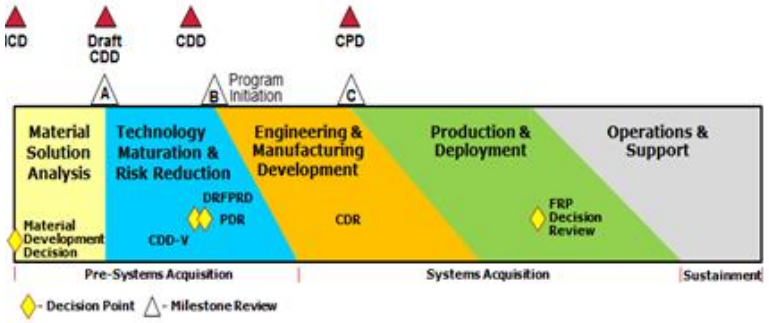
Cybersecurity and the Risk Management Framework for DoD Information Technology

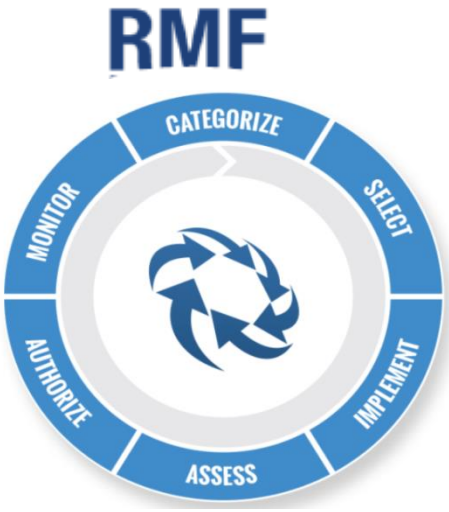
February 4, 2015 Lunch and Learn

Tim Denman
Systems Engineering and Technology Dept Chair/ Cybersecurity Lead
DAU – South, Huntsville
Tim.Denman@dau.mil

Outline

- Current State of Cybersecurity in the DoD
- Current Needs
  - Communications focus
  - Changing the culture
- Defining cybersecurity
- Risk Management Framework Concepts
- The RMF Process
- RMF Transition





Defense Science Board Cybersecurity Observations

- "Current DoD actions, though numerous are **fragmented**. Thus DoD is not prepared to defend against this threat."
- "DoD Red Teams, using cyber **attack tools** which can be downloaded from the internet, are **very successful at defeating our systems**"
- "With present capabilities and technology **it is not possible to defend with confidence** against the most sophisticated cyber attacks."
- "**It will take years** for the Department to build an effective response to the cyber threat."

Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. (January 2013)

We must move faster than the Enemy

Nearly every U.S. arms program found vulnerable to cyber attacks

BY ANDREA SHALAL

WASHINGTON Tue Jan 20, 2015 8:04pm EST

"The continued development of advanced cyber intrusion techniques makes it likely that determined cyber adversaries can acquire a foothold in most (Department of Defense) networks, and could be in a position to degrade important DOD missions when and if they chose to." Michael Gilmore, Director of Operational Test and Evaluation (DOT&E)

DoD Communications
What has changed in the last 7 years?

DoD Strategy

Department of Defense

Cyberspace Workforce Strategy

December 4, 2013

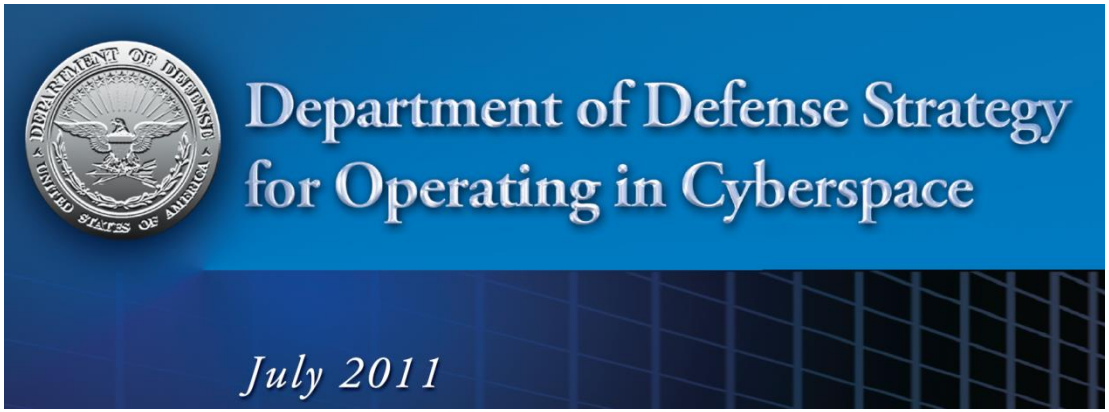
Cloud Computing Strategy

July 2012

DOD Memo, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 Dec 2014

The Department of Defense Strategy for Implementing the Joint Information Environment

