

DIACAP to Risk Management Framework (RMF) Transformation

Cybersecurity Policy Directorate



DIACAP to RMF Transformation Background

Evolved into the Joint Task Force (JTF) Transformation Initiative Interagency Working Group (DoD, ODNI, NIST and CNSS), ongoing effort to produce a unified information security framework for the federal government

Used existing NIST Special Publications as basis for developing Joint Transformation core documents

DIACAP

JTF

Revised 8500 Series

Began as the Intelligence Community (IC) Transformation effort to standardize Certification and Accreditation (C&A) in the IC and to address reciprocity with DoD

DoD is currently revising
DoDD 8500.01, DoDI 8500.02, and DoDI 8510.01
to align with NIST Joint Task Force documents

Transition Bottom Line – DoD will continue to follow the DoD 8500 series documentation for information assurance and risk management processes, procedures, and guidance





Transformation benefits the entire enterprise

	Benefits						
CIOs	 Standardize IA language across the Federal government Efficient enterprise management of IA Potential cost savings by supporting tighter integration of security into the systems development life cycle and acquisition processes Compliance with FISMA review and reporting requirements 						
Warfighters	 More rapid deployment of solutions Significant improvement in interoperability because information is visible, available, and usable Greater assurance that systems are secure Enhanced compatibility with intelligence community IA processes 						
Business System Owners	 More consistent and assured protection of individual privacy and the data supporting DoD business operations More efficient and effective delivery of services due to globally accessible business information 						
System Developers	 Increased coordination and integration of security into the systems development and acquisition processes Standardized IA requirements and validation procedures Dynamic controls allow for better risk management 						





Cybersecurity Policy Development Partnerships

DoD
participates in
development
of CNSS and
NIST
documents
ensuring DoD
equities are
met

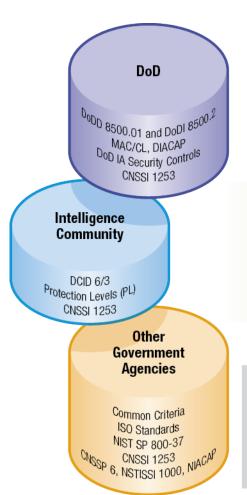


DoD leverages
CNSS and NIST
policies and
filters
requirements
to meet DoD
needs

DoD participates in CNSS and NIST policy development as a vested stakeholder with the goals of a more synchronized cybersecurity landscape and to protect the unique requirements of DoD Missions and warfighters



DoD is transforming IA policies and practices to align with Federal government risk management policies and practices



Joint Task Force Transformation Initiative

DoD is aligning IA and risk management policies, procedures, and guidance with Joint Transformation NIST documents, the basis for a unified information security framework for the Federal government.







DoD is transforming IA policies and practices to improve IT categorization and control selection, and risk management procedures

Current versions of DoDD 8500.01, DoDI 8500.2, and DoDI 8510.01

Mission Assurance Category (MAC) / Confidentiality Level (CL)

IS Definitions

DoD Defined Security Controls

C&A Process

Draft revisions of DoDD 8500.01, DoDI 8500.02, and DoDI 8510.01

Impact Value: Low / Moderate / High Security Objectives: Confidentiality / Integrity / Availability

Expanded IT definition to align with CNSSI 4009 and encompass new and emerging capabilities

Using NIST SP 800-53 Security Control Catalogue.
Creating DoD Assignment Values, validation procedures, and implementation guidance.

Risk Management Framework includes processes to further mitigate and remediate risk to systems

Joint Task Force Transformation Initiative



Joint Task Force Transformation Goals

Transformation Goals

- Define a common set of trust (impact) levels and adopt and apply them using CNSSI 1253 across the Intelligence Community (IC), DoD, and other organizations that have National Security Systems (NSS). Organizations will no longer use different levels with different names based on different criteria.
- 2. Adopt **reciprocity** as the norm, enabling organizations to accept the approvals by others without retesting.
- 3. Define, document, and adopt **common security controls**, using NIST Special Publication (SP) 800-53 as a baseline.
- 4. Adopt a **common lexicon**, using CNSS Instruction 4009 as a baseline thereby providing DoD and IC a common language and common understanding.
- 5. Institute a **senior risk executive function**, which bases decisions on an "enterprise" view of risk considering all factors, including mission, IT, budget, and security.
- 6. Incorporate **information assurance (IA) into Enterprise Architectures** and deliver IA as common enterprise services across the IC, DoD, and other organizations that have NSS.
- 7. Enable a common process that incorporates security within the "lifecycle" processes and eliminate security-specific processes. The common process will be adaptable to various development environments.





