

Cybersecurity Throughout DoD Acquisition



Foundational Learning



Workflow Learning



Performance Learning

July 2015

Tim Denman

Cybersecurity Performance Learning Director
DAU – Learning Capabilities Integration Center

Tim.Denman@dau.mil

Acquisition.cybersecurity@dau.mil

- **Current State of Cybersecurity in the DoD**

- DoD Cyber Strategy
- Communications and Cybersecurity

- **Cybersecurity – A Team Sport**

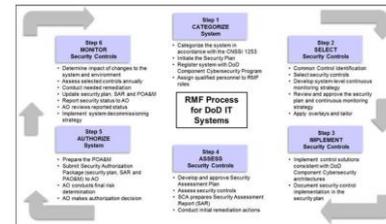
- Leadership/ Program Management
- Logistics
- Contracts
- Engineering
- Test and Evaluation (T&E)

- **Risk Management Framework**

- Concepts
- Process
- Transition

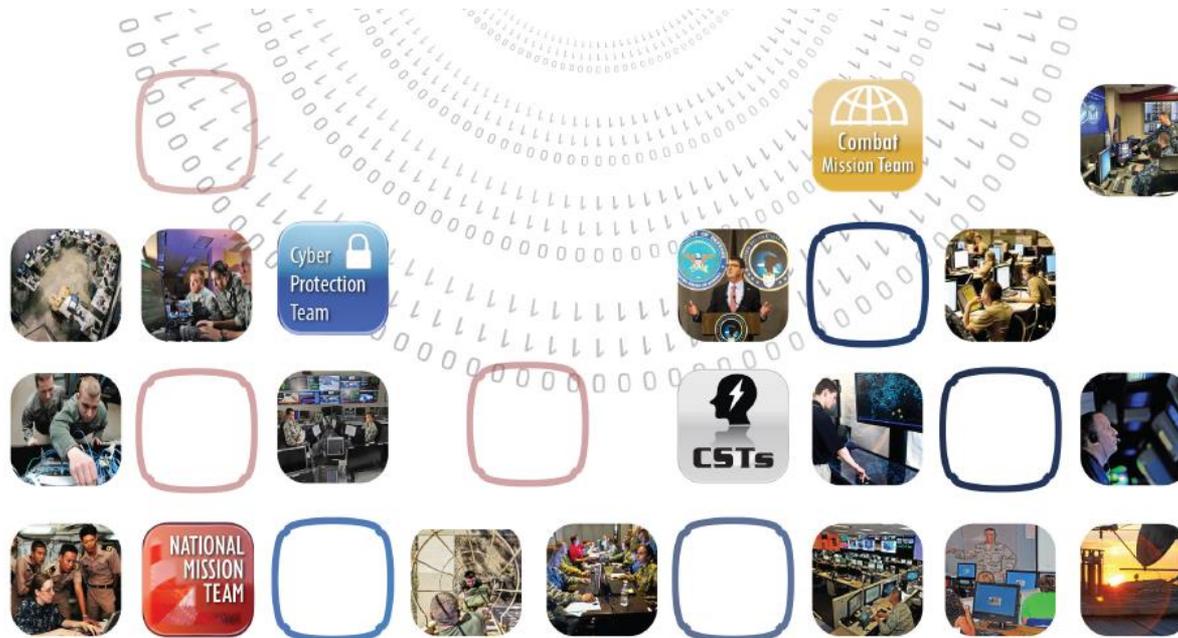
- **DAU and Cybersecurity**

THE DOD CYBER STRATEGY





The DoD Cyber Strategy (April 2015)



THE DEPARTMENT OF DEFENSE



Five Strategic Goals for DoD Cyberspace Missions

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

For DoD to succeed in its mission of defending the United States and its interests in cyberspace, leaders from across the Department must take action to achieve the objectives outlined in this document. They must also hold their organizations accountable.



DoD Communications

What has changed in the last 8 years?





Cybersecurity – A Team Sport

Who should be involved and how?

