

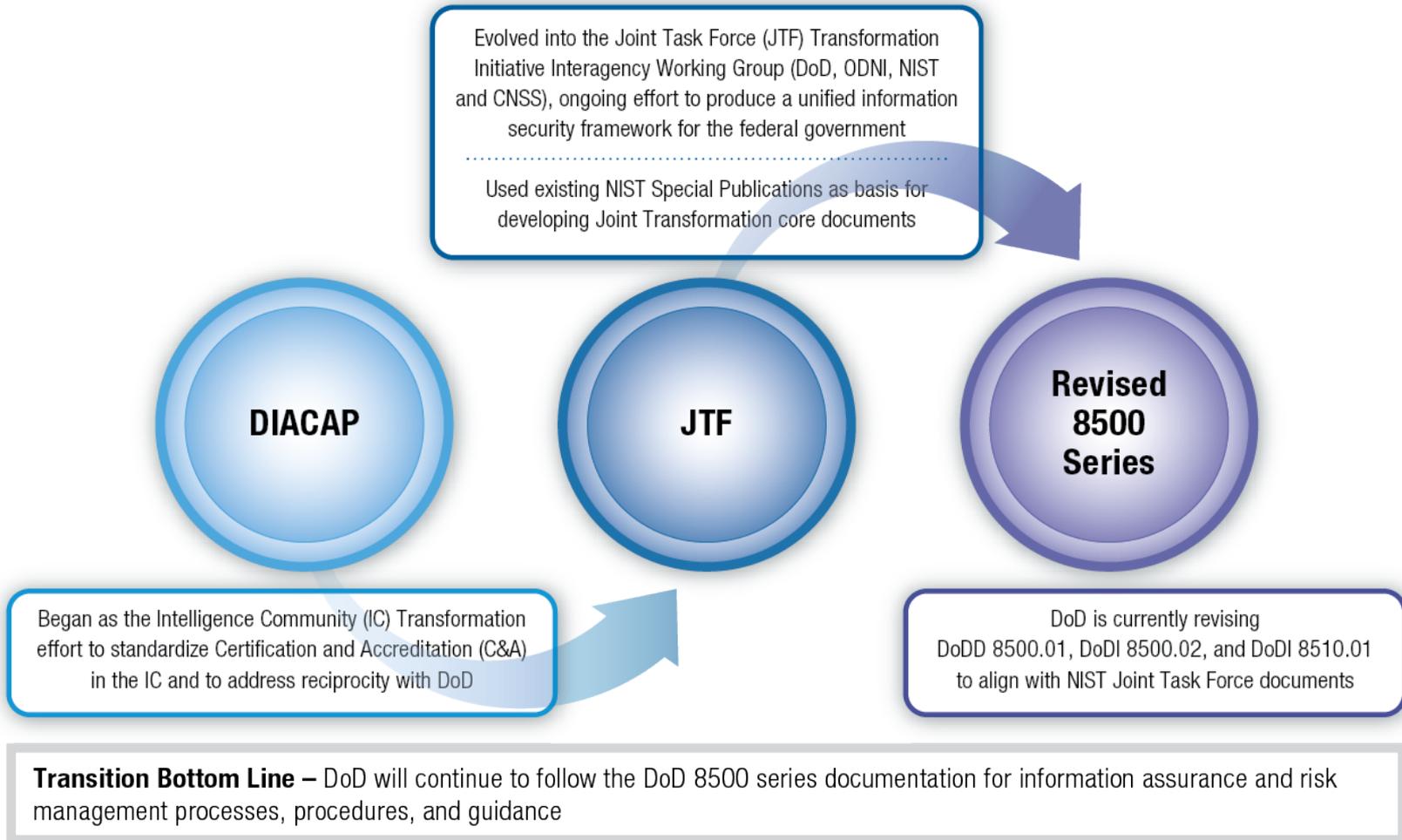


DIACAP to Risk Management Framework (RMF) Transformation

Cybersecurity Policy Directorate



DIACAP to RMF Transformation Background





Transformation benefits the entire enterprise

	Benefits
CIOs	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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





