DOD Cybersecurity and the Risk Management Framework (RMF) Process for the Acquisition Community (Industry & Government Training)

Presented by Professor Derek Duchein
DAU Cybersecurity Enterprise Team Member
November 30, 2016
Lunch ‘N Learn Forum Overview

• The Cybersecurity Landscape in the DoD

• The Risk Management Framework (RMF) Process in the DoD Acquisition Lifecycle
Learning Objectives

• Recognize the relationship of the DoD Risk Management Framework (RMF) for DoD Information Technology across the Acquisition Lifecycle to overall DoD Risk Management

• Recognize the Department of Defense (DoD) transition to authorizing the operation of DoD Information Technology

• Recognize the DoD RMF steps and Governance structure

• Recognize how the RMF Knowledge Service supports the RMF process as the authoritative source for DoD RMF guidance
The Importance of Cybersecurity

The Department of Defense has the largest network in the world and DoD must take aggressive steps to defend its networks, secure its data, and mitigate risks to DoD missions.

The Defense Department’s own networks and systems are vulnerable to intrusions and attacks. In addition to DoD’s own networks, a cyber attack on the critical infrastructure and key resources on which DoD relies for its operations could impact the U.S. military’s ability to operate in a contingency. DoD has made gains in identifying cyber vulnerabilities of its own critical assets through its Mission Assurance Program – for many key assets, DoD has identified its physical network infrastructure on which key physical assets depend – but more must be done to secure DoD’s cyber infrastructure.
What is not Vulnerable?

Virtually Everything is Vulnerable, Especially Critical Infrastructure
How Well Prepared is Your Organization?

<table>
<thead>
<tr>
<th>Question</th>
<th>Option A</th>
<th>Option B</th>
<th>Option C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you expect a cyber attack to strike your organization in 2015?</td>
<td>a. Yes – 54%</td>
<td>b. No – 21%</td>
<td>c. Not sure – 25%</td>
</tr>
<tr>
<td>Do you believe there is a shortage of skilled cybersecurity professionals?</td>
<td>a. Yes – 90%</td>
<td>b. No – 5%</td>
<td>c. Not sure – 6%</td>
</tr>
</tbody>
</table>

*2015 survey includes 1,211 US business and IT professionals from industry and government organizations

The Department of Defense has the largest network in the world and DoD must take aggressive steps to defend its networks, secure its data, and mitigate risks to DoD missions. DoD has made gains in identifying cyber vulnerabilities of its own critical assets through its Mission Assurance Program – for many key assets, DoD has identified its physical network infrastructure on which key physical assets depend – but more must be done to secure DoD’s cyber infrastructure. THE DEPARTMENT OF DEFENSE CYBER STRATEGY April 2015
Federal agencies have reported increasing numbers of cybersecurity incidents that have placed sensitive information at risk, with potentially serious impacts on federal and military operations; critical infrastructure; and the confidentiality, integrity, and availability of sensitive government, private sector, and personal information.
Attackers are Winning

Attacker Efficiency is increasing faster than Defender Efficiency

DOT&E observed improvements in several cybersecurity areas within the Department of Defense (DOD) this past year; however, the Department’s warfighting missions and systems remain vulnerable to cyber-attack.

As in previous years, assessment teams consistently found four categories of vulnerabilities in both system tests and exercise assessments:

- Exposed or poorly managed credentials
- Systems not configured to identified standards
- Systems not patched for known vulnerabilities
- System/network services and trust relationships that provide avenues for cyber compromise
Cybersecurity-Related Policies & Issuances

http://iac.dtic.mil/csiac/ia_policychart.html

Developed by the DoD Deputy CIO for Cybersecurity
(Updated 08/16/16)

Policy Chart references over 180 documents. Most are less than 3 years old.
Key Cybersecurity Policies

- DoDI 5000.02 - Operation of the Defense Acquisition System
- DoDI 8500.01 – Cybersecurity
- DoDI 8510.01 – Risk Management Framework (RMF) for DoD Information Technology (IT)
- DoDD 8140.01 – Cyberspace Workforce Management
- National Initiative for Cybersecurity Education (NICE)
• a. Cybersecurity Risk Management Framework (RMF). 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. Integration of the RMF in acquisition processes reduces required effort to achieve authorization to operate and subsequent management of security controls throughout the system life cycle.

