Dr. Charles Kiriakou, Ms. Kate Cunningham, Mr. Kevin Winters, & Mr. Carl Rice

September 3, 2014

UNCLASSIFIED
Bottom Line Up Front (BLUF)

- The Department of Defense (DoD) has mandated the transition from DoD Information Assurance Certification and Accreditation Process (DIACAP) to the National Institute of Standards and Technology (NIST) based DoD Risk Management Framework (RMF) Authorization Process.

- Both are constructs/policies by which the DoD approves systems to operate at an acceptable level of risk.

- RMF introduces more complexity into the system approval process
Transition from the DIACAP to DoD RMF

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

- Previous versions of DoDD 8500.01, DoDI 8500.2 and DoDI 8510.01 for DIACAP
- Mission Assurance Category (MAC)/Confidentiality Level (CL): 9 possible MAC/CL combinations
- IS Definitions
- DoD Defined IA Security Controls
- Impact Value: Low / Moderate / High
- Security Objectives: Confidentiality / Integrity / Availability
- 27 possible baseline combinations
- Expanded IT definition to align with CNSSI 4009 and encompasses new and emerging capabilities
- Using NIST SP 800-53 Security Control Catalog. Creating DoD Assignment Values, validation procedures, and implementation guidance.
- New revisions of DoDD 8500.01, DoDI 8500.2 and DoDI 8510.01 for RMF
**DoD 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 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 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 PAO&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

---

**U.S. FLEET CYBER COMMAND / U.S. TENTH FLEET**
RMF Overview

• The basic process steps are similar to DIACAP but there are significant differences in several of the RMF process steps:
  – Categorization using impact levels associated with the three security objectives of Confidentiality, Integrity, and Availability (CIA) vice Mission Assurance Category (MAC) and Confidentiality Level (CL)
  – RMF has two process options Assess Only and Assess and Authorize
  – RMF has added Overlays for special assessment categories (e.g., Space, Cross Domain Solution, Privacy, Classified) and are attachments to the CNSSI 1253. An overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines.
RMF Overview (Cont)

- There is a significant increase in the number of security controls and validation procedures:
  - For a DIACAP MAC I Classified system there are 110 Information Assurance (IA) Controls and 173 Validation procedures by comparison an RMF Baseline with a CIA Security Category of High/High/High initially has 950 Security Controls and 2769 Validation procedures before tailoring is accomplished.
  - For a DIACAP MAC III Public system there are 75 IA Controls and 102 Validation procedures by comparison an RMF package with a CIA Security Category of Low/Low/Low initially has 940 Security Controls and 2740 Validation procedures before tailoring is accomplished.
  - These figures do not include any additional overlays (e.g., Privacy, Classified, or Space Systems)
- Impact levels change from Low/Medium/High to Low/Moderate/High and risk levels change from Low/Medium/High to Very Low/Low/Medium/High/Very High
• Anticipate there will be considerably more resources (e.g., time and personnel) required across the board by Program Managers, system owners, validators, Security Control Assessor (SCA), and the Authorizing Official (AO).

• Interim Authorizations To Operate (IATO) are no longer an accreditation vehicle, Authorizations To Operate (ATO) with conditions replace IATOs but the criteria is slightly different.
DoD RMF IT Definitions

- **DoD Information Technology (IT) has been divided into four forms:**
  - **Information System (IS):** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
  - **Platform Information Technology (PIT):** May consist of both hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems (i.e., platforms). PIT differs from products in that it is integral to a specific platform type as opposed to being used independently or to support a range of capabilities (e.g., major applications, enclaves or PIT systems).
    - PIT subcategories include “PIT” and “PIT Systems”.
    - PIT Systems are subject to “assess and authorize”; PIT is required to be assessed only and do not require authorization by the AO. PIT introduces a new element of complexity into an already complex and misinterpreted process.
DoD RMF IT Definitions (Cont)

- **IT Services**: IT services are outside the service user organization’s authorization boundary, and the service user’s organization has no direct control over the application or assessment of required security controls. DoD organizations that use IT services are typically not responsible for authorizing them (i.e., issue an authorization decision). IT Services are required to be assessed only and do not require authorization by the AO.