TEST AND EVALUATION

IT Professional

Cybersecurity Professional

**Configuration
Management**

Contracts

Program Manager

Architecture

Logistics and Purchasing

**Requirements
Engineers**

PRODUCTION AND QUALITY

Others

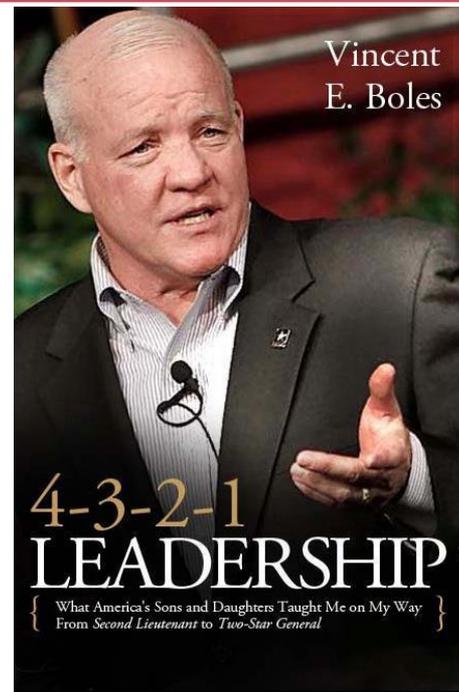
Cybersecurity in the DoD acquisition workforce requires vigilance from everyone who communicates information digitally. It is a true team sport that affects everyone's job and it is the responsibility of the entire DoD workforce.



Leadership and Cybersecurity Professionals

- Leadership must lead the way
 - Be accountable and hold others accountable
 - Understand and prioritize cybersecurity
 - Involve cybersecurity professionals throughout the acquisition process
- Cybersecurity professionals must lead
 - Educate and communicate
 - Work as a team to enable cybersecurity and IT
- PMs, under the supervision of Program Executive Officer (PEOs) and Component Acquisition Executives (CAEs), are expected to:
 - Design acquisition programs
 - Prepare programs for decisions
 - Execute approved program plans

PM - The individual with responsibility and accountability for the implementation of DoD security requirements IAW DoDI 8500.01



“The most critical component in any organization is trust.”
Vinny Boles, 4-3-2-1 Leadership



Cybersecurity Implementation into Acquisition Programs – 3 Sub-processes

- **Requirements Generation**
 - The PM team and requirements developers must be cognizant of the mandatory System Survivability KPP, which includes cyber survivability requirements.
 - PMs will need to deliver systems that are able to operate and complete their missions in a cyber-contested environment.
- **Acquisition and Program Management**
 - PMs must address cybersecurity in program reviews, including Deep Dives, In-Process Reviews, and Overarching Integrated Product Team (OIPT) meetings
 - The PM needs to build an IPT structure that includes cybersecurity expertise.
- **Systems Engineering and Test and Evaluation**
 - Implementation of a disciplined systems engineering process that includes cybersecurity is required from requirements analysis through design, test and evaluation, fielding, sustainment, and decommissioning.
 - The PM must develop a cybersecurity Test and Evaluation (T&E) strategy, allocate resources for cybersecurity T&E, and ensure they are described in the TEMP.

- The Chinese government has adopted new regulations requiring companies that sell computer equipment to Chinese banks to turn over secret source code, submit to invasive audits and build so-called back doors into hardware and software
- In 2013 a Defense Science Board report [accused](#) China of using cyber attacks to access information from almost 40 Pentagon weapons programs

Contractors may be removed from information technology procurements supporting national security systems for failure to satisfy standards related to supply chain risk, and in some cases they will be unable to protest their removal. DoD rules governing Information Relating to Supply Chain Risk, 78 Fed. Register 69,268 (Nov. 18, 2013), NDAA Section 806

The New York Times

Wednesday, January 28, 2015 | Today's Paper | Video | 33°F | Dow -1.13%

New Rules in China Upset Western Tech Companies

By PAUL MOZUR JAN. 28, 2015

HONG KONG — The Chinese government has adopted new regulations requiring companies that sell computer equipment to Chinese banks to turn over secret source code, submit to invasive audits and build so-called back doors into hardware and software, according to a copy of the rules obtained by foreign technology companies that do billions of dollars' worth of business in China.

Supply Chain Risk -the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.