• b. Cybersecurity Strategy. All acquisitions of systems containing IT, including NSS, will have a Cybersecurity Strategy. The Cybersecurity Strategy is an appendix to the Program Protection Plan (PPP) that satisfies the statutory requirement in section 811 of P.L. 106-398.
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
“Policy: Cybersecurity…must be included throughout the lifecycle…to include *acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement of all DoD IT supporting DoD tasks and missions”

• DoD CIO coordinates with the DOT&E to ensure that cybersecurity responsibilities are integrated into the operational testing and evaluation for DoD acquisition programs

• USD(AT&L) ensures the DoD acquisition process incorporates cybersecurity planning, implementation, testing, and evaluation and ensures acquisition community personnel are qualified

• DoD COMPONENT HEADS ensure that system security engineering and trusted systems and networks processes, tools and techniques are used in the acquisitions under their purview.

* Note the different job responsibilities that must be involved.
DoDI 8500/8510: Cybersecurity/ RMF

- Adopts “Cybersecurity” instead of “Information Assurance”
- Extends applicability to all DoD information technology processing DoD information
- Emphasizes operational resilience, integration, reciprocity, and interoperability
- Aligns with Joint Task Force Transformation Initiative (DoD, NIST, IC, and CNSS)
- 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 early/continuously in acquisition lifecycle
This process parallels the system life cycle, with the RMF activities being initiated at program or system inception.
Risk Management Guidance As It Relates to the DoD RMF

The DoD leverages several policy and guidance documents to address the Department’s focus on risk management. Per Department of Defense Instruction (DoDI) 5000.02 and DoDI 8500.01, building cybersecurity into the system early and throughout the life cycle is required to enable operational and technical cybersecurity risks to be identified and sufficiently mitigated throughout the acquisition process. It will also lead to decreased program costs, shortened schedules, and improved system performance, resilience, and trustworthiness.

Following are two references cybersecurity professionals and program managers can use for guidance:

- The DoD Risk, Issue, Opportunity Management Guide for Defense Acquisition Programs
- The Program Manager’s Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle
The RMF Initial Transition Timeline and Instructions table establishes the timeline for the authorized continued use of DIACAP. The emphasis is on the date an IS or PIT system received AO signature. From that date, all DoD Information and PIT systems must transition to the RMF within the timelines specified in the right hand column based on the system's DIACAP AO signature timeline in the left hand column.

<table>
<thead>
<tr>
<th>Completed DIACAP (Department of Defense Information Assurance Certification and Accreditation Process) Package Submitted to AO (Authorizing Official) for Signature</th>
<th>ATO (Authority to Operate) Date</th>
<th>Maximum Duration of ATO under DIACAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature date of this document through May 31, 2015</td>
<td>Determined by AO Signature Date</td>
<td>2.5 years from AO signature date</td>
</tr>
<tr>
<td>June 1, 2015 through February 1, 2016</td>
<td></td>
<td>2 years from AO signature date</td>
</tr>
<tr>
<td>February 2, 2016 through October 1, 2016</td>
<td></td>
<td>1.5 years from AO signature date</td>
</tr>
</tbody>
</table>
Information and PIT systems must be both assessed and authorized to operate. PIT and IT services & products only need to be assessed.
People are a critical factor in any cyber security initiative. The following is a list of typical team members. They are the ones that your organization will depend on to throughout the RMF process.
The Purpose of the RMF Knowledge Service

- RMF KS is a Public Key Infrastructure (PKI)-enabled Common Access Card (CAC) or DoD-Approved External PKI Certificate required, web-based resource, managed by the DoD Chief Information Officer (CIO), that serves as DoD’s authoritative source for all RMF information.

- The RMF KS provides DoD RMF practitioners with immediate access to RMF policy and guidance to effectively and efficiently apply the appropriate methods, standards, and practices required to protect DoD Information Technology (IT). The RMF KS provides the most up to date implementation guidance and DoD intent in addressing evolving security objectives and risk.
eMASS is a DoD government-developed enterprise web-based application that provides visibility and automation for Cybersecurity Management processes.
Effective Cybersecurity in DoD Acquisition Programs

- Effective cybersecurity in DoD acquisition programs encompasses all of the actions taken to ensure the confidentiality, integrity, and availability of system information to enable warfighting operations.