September 18, 2013

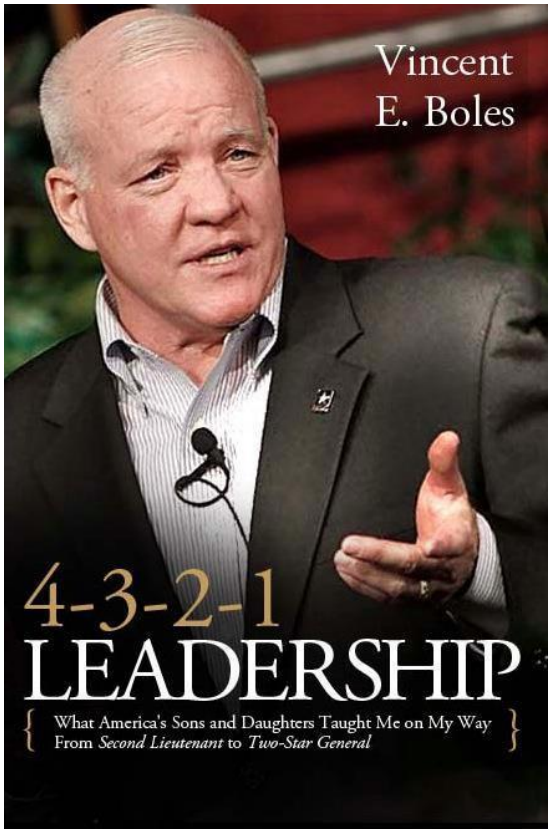


Changing the Culture

- Leadership and Cybersecurity Professionals
- Software Assurance
- Supply Chain Risk Management
- Cybersecurity, A Team sport

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 Information Technology



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

Software Assurance

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

Supply Chain Risk Management

- 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.

Cybersecurity – A Team Sport

Who should be involved and how?

TEST AND EVALUATION

IT Professional

Cybersecurity Professional

Configuration Management

Engineers

Architecture

Contracts

Program Manager

Logistics and Purchasing

Requirements

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.

Changing from Information Assurance to Cybersecurity?

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

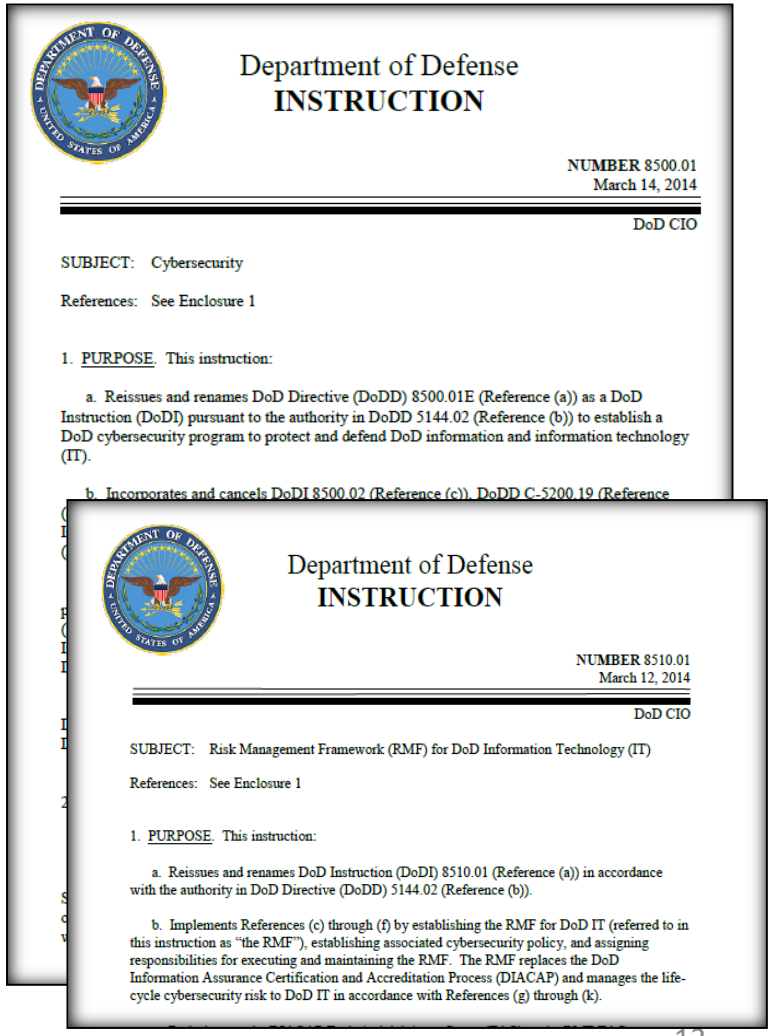
DoDI 8500.01 adopts the term "cybersecurity" to be used throughout the DoD instead of the term "information assurance (IA)."

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



Department of Defense
INSTRUCTION

NUMBER 8500.01
March 14, 2014

DoD CIO

SUBJECT: Cybersecurity

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).

b. Incorporates and cancels DoDI 8500.02 (Reference (c)), DoDD C-5200.19 (Reference

Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014

DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).

Why Change Policy?

- The new policy is more consistent with established disciplines and best practices for effective systems engineering, systems security engineering, and program protection planning outlined in DoDI 5000.02 & DAG.
- The new policy leverages and builds upon numerous existing Federal policies and standards so we have less DoD policy to write and maintain.