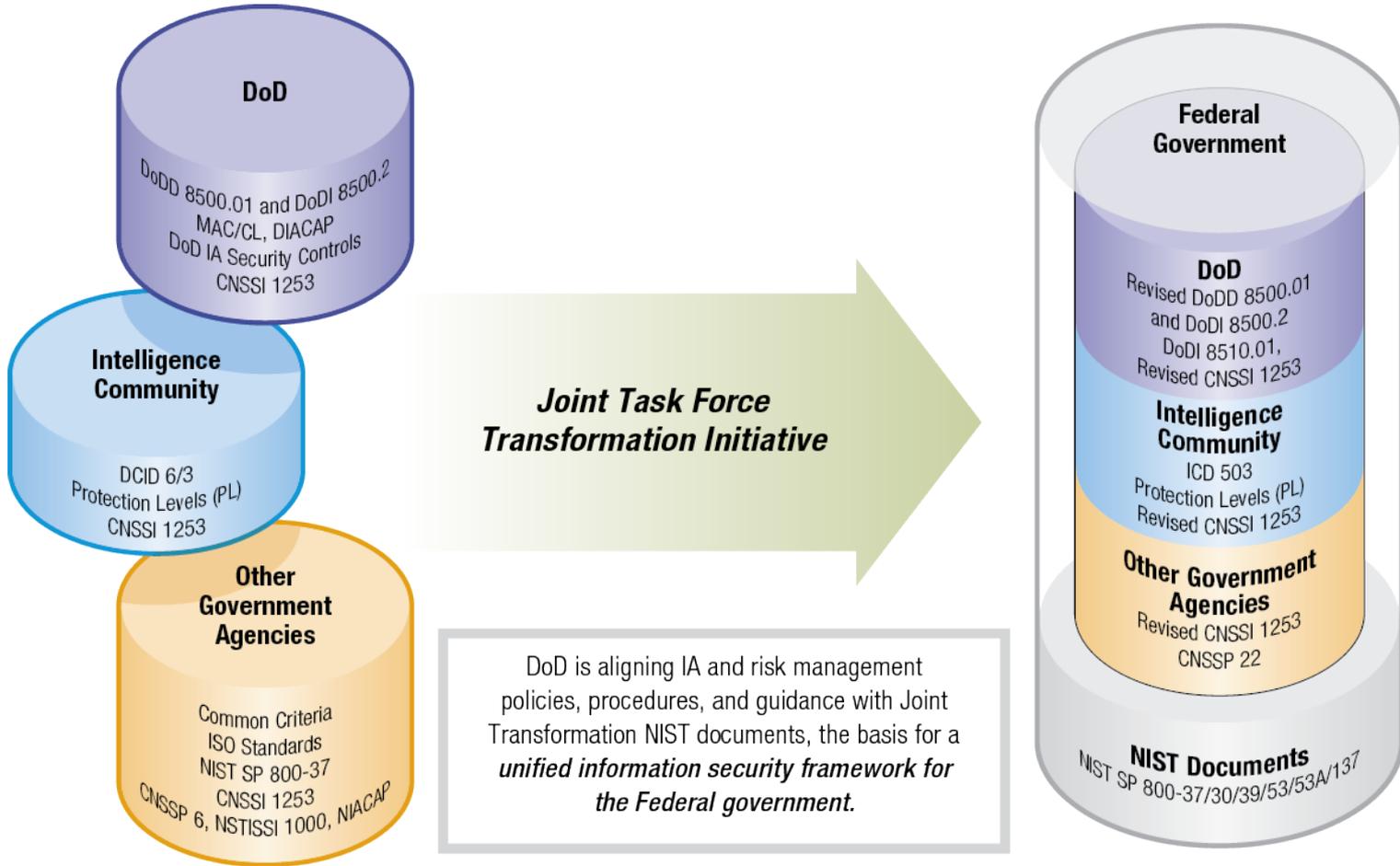
Cybersecurity Policy Development Partnerships