- Cybersecurity risk management tasks begin early in the system development life cycle and are important in shaping the security capabilities of the Information System (IS).
1. **Risk Planning** is developing and documenting organized, comprehensive, and interactive strategies and methods for identifying risks.
   - What is the program's risk management process?

2. **Risk Identification** is discovering, defining, describing, documenting and communicating risks before they become problems and adversely affect a project.
   - What can go wrong?

3. **Risk Analysis** is to assess all the risks identified during the Identification step in order to determine their likelihood of occurrence and most probable impact.
   - What are the likelihood and consequence of the risk?

4. **Risk Handling** is the methodology used by the DoD to handle risk as part of the DoD Risk, Issue and Opportunity Management Process. Four options are recognized by the DoD for handling risks. These include: Risk Acceptance, Risk Avoidance, Risk Transfer, and Risk Mitigation.
   - Should the risk be accepted, avoided, transferred, or mitigated?

5. **Risk Monitoring** is the process that systematically tracks and evaluates the effectiveness of risk-handling actions against established metrics. Monitoring results may also provide a basis for developing additional handling options and identifying new risks.
   - How has the risk changed?
Aligning the Risk, Issue & Opportunity Management (RIOM) Guide with the DoD RMF
RMF and the DoD Acquisition Life Cycle

Cybersecurity and Acquisition Lifecycle Integration Tool (CALIT)

This tool is available at: https://dap.dau.mil/smart/.
1. Analysis of Alternatives
   a) Leverage ICD for Requirements
   b) Approaches (i.e. three)
      a) COTS
      b) COTS & Reuse with Integration
      c) Custom Development
   c) Red Team / Threat Representative input to support security control selection and TMRR Source Selection process

2. Develop key acquisition documents which include the Acquisition Strategy (AS), System Engineering Plan (SEP), Test and Evaluation Master Plan (TEMP), Program Protection Plan (PPP). Cybersecurity Strategy (CSS). These documents must be effectively integrated with each other to ensure an executable program.

3. Draft CDD - This key user document must include all cybersecurity and program protection requirements to ensure these requirements are integrated into the final design.

4. The Cybersecurity Working IPT (WIPT) is established in this phase. The Cybersecurity WIPT should be chaired by the program's WIPT.
Materiel Solution Analysis Phase Aligned to RMF Step 2

- Establish Cybersecurity IPT to execute the RMF Process
  - Conduct Step 1 – Categorize System
  - Conduct Step 2 – Select Security Controls

- Program Protection Key Processes:
  - System Engineering Plan
    - Defines the Systems Engineering (SE) organizational responsibilities for program protection planning
    - Calls for program protection updates as entrance criteria for each of the planned SE technical reviews
    - Schedule of Program Management Office (PMO) activities
  - Program Protection Plan
    - Summarizes the planned PMO’s security protection activities for protecting the system during design and development
    - Contains the results of the Program Protection Plan (PPP) analysis identifying the key elements of the program which require protection
    - Summarizes the System Requirements Document (SRD) and Statement of Work (SOW) system security requirements as protection measures

Test and Evaluation Master Plan
- Contains the verification and validation plan of the system security requirements.
- Defines the Systems Engineering (SE) organizational responsibilities for program protection planning
- Calls for program protection updates as entrance criteria for each of the planned SE technical reviews
- Schedule of Program Management Office (PMO) activities
Materiel Solution Analysis Phase – System Security Engineering (SSE)

- SSE incorporates the selected set of security requirements into the system requirements documentation and the Statement of Work (SOW) used for a Request for Proposal (RFP) and contract.