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

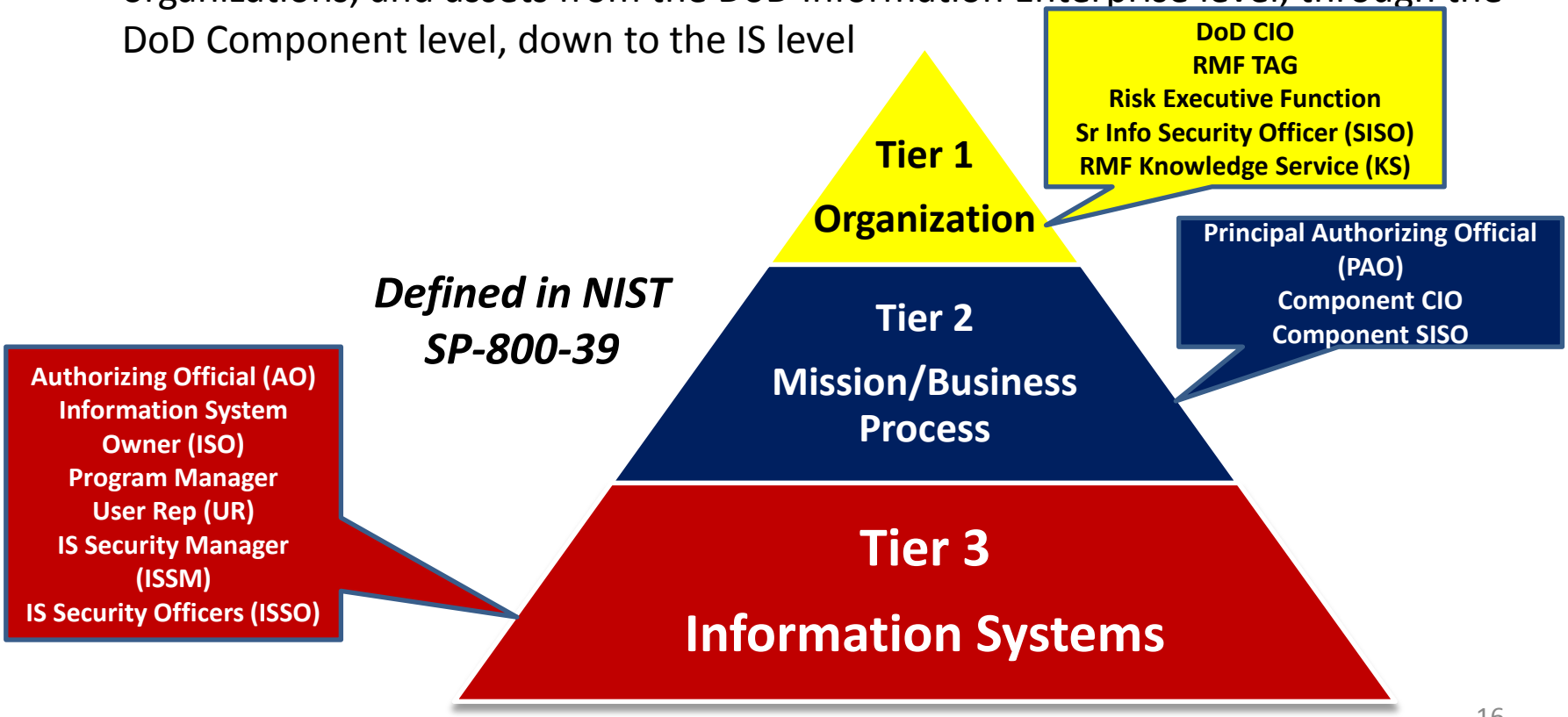
Key RMF Documents

- **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

DoDI 8500.01 - Cancels or supersedes 11 DoD Directives, Instructions, or Memorandums, and references a total of 132 policy documents, including 12 NIST Special Publications and 9 CNSS Instructions or Policies.