SCRM Sample Contract Language (Section C)

- **[SOWxxx4]** The contractor shall demonstrate that the contractor has mechanisms in place to effectively monitor the supply chain for critical components, understands how supply chain risk can be introduced through those components, and has implemented or plans to implement countermeasures to mitigate such risks.
- **[SOWxxx5]** The contractor shall plan for and implement countermeasures that mitigate the risk of foreign intelligence or foreign influence, technology exploitation, supply chain and battlefield threats, and vulnerabilities that result in Level I and Level II protection failures of the system; countermeasures include the following:
 1. The application of supply chain risk management best practices, ...
 2. The enumeration of potential suppliers of critical components, as they are identified, ...
- **[SOWxxx7]** The contractor shall ensure that updated assumptions, rationale, and results related to the criticality analyses, vulnerability assessments, risk assessments, supply chain risk information, and risk mitigations are made available for Government review at each Systems Engineering Technical Review (SETR).



From “Suggested SSE Language for TSN in DoD RFPs”, Jan 2014

Software Assurance (SwA)- *the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the life cycle.* CNSS Instruction 4009 “National Information Assurance Glossary”, Apr 26, 2010



The key to gaining assurance about your software is to make incremental improvements when you develop it, when you buy it, and when others create it for you. No single remedy will absolve or mitigate all of the weaknesses in your software, or the risk. However, by blending several different methods, tools, and change in culture, one can obtain greater confidence that the important functions of the software will be there when they are needed and the worst types of failures and impacts can be avoided.

<http://cwe.mitre.org/index.html>



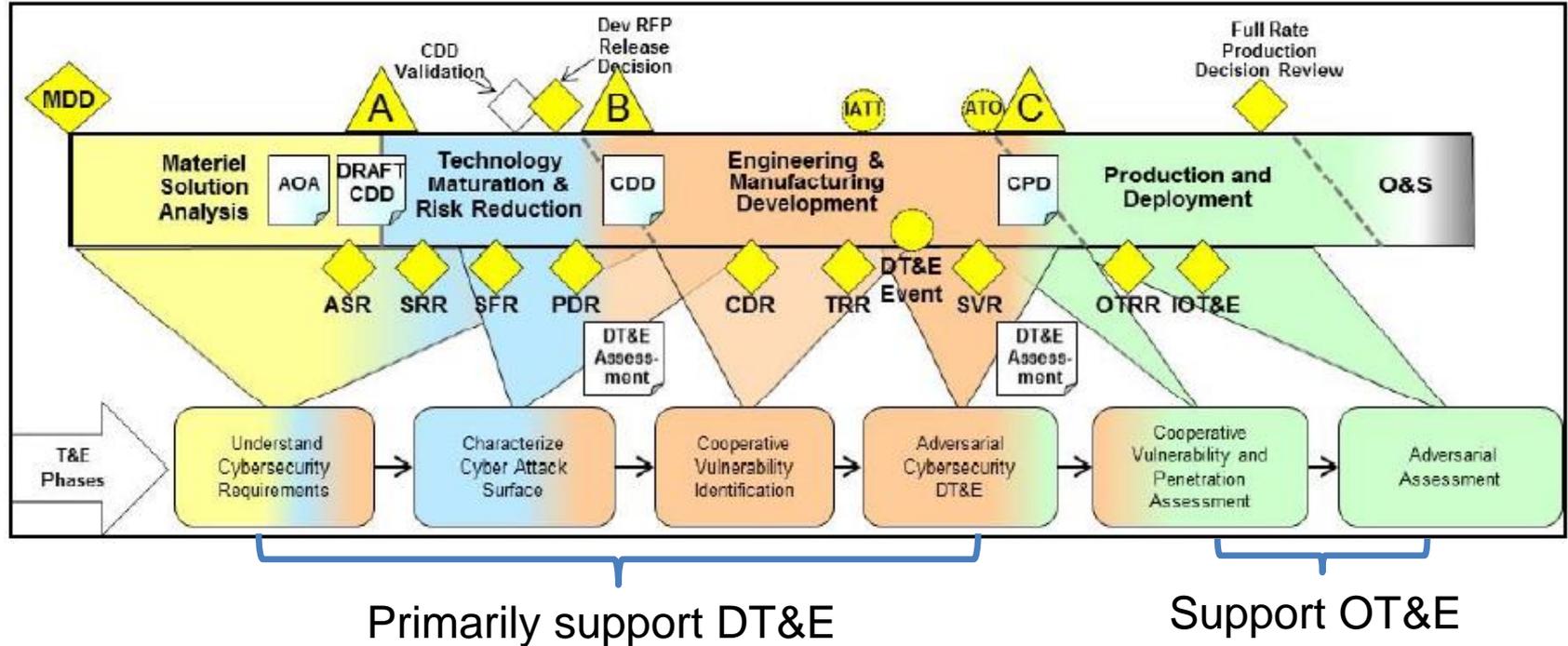
Common Weakness Enumeration

A Community-Developed Dictionary of Software Weakness Types



Cybersecurity T&E Phases and the Acquisition Life Cycle

Cybersecurity T&E phases are Iterative - Activities may be repeated several times due to changes in the system architecture, new or emerging threats, and changes to the system environment.