DoD participates in 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

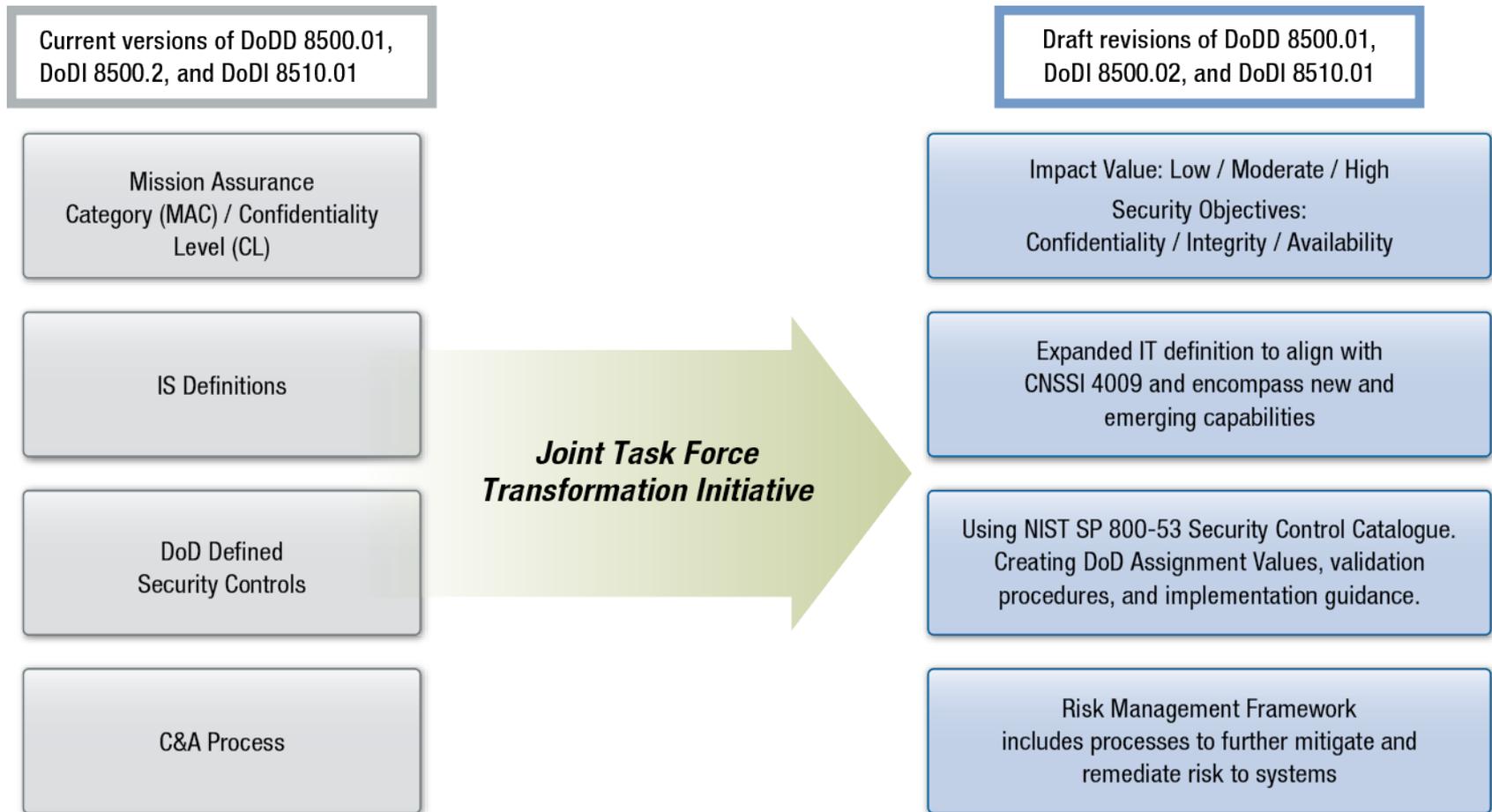


DoD is transforming IA policies and practices to align with Federal government risk management policies and practices





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





Joint Task Force Transformation Goals

Transformation Goals

1. 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.