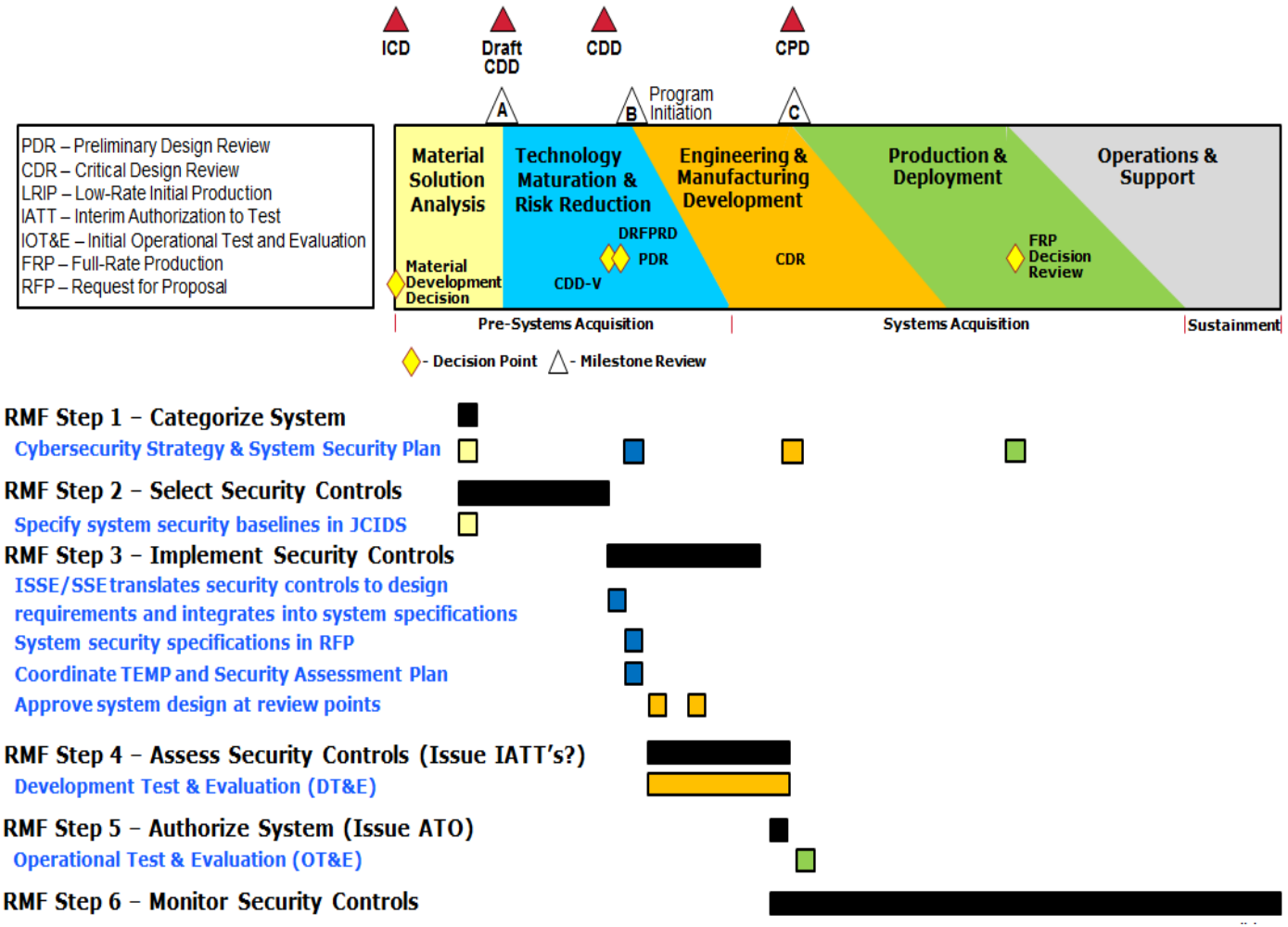
Risk Management and the RMF

- Multi-tiered Risk Management
  - DoD will implement a multi-tiered cybersecurity risk management process to protect U.S. interests, DoD operational capabilities, and DoD individuals, organizations, and assets from the DoD Information Enterprise level, through the DoD Component level, down to the IS level



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

RMF and Cybersecurity Reciprocity

- 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

RMF and Continuous Monitoring

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.

NIST SP 800-53
Security and Privacy Controls

- 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

NIST SP 800-53 Security and Privacy Controls (An Example)

Access Control – AC-6 – Least Privilege

- Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- Supplemental Guidance: Organizations employ least privilege for specific duties and information systems… Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.
- Control Enhancements:
  - (1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS
    - The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].
    - Supplemental Guidance: Security functions include, …
  - *(Enhancements 2 -9 - not shown)*
  - (10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS
    - The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
    - Supplemental Guidance: Privileged functions include, …
- References: None.
- Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-6(1) (2) (5) (9) (10)	**HIGH** AC-6(1) (2) (3) (5) (9) (10)

Assessing Security Controls Example Procedures

SI-4(15)	INFORMATION SYSTEM MONITORING
SI-4(15).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing wireless communications intrusion detection capability].

SI-4(16)	INFORMATION SYSTEM MONITORING
SI-4(16).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; event correlation logs or records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system monitoring responsibilities].

NIST Special Publication 800-53A

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 Process

Step 1: Categorize System
- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2: Select Security Controls
- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3: Implement Security Controls
- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Step 4: Assess Security Controls
- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5: Authorize System
- Prepare the POA&M
- Submit Security Authorization - - Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6: Monitor Security Controls
- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR, and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

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 Transition Timeline
(per RMF Knowledge Service)