DoDI 5000.02 clearly provides direction to integrate cybersecurity T&E early and continuously in the acquisition life cycle.



T&E Phases

Cybersecurity Test and Evaluation Guidebook, July 1, 2015

D
T
&
E

O
T
&
E

Phase	Purpose
Understand Cybersecurity Requirements	Understand the program's cybersecurity requirements and develop an initial approach and plan for conducting cybersecurity T&E.
Characterize the Cyber-Attack Surface	Identify the opportunities an attacker may use to exploit the system in order to plan testing that evaluates whether those opportunities continue to allow exploitation.
Cooperative Vulnerability Identification	Identify vulnerabilities that may be fed back to systems designers, developers, and engineers so that mitigations can be implemented to improve resilience.
Adversarial Cybersecurity DT&E	Discover critical vulnerabilities and determine their impacts.
Cooperative Vulnerability & Penetration Assessment	Provide a comprehensive characterization of the cybersecurity status of a system in a fully operational context, and to substitute for reconnaissance activities in support of adversarial testing.
Adversarial Assessment	Attempt to induce mission effects by exploiting vulnerabilities to support evaluation of operational mission risks.



Cybersecurity Defined

Information Assurance (IA) - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Department of Defense Directive (DoDD) 8500.01E, April 23, 2007

Cybersecurity - Prevention of damage to, protection of, and restoration of computers, electronic **communications systems**, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its **availability, integrity, authentication, confidentiality, and nonrepudiation.**

Department of Defense Instruction (DoDI) 8500.01, March 14, 2014

DoDI 8500.01 adopts the term “cybersecurity” to be used throughout the DoD instead of the term “information assurance (IA).”

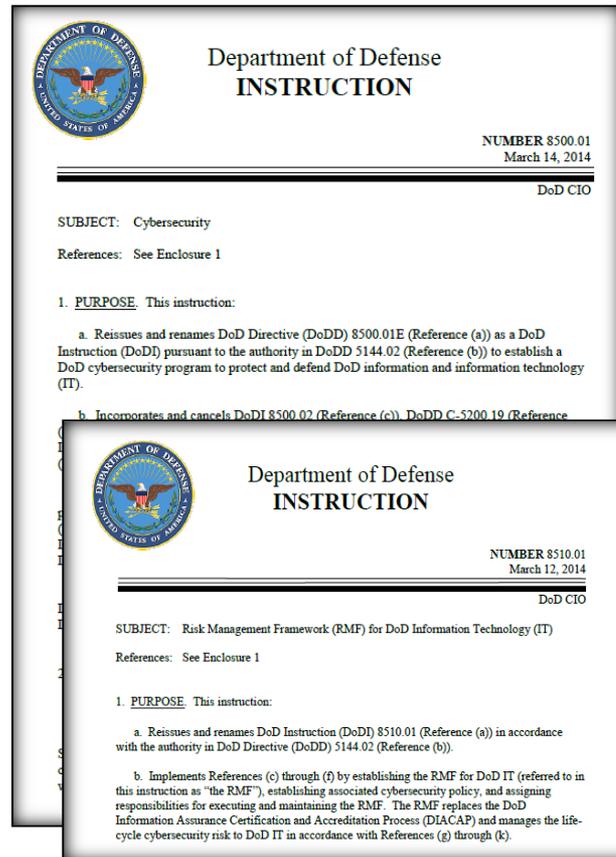


DoD Risk Management Framework (RMF) Policy

- DoD Instruction 8500.01
 - Cybersecurity
 - Signed March 14, 2014
- DoD Instruction 8510.01
 - Risk Management Framework (RMF) for DoD Information Technology (IT)
 - Signed March 12, 2014

Cybersecurity RMF steps and activities, as described in DoD Instruction 8510.01, should be initiated as early as possible and fully integrated into the DoD acquisition process including requirements management, systems engineering, and test and evaluation.