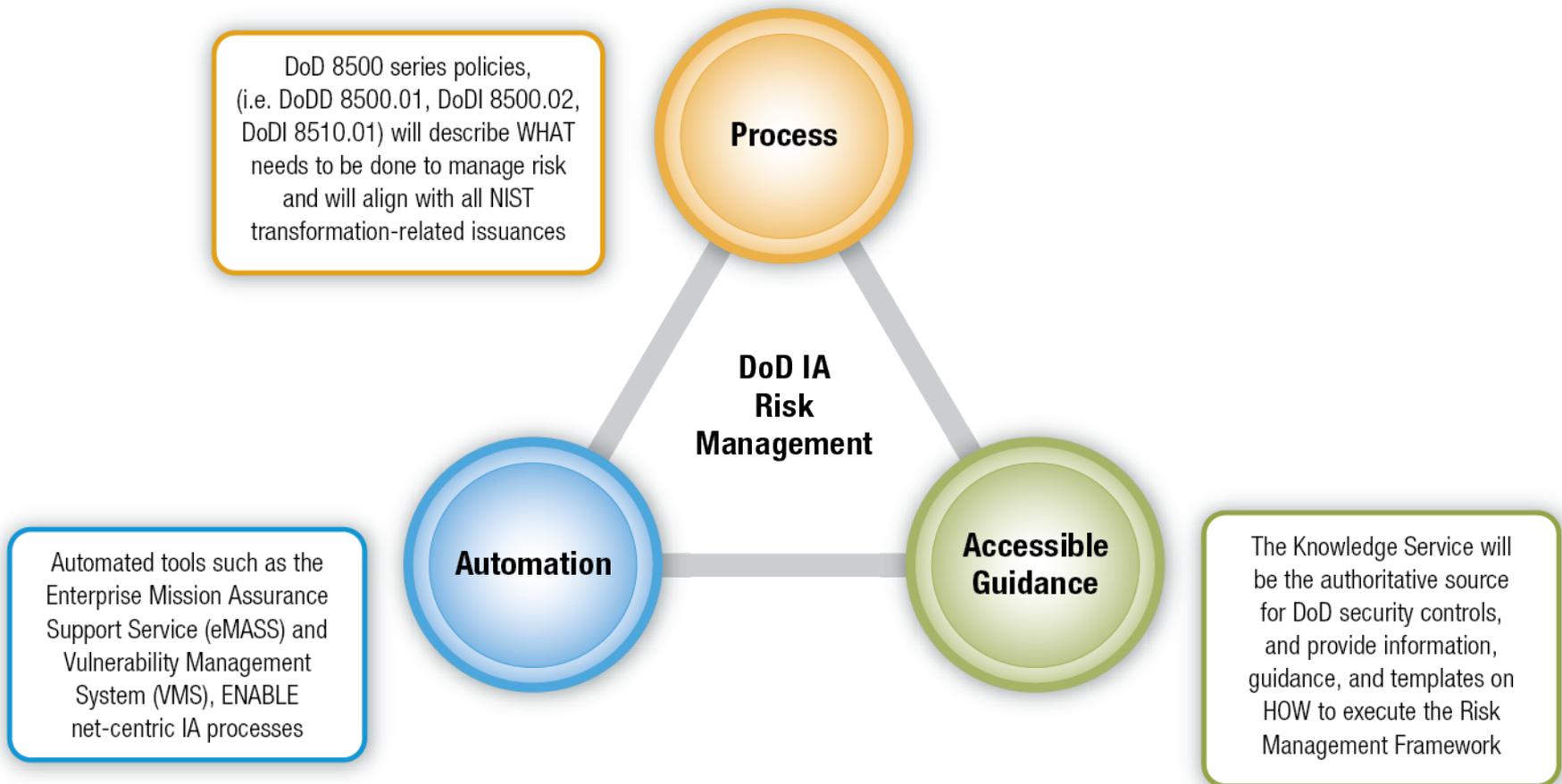
DoD supports implementation of Joint Transformation Goals

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.



