GSA

U.S. General Services Administration

GSA Federal Acquisition Training Symposium

May 10-11, 2016
Huntsville, AL

Learn > Discuss > Connect > Interact

Understanding Cybersecurity on DoD Acquisition Programs

Steve Mills – Professor of Program Management
DAU South Cyber Lead
Steve.mills@dau.mil
256.922.8761

Date

Overview

- Cybersecurity Policy Overview
  - DoDI 8500.01
  - DoDI 8510.01
  - Cybersecurity Appendix, DoDI 5000.02
  - PM Guidebook for Integrating RMF into the System Acquisition Lifecycle
  - Cybersecurity T&E Guidebook
- Integration of Cybersecurity related processes with the Acquisition Lifecycle:
  - Cybersecurity/RMF & Acquisition Lifecycle Integration Tool Ver 1.0
  - Challenges
  - How do we improve?
- DAU's Cybersecurity Support to our customers

DoDI 8500.01 – Cybersecurity

- Adopts the term "Cybersecurity" in lieu of "Information Assurance"
- Extends applicability to all DoD information technology processing DoD information – This is new!!
- Emphasizes operational resilience, integration, and interoperability
- Leverages and builds upon numerous existing Federal policies and standards so we have less DoD policy to write and maintain
- Adopts common Federal Cybersecurity terminology so we are all speaking the same language
- Transitions to the newly revised NIST SP 800-53 Security Control Catalog
- Incorporates Cybersecurity early and continuously throughout the acquisition lifecycle (Bake it in, Don't Bolt it On!)

DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT

- New approach for DoD to manage Cybersecurity risk – RMF adds another dimension to the DoD Risk Management Process
- A 6 step process that emphasizes continuous monitoring and timely correction of deficiencies
- Adopts NIST's Risk Management Framework, used by Civil and Intelligence communities
- Moves from a checklist-driven process to a risk based approach
- Embeds the RMF steps and activities in the DoD Acquisition Lifecycle
- Promotes DT&E and OT&E integration
- Implements Cybersecurity via security controls vice numerous policies and memos
- Supports and encourages use of automated tools

DoD RMF 6 Step 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

Step 5 AUTHORIZE System

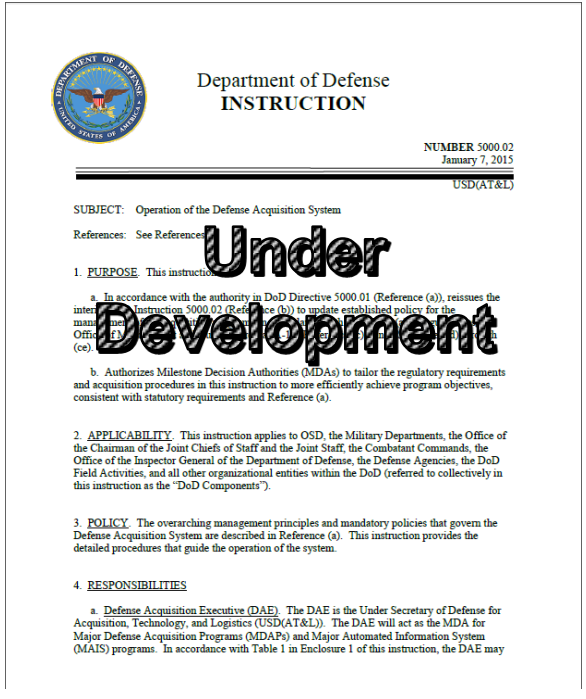
- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls

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

Cybersecurity Appendix to DoDI 5000.02

- In response to BBP 3.0, DoD is developing a Cybersecurity Appendix to DoDI 5000.02
- Numerous key DoD stakeholders are involved in this effort to include DAU
- The goal of this Appendix is:
  - Provide PMs and their staffs clarity on how Cybersecurity integrates with the acquisition lifecycle
- Key Focus Areas:
  - Cybersecurity and Source Selection
  - Cybersecurity as a design consideration
  - Cybersecurity's impact on overall program risk
  - Interaction between the PM and AO
  - Cybersecurity T&E
- Release date for this effort is TBD



Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

Under Development

1. PURPOSE. This instruction

a. In accordance with the authority in DoD Directive 5000.01 (Reference (a)), reissues the inter Instruction 5000.02 (Reference (b)) to update established policy for the mana Office (ce).