DoDI 5000.02, January 7, 2015



- **NIST Special Publications (SP)**

- 800-37 – Guide for Applying the RMF
- 800-39 – Managing Information Security Risks
- 800-53 – Security and Privacy Controls
- 800-53A - Guide for Assessing the Security Controls
- 800-60 – Guide for Mapping Types of Information and Information Systems to Security Categories
- 800-137 – Information Security Continuous Monitoring



- **Committee on National Security Systems (CNSS)**

- Instruction 1253 - Security Categorization and Control Selection for National Security Systems
- Instruction 4009 – Information Assurance Glossary
- Policy 11 - National Policy Governing the Acquisition of IA and IA-Enabled IT Products

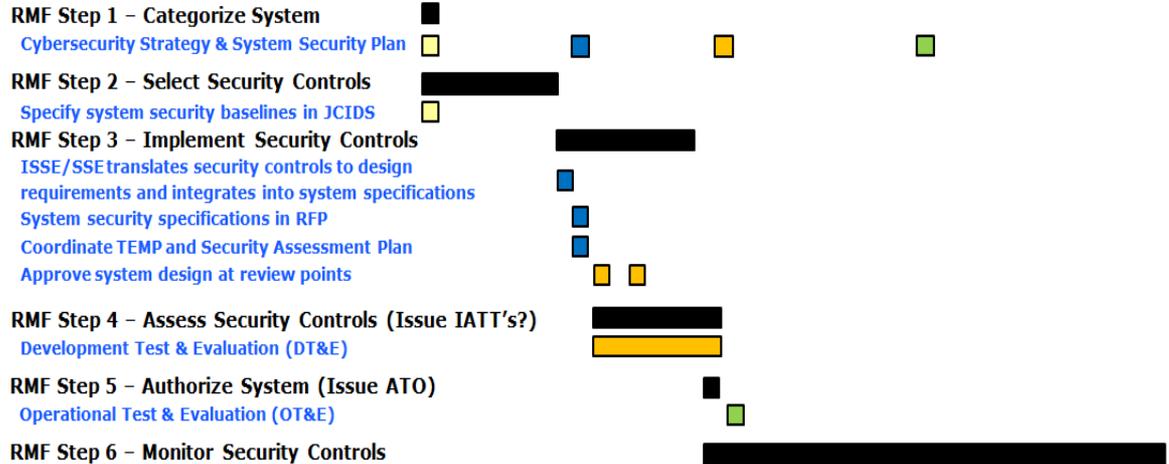
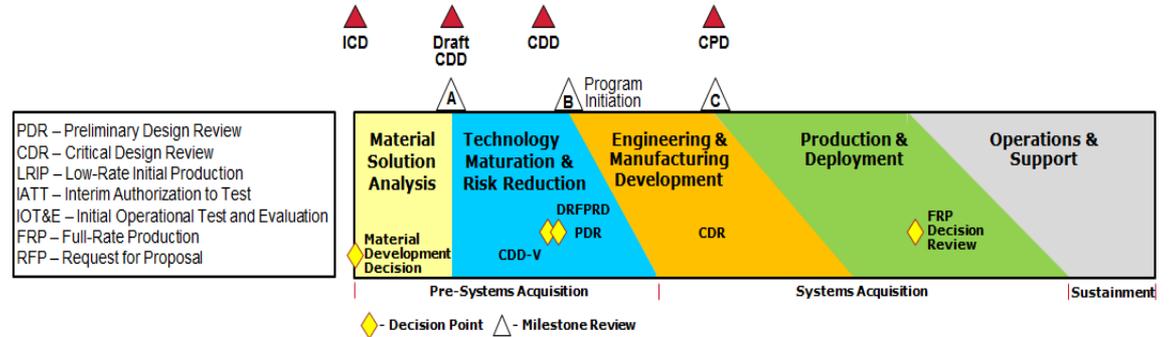


DoD participates in CNSS and NIST policy development as a vested stakeholder with the goals of a more synchronized cybersecurity landscape and to protect the unique requirements of DoD Missions and warfighters



RMF and the Acquisition Life Cycle

Cybersecurity requirements must be identified and included throughout the lifecycle of systems to include acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement of all DoD IT supporting DoD tasks and missions.