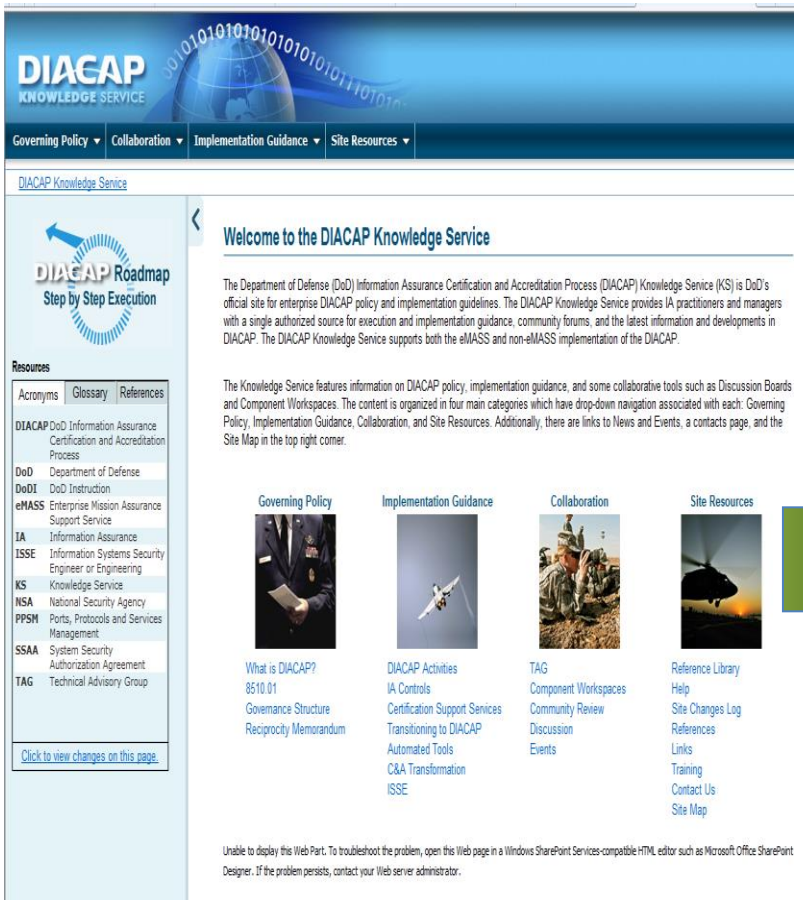
Completed DIACAP Package Submitted to AO for Signature	ATO Date	Maximum Duration of ATO under DIACAP
Present through May 31, 2015	Determined by AO Signature Date	2.5 years from AO signature date
June 1, 2015 through February 1, 2016		2 years from AO signature date
February 2, 2016 through October 1,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

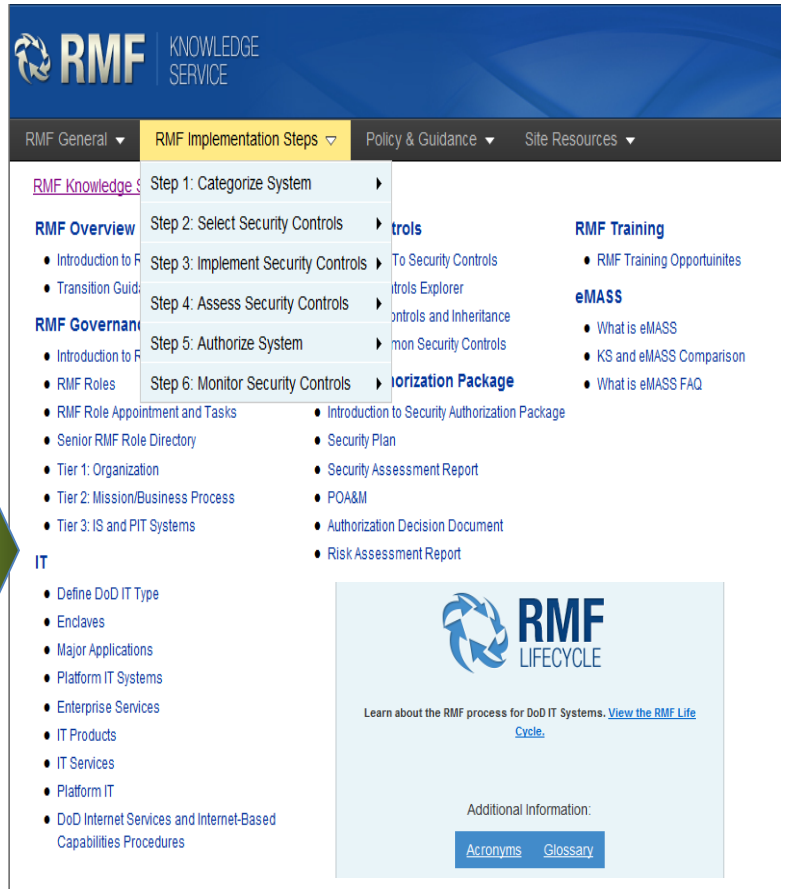
What this means:

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

RMF Knowledge Service

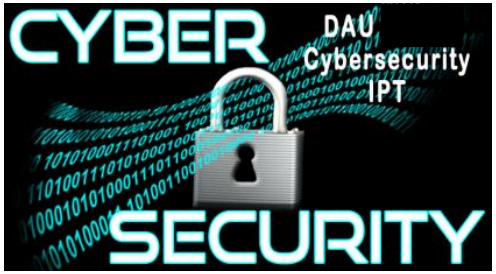
The Knowledge Service is the **authoritative source** for information, guidance, procedures, and templates on how to execute the DIACAP and Risk Management Framework





