information Security Officer (SISO)

RMF Acronyms



- Assessment & Authorization (A&A)
- Assured Compliance Assessment Solution (ACAS)
- Authorization Decision Document (ADD)
- Authorization to Operate (ATO)
- Committee on National Security Systems Instruction (CNSSI)
- Continuous Monitoring Risk Strategy (CMRS)
- Enterprise Mission Assurance Support Service (eMASS)
- Host Based System Security (HBSS)
- Platform Information Technology (PIT)
- Plan of Action and Milestones (POA&M)
- Risk Assessment Report (RAR)
- Risk Management Framework (RMF)
- Security Authorization Package (SAP)
- Security Assessment Report (SAR)
- Security Control Assessments (SCA)
- Security Plan (SP)
- Tactics, Techniques, and Procedures (TTPs)

Other Acronyms



- Defense Enterprise Computing Center (DECC)
- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- Defense Information Systems Agency (DISA)

- Please complete your evaluations

Contact Information



Jeffrey Eyink

Chief, Assessment and Authorization Branch,
Cybersecurity Division

Jeffrey.A.Eyink.civ@mail.mil