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

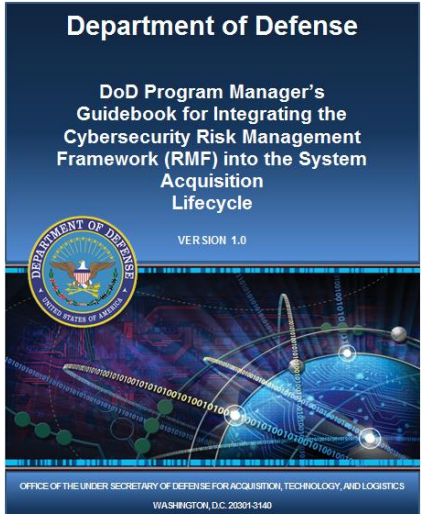
3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

4. RESPONSIBILITIES

a. Defense Acquisition Executive (DAE). The DAE is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DAE will act as the MDA for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. In accordance with Table 1 in Enclosure 1 of this instruction, the DAE may

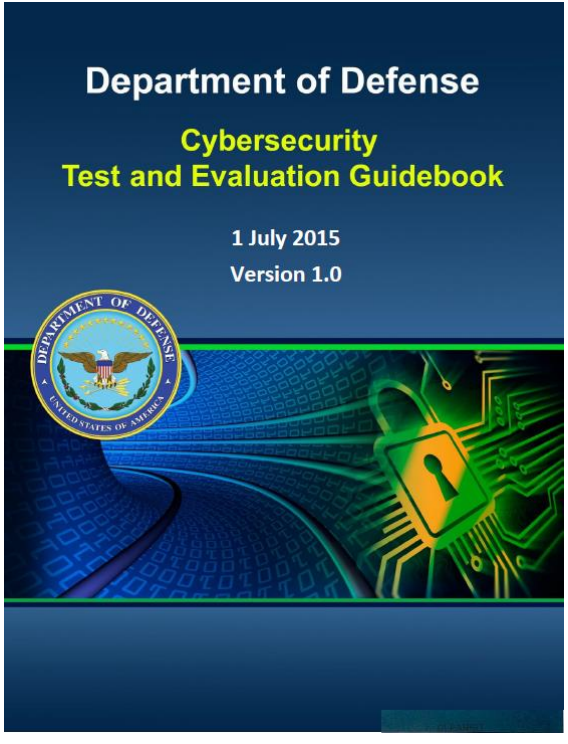
DoD PM Guidebook for RMF

- Purpose: Assist Program Managers (PM) in the efficient and cost effective integration of Cybersecurity into their systems
- Incorporates applicable Cybersecurity policy, processes and best practices into one document
- Emphasizes integrating Cybersecurity activities into existing processes including requirements, SSE, program protection planning, trusted systems and networks analysis, DT&E, OT&E, financial management and cost estimating, and sustainment and disposal.
- Contains 2 excellent examples of RMF integration across the acquisition lifecycle – found in Annex M:
  - Unmanned Aerial Bomber System (UABS)
  - Practical Automobile Example