https://rmfks.osd.mil/

DAU and Cybersecurity

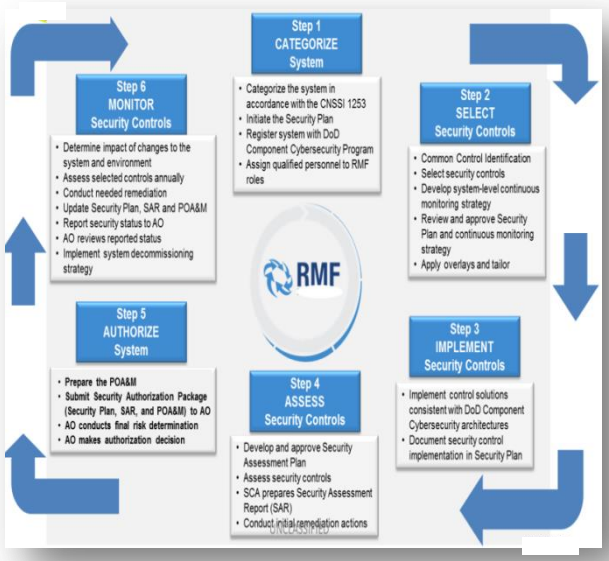


- Cybersecurity and DoD Acquisition – CLE 074
  - 4 - 5 hour on-line course – Tim Denman – POC
  - Deployment – April 2015
- RMF Implementer's Course – ISA 220
  - 3 to 4 day on-line course– Steve Mills – POC
  - Deployment – Early 2016
- 2 Program Protection Planning (PPP) Courses are also being developed (100 and 200 level – Online and classroom)
- DAU Cybersecurity Integrated Product Team (IPT)
  - Training, Consulting, Curriculum Development and subject matter expertise
  - Ongoing mission assistance/ consulting work at Eglin Air Force Base, SPAWAR, Redstone Arsenal (AMRDEC), Wright Patterson AFB, …
  - For more information contact: **Tim Denman (Huntsville, AL) –** Tim.Denman@dau.mil **Phone: 256-922-8174**

- **BACKUPS**

Summary

- Introduction and Applicability
- Major RMF Concepts
  - Risk Management
  - Cybersecurity Throughout the Program Lifecycle
  - Operational Resilience, Integration and Interoperability
  - Reciprocity
  - Continuous Monitoring
- RMF Security Controls
- RMF Responsibilities
- The RMF Cybersecurity Process
- RMF Transition



RMF Process

Step 1: Categorize System
- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2: Select Security Controls
- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3: Implement Security Controls
- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Step 4: Assess Security Controls
- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5: Authorize System
- Prepare the POA&M
- Submit Security Authorization - - Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6: Monitor Security Controls
- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR, and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Tier 1 RMF Governance Structure

Tier 1 is the Office of Secretary of the Defense - OSD, and/or strategic level, and it addresses risk management at the DoD enterprise level.

The key governance elements in Tier 1 are:

- DoD CIO Directs and oversees the cybersecurity risk management of DoD IT
- Risk Executive Function DoD Information Security Risk Management Committee (ISRMC) (formerly the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel) performs the DoD Risk Executive Function. Defense IA Security Accreditation Working Group (DSAWG) supports the DoD ISRMC and develops and provides guidance to the Authorizing Officials for IS connections to the DoD Information Enterprise
- DoD Senior Information Security Officer (SISO) The DoD SISO represents the DoD CIO, directs and coordinates the DoD Cybersecurity Program, and establishes and maintains the DoD RMF
- The RMF Technical Advisory Group (TAG) The TAG provides implementation guidance for the DoD RMF
- The RMF Knowledge Service (KS) The KS is the **authoritative source** for RMF procedures and guidance. The KS supports RMF by providing access to DoD security control baselines, security control descriptions, security control overlays, and DoD implementation guidance and assessment procedures

Tier 2 RMF Governance Structure

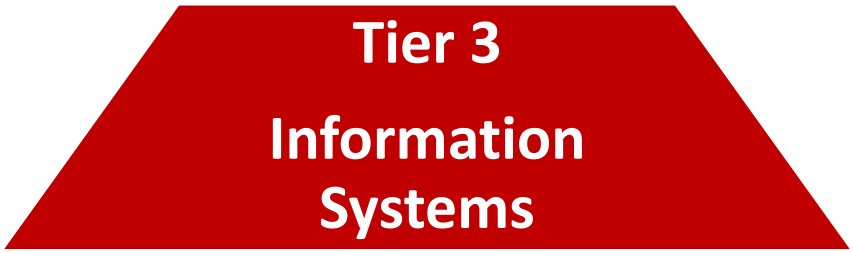
Tier 2 are the Mission Areas and Component level and addresses risk management at this level. The key governance elements in Tier 2 are:

- Principal Authorizing Official (PAO) A PAO is appointed for each of the 4 DoD Mission Areas (MAs), the Enterprise Information Environment MA (EIEMA), Business MA (BMA), Warfighting MA (WMA), and DoD portion of the Intelligence MA (DIMA)
- DoD Component CIO Component CIOs are responsible for administration of the RMF within the DoD Component Cybersecurity Program, including:
  - Enforcing training requirements for persons participating in the RMF
  - Verify that a Component Program Manager or System Manager is identified for each IS or Platform IT system
  - Appoint Component SISO
- Component SISO Component SISOs have authority and responsibility for security controls assessment, including:
  - Establishing and managing a coordinated security assessment process
  - Performing as the Security Controls Assessor (SCA) or formally delegate the security control assessment role