RMF - Operational Resilience, Integration, and Interoperability

Operational Resilience

1. Information and computing services are available to authorized users whenever and wherever needed
2. Security posture is sensed, correlated, and made visible to mission owners, network operators, and to the DoD Information Enterprise
3. Hardware and software have the ability to reconfigure, optimize, self-defend, and recover with little or no human intervention

Integration and Interoperability

1. Cybersecurity must be fully integrated into system life cycles and will be a visible element of IT portfolios.
2. Interoperability will be achieved through adherence to DoD architecture principles
3. All interconnections of DoD IT will be managed to minimize shared risk



- Definition: Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.
- If applied appropriately, reciprocity will reduce:
 - Redundant testing
 - Redundant assessment and documentation
 - Overall costs in time and resources



Information System Continuous Monitoring - maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

- Continuous monitoring capabilities will be implemented to the greatest extent possible.





- Security controls are the safeguards/countermeasures prescribed for information systems or organizations that are designed to:
 - Protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and
 - Satisfy a set of defined security requirements
- Key questions
 - What security controls are needed to satisfy the security requirements and to adequately mitigate risk incurred by using information and information systems in the execution of organizational missions and business functions?
 - Have the security controls been implemented, or is there an implementation plan in place?
 - What is the desired or required level of assurance that the selected security controls, as implemented, are effective in their application?

The answers to these questions are not given in isolation but rather in the context of an effective risk management process for the organization that identifies, mitigates as deemed necessary, and monitors on an ongoing basis, risks arising from its information and information systems.



NIST SP 800-53 Security and Privacy Controls

Security Control Structure

- Each family contains security controls related to the general security topic of the family
- Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems/devices
- There are 18 security control families and over 900 controls included in NIST SP 800-53

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness & Training	PE	Physical & Environmental Protection
AU	Audit & Accountability	PL	Planning
CA	Security Assessment & Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System & Services Acquisition
IA	Identification & Authentication	SC	System & Communications Protection
IR	Incident Response	SI	System & Information Integrity
MA	Maintenance	PM	Program Management