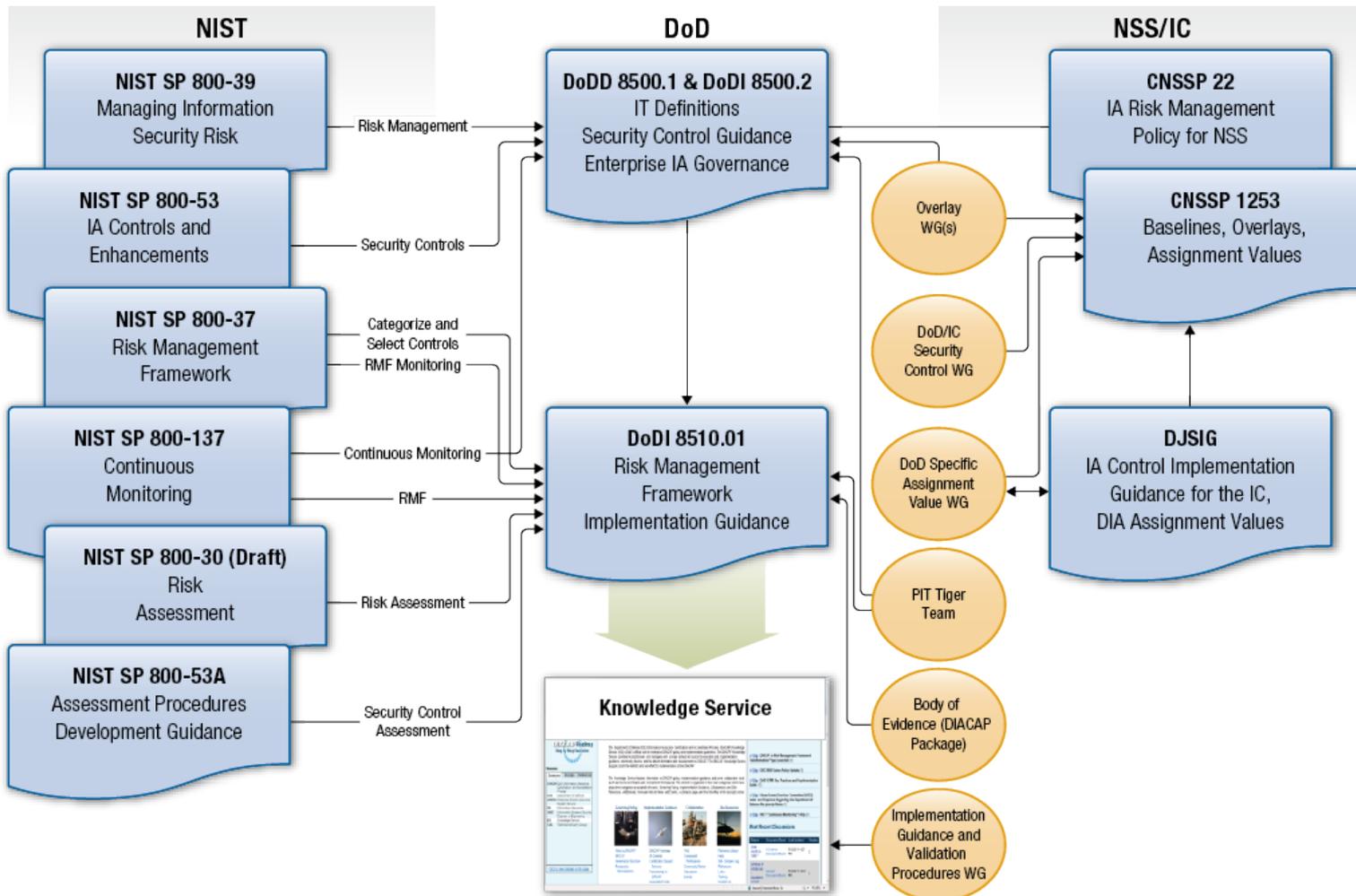


Successful execution of RMF Transformation is enabled through three inter-related DoD CIO initiatives





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

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

- | | |
|--|---|
| <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 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)



1 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).
- Low: Limited adverse effect
- Moderate: Serious adverse effect
- High: Severe or catastrophic adverse effect

3 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.

2 Select baseline controls from Table D-1 of CNSSI 1253

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

4 Further tailor and supplement depending on particular circumstances

- Controls will not be removed for convenience.
- 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

KNOWLEDGE SERVICE

Governing Policy ▾ Implementation Guidance ▾ Collaboration ▾ Site Resources ▾

SEARCH:

Implementation Guidance

DIACAP to Risk Management Framework Transformation

This section will be continually updated to provide the most up-to-date developments and guidance on the DoD transition timeline and plan.

[C&A Transformation News](#)

- [Title : DOD 8500 Series Policy Update \(1\)](#)
- [Title : DoDI 8500.2 to NIST 800-53 IA Control Transition - UPDATE \(1\)](#)
- [Title : DoDI 8510.01 to NIST SP 800-37 Informational Crosswalks Developed \(1\)](#)
- [Title : Status of Governing DoD Issuances \(1\)](#)

[C&A Transformation Links](#)

- DoDI 8500 2 to NIST 800-53 IA Control Mapping
- DoDI 8510 01 to NIST SP 800-37 Informational Crosswalks
- DoD 8500s Update IAS Brief 2011

1. Has the DIACAP been cancelled now that the new, transformational IA risk management policies (NIST SP 800-37, Revision 1; NIST SP 800-53, Revision 3; and CNSSI 1253) are published?

2. Will DoD publish guidance on how to transition to the new, transformational IA risk management policies?

3. What will be the impact of the transition to the DoD?

4. Where can I find guidance on determining the appropriate IA protection for Information Technology (IT) that does not fit the definition of a DoD information system (IS) (e.g. platform IT without GIG interconnections, weapons systems, industrial control systems, applications, etc.)?