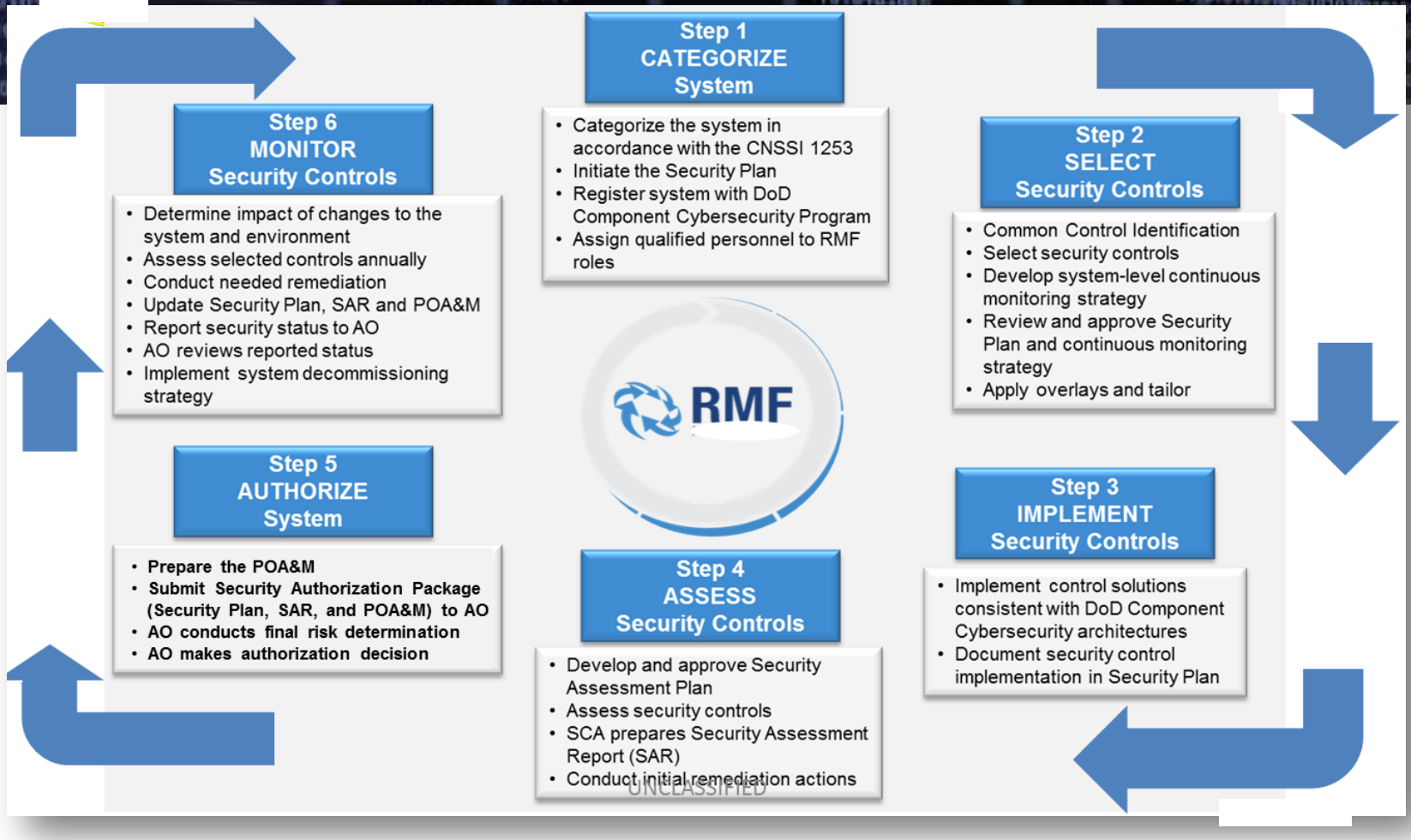
Tier 3 RMF Governance Structure

Tier 3 – is the System Level, and addresses risk management at this level. The key governance elements in Tier 3 are:

- Authorizing Official (AO) The DoD Component heads are responsible appointing trained and qualified AOs for all DoD ISs and PIT systems within their Component. AOs should be appointed from senior leadership positions within business owner and mission owner organizations
- System Cybersecurity Program The system cybersecurity program consists of the policies, procedures, and activities of the:
  - Information System Owner (ISO) Appoints a User Representative (UR) for assigned IS or PIT system
  - Program Manager/System Manager (PM/SM) Ensures an IS Systems Engineer is assigned for IS or PIT systems and implements the RMF for assigned IS or PIT systems
- User Representative (UR)
- IS Security Manager (ISSM)
- IS Security Officers (ISSO)

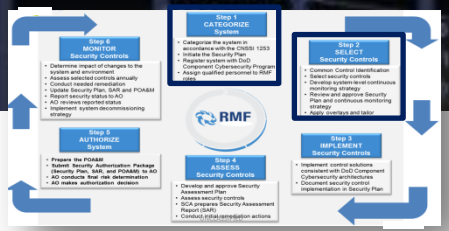


RMF – 6 Step Process



This process parallels the system life cycle, with the RMF activities being initiated at program or system inception