Security Control Identifiers and Family Names

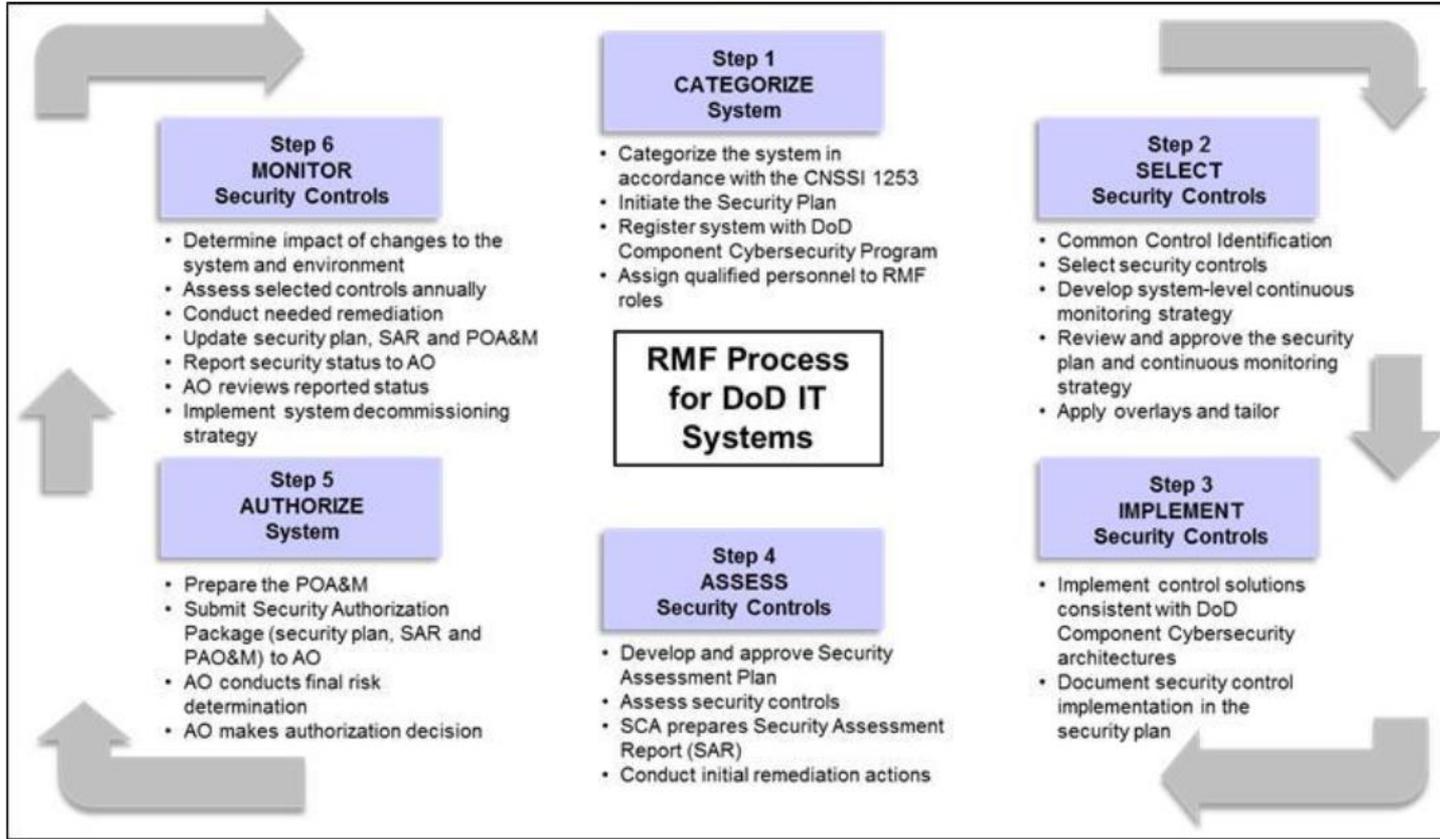


Changes to Cybersecurity Roles & Responsibilities

DIACAP role DODI 8510.01, 2007	RMF role DODI 8510.01 2014	Responsibilities (Reference DoDI 8510.01 for a complete definition of roles and responsibilities)
Designated Accrediting Authority (DAA)	Authorizing Official (AO)	The AO ensures all appropriate RMF tasks are initiated and completed, with appropriate documentation, for assigned ISs and PIT systems, monitor and track overall execution of system-level POA&Ms, Promote reciprocity.
Certifying Authority	Security Control Assessor (SCA)	The SCA is the senior official with authority and responsibility to conduct security control assessments.
No explicit role	Information System Owner (ISO)	In coordination with the information owner (IO), the ISO categorizes systems and documents the categorization in the appropriate JCIDS document (e.g., CDD).
Information Assurance Manager (IAM)	Information System Security Manager (ISSM)	The ISSM maintains and reports IS and PIT systems assessment and authorization status and issues, provides ISSO direction, and coordinates with the security manager to ensure issues affecting the organization's overall security are addressed appropriately.
Information Assurance Officer	Information System Security Officer (ISSO)	The ISSO is responsible for maintaining the appropriate operational security posture for an information system or program .



RMF 6 Step Process





RMF Authorizations

Authorization Type	Decision Criteria	Authorization Period
Authorization to Operate (ATO)	Overall risk is determined to be acceptable, and there are no NC controls with a level of risk of “Very High” or “High”.	Must specify an Authorization Termination Date (ATD) that is within 3 years of the authorization date unless the IS or PIT system has a system-level, DoD policy compliant ,continuous monitoring program.
ATO with conditions (Only with permission of the DoD Component Chief Information Officer (CIO))	NC controls with “Very High” or “High” risk that can’t be corrected or mitigated immediately, but overall system risk is determined to be acceptable due to mission criticality	Should specify an AO review period that is within 6 months of the authorization date. If the system still requires operation with a level of risk of “Very High” or “High” after 1 year, the DoD Component CIO must again grant permission for continued operation of the system.
Interim Authority To Test (IATT)	Risk determination is being made to permit testing of the system in an operational information environment or with live data, and the risk is acceptable,	Should expire at the completion of testing (normally for a period of less than 90 days)
Denial of Authorization to Operate (DATO)	Risk is determined to be unacceptable	Immediate or in concert with a system decommissioning strategy



RMF Knowledge Service

The Knowledge Service is the **authoritative source** for information, guidance, procedures, and templates on how to execute the DIACAP and Risk Management Framework