- **IT Products**: Products (including applications), are defined in DoDI 8500.01 as “individual IT hardware or software items”. They can be commercial or government provided and can include for example, operating systems, office productivity software, firewalls, and routers. IT Products are required to be assessed only and do not require authorization by the AO.

Sources: RMF Knowledge Service: https://rmfks.osd.mil/rmf/Pages/default.aspx and CNSSI 4009
RMF Categorization

• Categorization is accomplished as per the Committee on National Security Systems Instruction (CNSSI) No. 1253. As part of the categorization process under RMF, the impact levels are determined for both the information type and the information system.
  – Categorization uses impact levels associated with the three security objectives of Confidentiality, Integrity, and Availability (CIA) as defined in Federal Information Processing Standards Publication 199 (FIPS-199)
• **DoD has directed risk assessments will be conducted as per the NIST Special Publication (SP) 800-30 Guide for Conducting Risk Assessments.**
  
  – The process is significantly more comprehensive than was used for DIACAP and will provide a considerably more detailed analysis and understanding of the vulnerabilities to the Authorizing Official (AO).
eMASS Transition Timeline

• Enterprise Mission Assurance Support Service (eMASS) is the web-enabled DoD tool which supports processing DIACAP packages. It will be updated to support the RMF processes and approval decisions.

• eMASS Release 5.0 (July 2014 release)
  – Added some capabilities for supporting RMF:
    • Dual policy (DIACAP & RMF) support
    • DIACAP to RMF System Migration
    • System Dashboard & Controls View updates
    • Executive Dashboard – Registration Metrics
    • Enhanced User Interface
  – What's missing:
    • Not all of the validation procedures, baselines, overlays, and organizational assigned values will be approved and available
    • Reciprocity and inheritance will not be fully supported

• eMASS will not be fully capable of supporting RMF until release 5.1 which is scheduled for release late December 2014.
  – Organizational assigned values
  – Inheritance redesign
  – Validation procedures
  – Baselines and overlays
Information Security Continuous Monitoring (ISCM)

- **ISCM is DoD mechanism to constantly monitor status of IT systems’ security**
- **ISCM policy is under development; technical implementation is likely years away. A functional ISCM solution is necessary to fully realize the potential advantages of RMF.**
- **ISCM and continuous authorization do not remove the security authorization requirement:**
  - In accordance with Appendix III to OMB Circular A-130 (Reference (ab)), systems must be reassessed and reauthorized once every 3 years. The results of an annual review or a major change in the cybersecurity posture at any time may also indicate the need for reassessment and reauthorization of the system.
  - Systems that have been evaluated as having a sufficiently robust system-level continuous monitoring program (as defined by emerging DoD continuous monitoring policy) may operate under a continuous reauthorization. Continuous monitoring does not replace the security authorization requirement; rather, it is an enabler of ongoing authorization decisions.

**DOD directives for implementing RMF are not contingent on ISCM capabilities**
Questions?
RMF References

- Department Of Defense Instruction (DODI) 8500.01 – Cybersecurity, implements Cybersecurity and cancels the DODI 8500.02 and DODI 8500.01E
- DODI 8510.01 – Risk Management Framework (RMF), directs DOD to use the NIST RMF
- Committee on National Security Systems Instruction (CNSSI) No. 1253 – Security Categorization and Control Selection for National Security Systems, used for categorizing all DOD IS and PIT and contains the DOD Specific Security Control Baselines
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 – Guide for Conducting Risk Assessments
- NIST SP 800-37 – Guide for Applying RMF
- NIST SP 800-53 – Catalog of Security Controls, this is the Security controls Catalog the CNSSI 1253 is based on the
- NIST SP 800-53 – Guide for Assessing the Security Controls in Federal Information Systems and Organizations, contains the assessment procedures for DOD IT
- NIST SP 800-60 (Vol I & II) – Guide for Mapping Types of Information and Information Systems to Security Categories
- CNSSI 4009 – National Information Assurance (IA) Glossary
- RMF Knowledge Service – The authoritative source for RMF documentation, guidance, and updates https://rmfks.osd.mil/rmf/Pages/default.aspx (CAC Required)
- Security Overlays are located at: https://www.cnss.gov/CNSS/issuances/Instructions.cfm