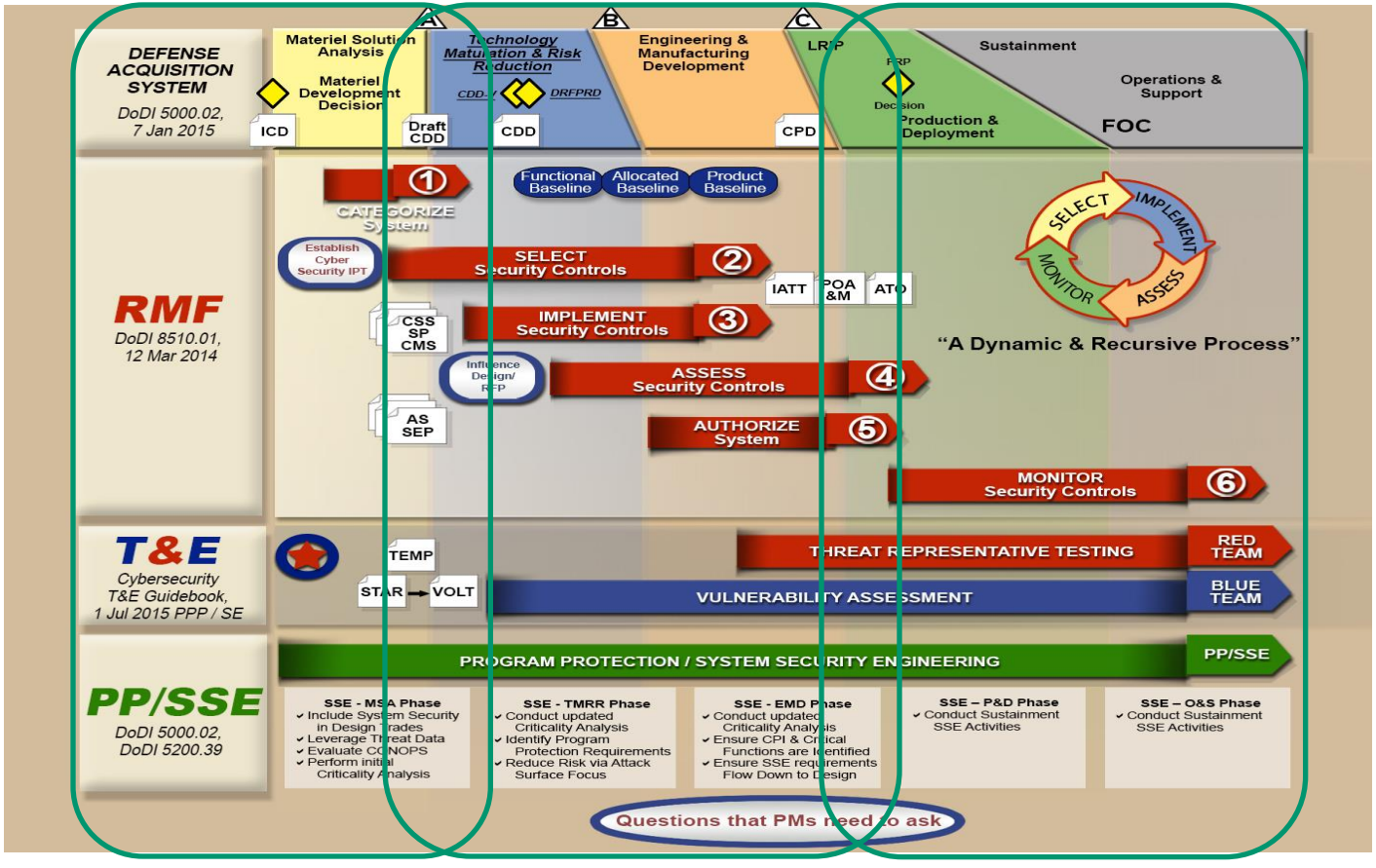


DoD Cybersecurity T&E Guidebook

- Purpose: Guidance on planning, analysis, and implementation of Cybersecurity T&E.
- 3 sections:
  - Introduction
  - T&E support to RMF Implementation
  - Implementation of Cybersecurity T&E across the Acquisition Lifecycle
- Provides detailed overviews on:
  - Analysis of RMF documents and artifacts to support T&E
  - Review and use of Program Protection Plans (PPPs) from a T&E perspective
  - Cybersecurity T&E test team resources
  - Use of Cyber ranges in support of T&E
  - Examples of common vulnerabilities related to Cybersecurity



Cybersecurity/RMF & Acquisition Lifecycle Integration Tool Ver 1.0



Did we correctly identify Cybersecurity requirements for this system?

Did we "bake" Cybersecurity into our system or will we have to "bolt on" items later?

Do we have an effective Continuous Monitoring Strategy in place for our system?

Cybersecurity Integration Challenges

- Successfully capturing and implementing Cybersecurity requirements for systems throughout the acquisition lifecycle
- Failure to recognize Cybersecurity as a "Design Consideration"
- Program Managers view of Cybersecurity as just another unfunded requirement
- Lack of a common understanding and definition of Cybersecurity
  - Effective Cybersecurity on DoD acquisition programs is much more than just the RMF
- Dynamic nature of the Cyber Threat
- Dynamic nature of the Cybersecurity posture of our DoD system(s)
- Lack of top management support
- DoD Cybersecurity Workforce Issues:
  - Cybersecurity expertise and training – The right folks with the right skills
  - Keeping Cybersecurity talent

Cybersecurity Integration Challenges
How do we improve?

- Ensure Cybersecurity related requirements are identified "up front and early"
  - Leverage key opportunities while mitigating key Cybersecurity acquisition risks
  - MSA & TMRR Phase Impacts
- Make Cybersecurity a key component of the Source Selection and Contract Administration processes. Use CPARS to document performance
- Adopt and use common Cybersecurity language
- Identify, provide and leverage relevant training
  - Weapon System / Acquisition related Cybersecurity awareness and training for all
  - Program Protection Planning, Development and implementation expertise and training
  - Robust System Security Engineering (SSE) across the acquisition lifecycle
- Integrate Cybersecurity Risk Management Framework into overall program risk
- Establish a Cybersecurity "Champion" for the PM – Cyber Integrator Concept

How DAU Can Help

- **DAU Web Presence:**
  - Links to current Cybersecurity Guidance and Policy
  - Cybersecurity related articles & content
  - Cybersecurity/RMF & Acquisition Lifecycle Integration Tool Ver 1.0
- **Education**
  - CLE074 Cybersecurity Throughout Acquisition
  - ACQ160 - Program Protection (Late 2016)
  - ENG260 – Program Protection Planning (Late 2016)
  - ISA220 RMF for Practitioners (Early 2017)
- **Execution** – Mission Assistance is one of our core competencies. We help our customers solve their acquisition challenges at the point of need
- **Expertise** – We have Cybersecurity faculty on our team to help solve your Cybersecurity related challenges

Questions?

Steve Mills
Professor of Program Management
Steve.mills@dau.mil
256.922.8761