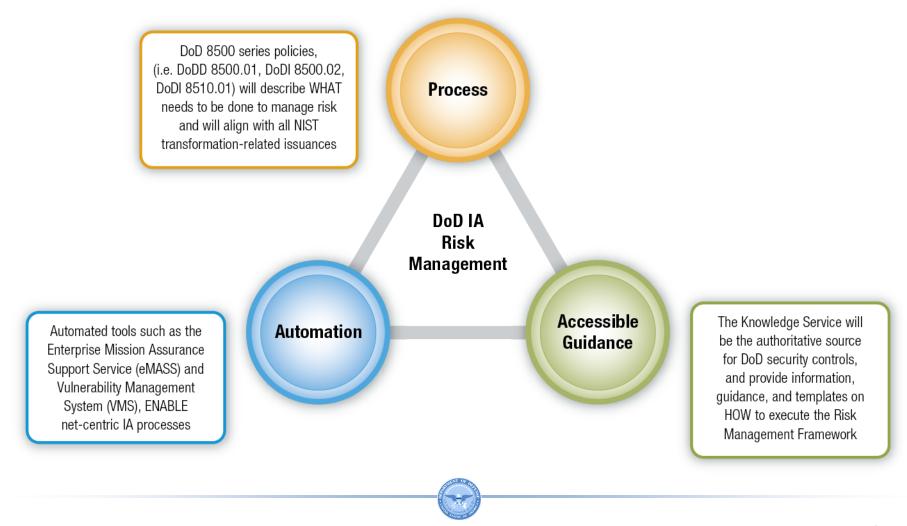
DoD supports implementation of Joint Transformation Goals

Goal	Implementation
1	Moving from Mission Assurance Category levels (MAC I, II, III), and Classification Level (Classified, Sensitive, Public), to Impact Values (Low/Moderate/High) and Security Objectives (Confidentiality, Integrity, Availability). Synchronizes DoD Impact Values with NIST recommendations and Intelligence Community practices. Implemented through DoDI 8500.02 and CNSSI 1253.
2	Reciprocity will be addressed by DoDI 8510.01.
3	DoD will use NIST SP 800-53 security control catalog with DoD specific assignment values, implementation guidance, and validation procedures. DoD security control categorization and control selection processes are synchronized with NIST recommendations and Intelligence Community practices. Directed by DoDI 8500.02 to be implemented on the Knowledge Service.
4	Incorporate new IT structure and other new Risk Management Framework terms into CNSSI 4009, and continue its use as the official glossary for the DoD 8500 series.
5	Continue DoD enterprise governance structure and strengthen interfaces to IC enterprise governance. Implemented through DoDI 8500.02 and DoDI 8510.01.
6	Continue co-evolution of security control categorization and selection, Risk Management Framework, IA Component of GIG Integrated Architecture, Alignment Framework for GIG IA and other supporting elements of the GIG Technical Framework, and GIG IA Portfolio.
7	Incorporate transformation concepts into DoD policies; adapt new concepts via enterprise governance structure and promulgate via Knowledge Service. Continue to influence GIG IA Portfolio for configuration management, automated monitoring, other enablers.



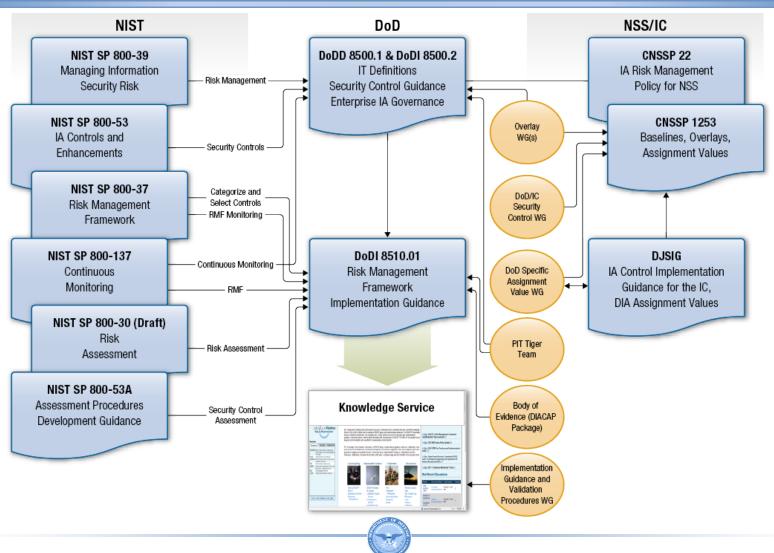


Successful execution of RMF Transformation is enabled through three inter-related DoD CIO initiatives





Policy Interdependencies





Why are there more NIST SP 800-53 controls than the legacy DoD controls?