RMF – Steps 1 and 2



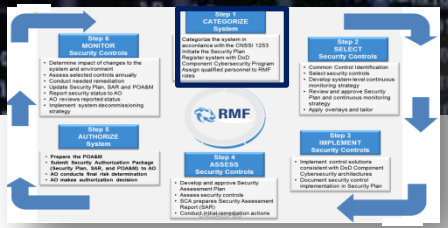
- **Step 1 - Categorize System**
  - Categorize the system in accordance with CNSSI 1253 and document the results in the security plan.
  - Describe the system (including system boundary) and document the description in the security plan.
  - Register the system with the DoD Component Cybersecurity Program
  - Assign qualified personnel to RMF roles.
- **Step 2 - Select Security Controls**
  - Common Control Identification - Common controls are selected as "common" and provided via the Knowledge Service based on risk assessments conducted by these entities at the Tier 1 and Tier 2 levels
  - Security Control Baseline and Overlay Selection - Identify the security control baseline for the system
  - Monitoring Strategy - Develop and document a system-level strategy for the continuous monitoring of the effectiveness of security controls

RMF – Step 1 – Categorize System

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

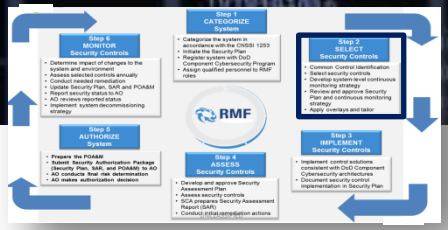
FIPS Publication 199 - Standards for Security Categorization of Federal Information and Information Systems



From CNSSI 1253

The security categorization method builds on the foundation established in FIPS 199, which defines three impact values (low, moderate, or high) reflecting the potential impact on organizations or individuals should a security breach occur (i.e., a loss of confidentiality, integrity, or availability). Organizations that employ NSS applying these definitions must do so within the context of their organization and the overall national interest.

Overlays - Can be applied in Step 2



Overlays address additional factors beyond impact (baselines only address impact of loss of confidentiality, integrity, and availability)

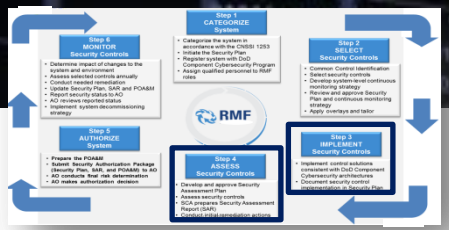
Enterprise Tailoring

- Consistent approach and set of security controls by subject area
- One time resource expenditure vs. continued expenditures of single system tailoring
- Promotes reciprocity

Current approved overlays include:

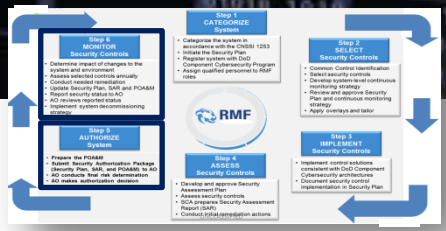
- *Intelligence (FOUO, October 2012)*
- *Space Platforms (June 2013)*
- *Cross Domain Solutions (September 2013)*

RMF – Steps 3 and 4



- **Step 3 - Implement Security Controls**
  - Implement the security controls specified in the security plan
  - Document the security control implementation
  - Security controls that are available for inheritance (e.g. common controls) by IS and PIT systems will be identified and have associated compliance status provided by hosting or connected systems
- **Step 4 - Assess Security Controls**
  - Develop, review, and approve a plan to assess the security controls.
  - Assess the security controls in accordance with the security assessment plan and DoD assessment procedures
  - Prepare the Security Assessment Report, documenting the issues, findings, and recommendations from the security control assessment
  - Conduct remediation actions on non-compliant security controls based on the findings and recommendations of the SAR and reassess remediated control(s)

RMF – Steps 5 and 6



- **Step 5 - Authorize System**
  - Prepare the Plan of Actions and Milestones (POA&M) based on the vulnerabilities identified during the security control assessment
  - Assemble the security authorization package and submit the package to the AO for adjudication.
  - Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation
  - Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable
- **Step 6 - Monitor Security Controls**
  - Determine the security impact of proposed or actual changes to the IS or PIT system and its environment of operation
  - Assess a subset of the security controls employed within and inherited by the IS or PIT system
  - Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M
  - Implement a system decommissioning strategy, when needed, which executes required actions when an IS or PIT system is removed from service

RMF Transition Timeline
(per DoDI 8510.01, Enclosure 8)

System Authorization Status		Transition Timeline And Instructions
1	New start or unaccredited	Transition to the RMF within six months
2	System has initiated DIACAP but has not yet started executing the DIACAP Implementation Plan	Transition to the RMF within six months
3	System has begun executing the DIACAP Implementation Plan	Either: a. Continue under DIACAP. Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline or b. Transition to the RMF within six months
4	System has a current valid DIACAP accreditation decision	Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline
5	System has a DIACAP accreditation that is more than 3 years old	Transition to the RMF within six months