DIACAP KNOWLEDGE SERVICE

Governing Policy | Collaboration | Implementation Guidance | Site Resources

DIACAP Knowledge Service

DIACAP Roadmap Step by Step Execution

Resources

Acronyms | Glossary | References

DIACAP DoD Information Assurance Certification and Accreditation Process

DoD Department of Defense

DoDI DoD Instruction

eMASS Enterprise Mission Assurance Support Service

IA Information Assurance

ISSE Information Systems Security Engineer or Engineering

KS Knowledge Service

NSA National Security Agency

PPSM Ports, Protocols and Services Management

SSAA System Security Authorization Agreement

TAG Technical Advisory Group

[Click to view changes on this page.](#)

Welcome to the DIACAP Knowledge Service

The Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) Knowledge Service (KS) is DoD's official site for enterprise DIACAP policy and implementation guidelines. The DIACAP Knowledge Service provides IA practitioners and managers with a single authorized source for execution and implementation guidance, community forums, and the latest information and developments in DIACAP. The DIACAP Knowledge Service supports both the eMASS and non-eMASS implementation of the DIACAP.

The Knowledge Service features information on DIACAP policy, implementation guidance, and some collaborative tools such as Discussion Boards and Component Workspaces. The content is organized in four main categories which have drop-down navigation associated with each: Governing Policy, Implementation Guidance, Collaboration, and Site Resources. Additionally, there are links to News and Events, a contacts page, and the Site Map in the top right corner.

Governing Policy

- What is DIACAP?
- 8E10.01
- Governance Structure
- Reciprocity Memorandum

Implementation Guidance

- DIACAP Activities
- IA Controls
- Certification Support Services
- Transitioning to DIACAP
- Automated Tools
- CSA Transformation
- ISSE

Collaboration

- TAG
- Component Workspaces
- Community Review
- Discussion
- Events

Site Resources

- Reference Library
- Help
- Site Changes Log
- References
- Links
- Training
- Contact Us
- Site Map

RMF KNOWLEDGE SERVICE

RMF General | RMF Implementation Steps | Policy & Guidance | Site Resources

RMF Knowledge Service

RMF Overview

- Introduction to F...
- Transition Guid...

RMF Governan...

- Introduction to F...
- RMF Roles

RMF Role Appointment and Tasks

- Senior RMF Role Directory
- Tier 1: Organization
- Tier 2: Mission/Business Process
- Tier 3: IS and PIT Systems

IT

- Define DoD IT Type
- Enclaves
- Major Applications
- Platform IT Systems
- Enterprise Services
- IT Products
- IT Services
- Platform IT
- DoD Internet Services and Internet-Based Capabilities Procedures

Step 1. Categorize System

- Step 2: Select Security Controls
- Step 3: Implement Security Controls
- Step 4: Assess Security Controls
- Step 5: Authorize System
- Step 6: Monitor Security Controls

RMF Training

- RMF Training Opportunities
- eMASS
- What is eMASS
- KS and eMASS Comparison
- What is eMASS FAQ

RMF Lifecycle

Learn about the RMF process for DoD IT Systems. [View the RMF Life Cycle.](#)

Additional Information:

[Acronyms](#) [Glossary](#)

<https://rmfks.osd.mil/>



RMF Transition Timeline

(per RMF Knowledge Service)

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

What this means:

The longer you stay with DIACAP, the shorter the ATO. DIACAP certified systems should be almost extinct by mid-year 2018.



DAU and Cybersecurity

- Cybersecurity and DoD Acquisition – CLE 074
 - 5 hour on-line course – Tim Denman – POC
 - Deployed –March 31, 2015
- RMF Implementer’s Course – ISA 220
 - 3 to 4 day on-line course– Steve Mills – POC
 - Deployment –2016
- 2 Program Protection Planning (PPP) Courses are also being developed (Online and classroom) – ENG 160 and ENG 260
- DAU Cybersecurity Activities
 - Training, Consulting, Curriculum Development and subject matter expertise
 - Currently seven people are doing this work DAU-wide. This will double by August
 - Ongoing mission assistance/ consulting work at Eglin Air Force Base, SPAWAR, Redstone Arsenal (AMRDEC), Wright Patterson AFB, ...
 - **Central POC: Tim Denman – DAU Cybersecurity Performance Learning Director**
Tim.Denman@dau.mil Phone: 256-922-8174
Acquisition.cybersecurity@dau.mil