NIST SP 800-53 CONTROLS

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

- 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

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

- 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





Categorization and Security Control Selection Process (Steps 1 and 2 of the Risk Management Framework)





Select Baseline Security Controls



Apply Overlay(s)



Tailor If Required

Determine impact values for each of the security objectives per CNSSI 1253

- Assign an impact value for each of the security objectives of Confidentiality, Integrity, and Availability (C, I, & A).
- Z Low: Limited adverse effect
- Moderate: Serious adverse effect
- → High: Severe or catastrophic adverse effect

Determine the need for and apply overlays

- Allow for uniform modifications to the baseline control set by adding or subtracting controls.
- Based on such factors as information type, mission area, location, etc.
- Examples: Health information (HIPAA), tactical systems, privacy (PII), etc.
- Overlays will reside on the CNSS Portal and will be linked from the Knowledge Service.

Select baseline controls from Table D-1 of CNSSI 1253

			Confidentiality			Integrity			Availability		
ID	Title	L	М	Н	L	М	Н	L	М	Н	
AC-1	Access Control Policy and Procedures	Х	Х	Х	X	Х	Χ	X	Х	Χ	
AC-9	Previous Logon (Access) Notification					Х	Х				
CP-7	Alternate Processing Site								Х	Χ	

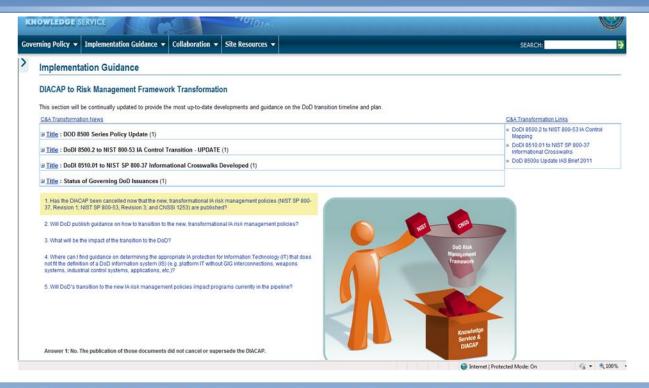
Further tailor and supplement depending on particular circumstances

- Controls will not be removed for convenience.
- 7 Tailoring decisions based on operational considerations and the environment of the information system.
- Rationale for tailoring and any compensating controls must be documented in the security plan.





The Knowledge Service is an authoritative source for DoD Transformation policy and guidance

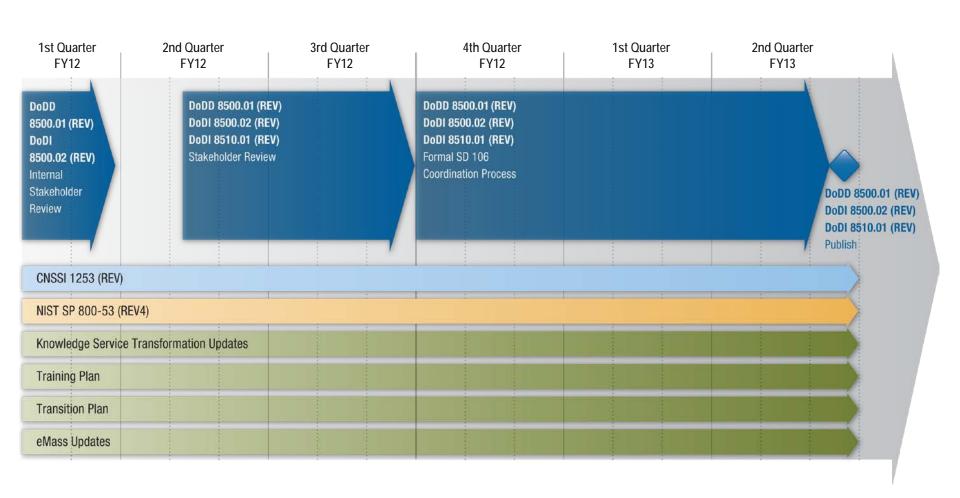


- Will maintain official policy, guidelines, and templates to facilitate the execution of the RMF to include security control categorization and control selection
- Manages, standardizes, and makes available the DoD RMF body of knowledge
- Enables DoD Components to augment the enterprise body of knowledge
- · Supports user community collaboration for solving problems through discussion boards, alerts, and news lists





WicktansfeithMasteritielmetyle





The Enterprise Mission Assurance Support Service (eMASS) is supporting DoD's RMF Transformation

eMASS is helping DoD to achieve the transition to IA Risk Management

- eMASS will support the transition from legacy DoD IA controls to the NIST SP 800-53 Control Catalog
- eMASS will also automate processes and business rules defined in the RMF
- 3. Working closely with DoD IA working groups, eMASS will continue to support reciprocity, process automation, reduced cost, and provide leaders with enterprise-level visibility into IA activities to improve security postures
- As DoD's recommended enterprise automated RMF service, eMASS allows organizations to offset cost and focus resources towards tactical operation and computer network defense activities



To become part of the DoD RMF community of interest, visit the online Knowledge Service:

https://diacap.iaportal.navy.mil *

* Access requires a DoD PKI certificate or an ECA PKI certificate