5. Will DoD's transition to the new IA risk management policies impact programs currently in the pipeline?

Answer 1: No. The publication of those documents did not cancel or supersede the DIACAP.

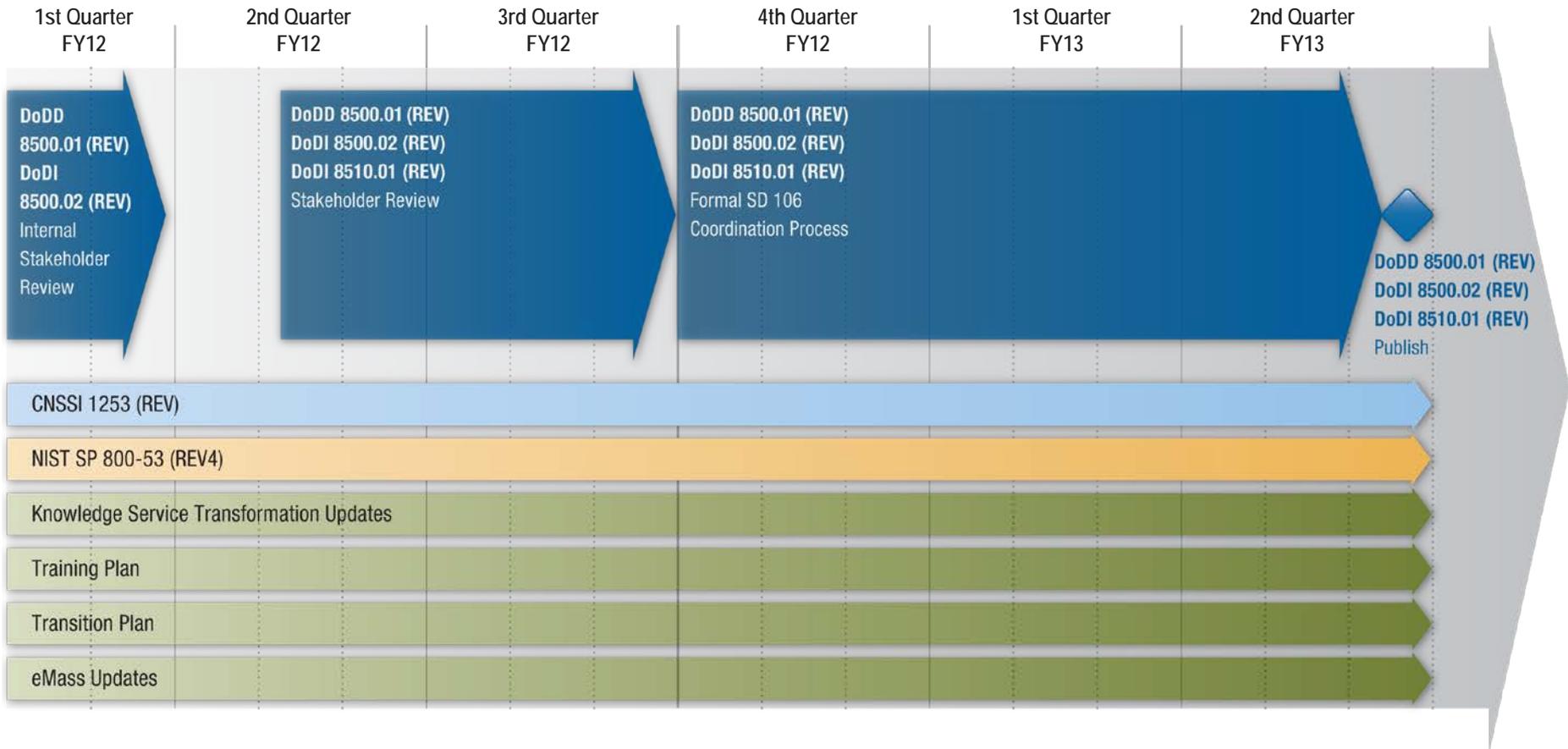
Internet | Protected Mode: On 100%

- 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





Click to edit Master title style





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

1. eMASS will support the transition from legacy DoD IA controls to the NIST SP 800-53 Control Catalog
2. 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
4. 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





Contact Information

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

<https://diacap.iportal.navy.mil> *

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