- There are three types of security requirements relevant to SSE:
  1. Protection measures that say what the system does are system security requirements included in the System Requirements Document (SRD) and referenced by the Program Protection Plan (PPP) and Test & Evaluation Master Plan (TEMP)
  2. Protection measures that specify how the contractor will develop the system are included in the SOW and referenced by the PPP
  3. Program Protection analysis activities necessary to continue to assess program and system security across the acquisition lifecycle are added to the Integrated Master Plan, SOW, and System Engineering and Management Plan
Materiel Solution Analysis Phase – System Security Engineering (SSE)

- Integrated system security requirements need contributions from all of the security engineering specialties:
  - 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.
  - Hardware Assurance (H/W A)
    - The level of confidence that hardware, e.g., electronic components such as integrated circuits and printed circuit boards, functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware throughout the life cycle.
  - Software Assurance (S/W A)
    - The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its life cycle and that the software functions in the intended manner.
  - Anti-tamper (A/T)
    - Systems engineering activities intended to prevent or delay exploitation of Critical Program Information (CPI) in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering.
  - Supply Chain Risk Management (SCRM)
    - The management of 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 (National Defense Authorization Act for Fiscal Year (FY) 2011, Section 806).
  - Defense Exportability Features
    - Efforts to develop and incorporate technology protection features into a system or subsystem during its research and development phase thus enabling availability of the capability to allies and other partners and reducing overall production cost.
Cybersecurity Test and Evaluation (T&E)

Testing is a key component of the DoD systems engineering process. Cybersecurity T&E is no different. To achieve acceptable Cybersecurity outcomes on DoD acquisition programs and systems, a robust Cybersecurity T&E effort is required. Cybersecurity T&E includes both Blue Team Testing (Vulnerability Assessment) and Red Team (Adversarial/Threat Representative) Testing

- **Blue Teams** conduct vulnerability assessments to:
  - Identify any/all known vulnerabilities present in systems
  - Reveal systematic weaknesses in the security program of a system
  - Focus on adequacy and implementation of technical security controls

  Vulnerability assessments are not a “one and done” event. Vulnerability assessments should be conducted throughout the acquisition lifecycle of a program to take into account changes in both system design and the threat.

- **Red Teams** conduct Adversarial (Threat Representative) testing:
  - Assess the ability of a unit equipped with a system to support its missions while withstanding validated and representative cyber threat activity
  - Exploit one or more known or suspected weaknesses
  - Develop an understanding of inherent weaknesses of a system
  - Address both internal and external threats

  In addition to assessing the effect on mission execution, the Operational Test Agency (Red Team) shall evaluate the ability to protect the system, detect threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity.

Cybersecurity T&E must be a key component of both the Test and Evaluation Master Plan (TEMP) and System Engineering Plan (SEP).

The DoD Cybersecurity Test & Evaluation Guidebook provides in-depth guidance and best practices for the acquisition workforce. The PM Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle—September 2015 has additional content regarding Cybersecurity T&E.
Technology Maturation & Risk Reduction Phase
Aligned to RMF Steps 2, 3, and 4

- **Acquisition**
  - Leverage Draft CDD
  - Influence Requirements
  - Develop Design Requirements
  - Release RFP
  - Conduct Competitive Prototyping
  - Conduct Developmental Testing
  - Blue Team Assessment
  - Conduct Preliminary Design Review

- **RMF**
  - Complete Step 2 – Select Security Controls
  - Conduct Step 3 – Implement Security Controls
  - Conduct Step 4 – Assess Security Controls
  - Initial Drafts of Security Assessment Report and POA&M.
  - Update Cybersecurity Strategy, Security Plan, and Monitoring Strategy
## TMRR Phase -- Coordination between the: Security Control Assessors -- Blue Team -- Red Team

<table>
<thead>
<tr>
<th>Security Controls Assessment Team</th>
<th>Vulnerability Assessment (Blue Team)</th>
<th>Threat Representative Testing (Red Team)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess compliance with security controls</td>
<td>Comprehensive</td>
<td>Exploit one or more known or suspected weaknesses</td>
</tr>
<tr>
<td>Execute the Security Assessment Plan</td>
<td>Identifies any/all known vulnerabilities present in systems</td>
<td>Attention on specific problem or attack vector</td>
</tr>
<tr>
<td>Linked to the Security Assessment Report Activities</td>
<td>Reveals systemic weaknesses in security program</td>
<td>Develops an understanding of inherent weaknesses of system</td>
</tr>
<tr>
<td>Based on STIGs or similar documentation</td>
<td>Focused on adequacy and implementation of technical security controls and attributes</td>
<td>Both internal and external threats</td>
</tr>
<tr>
<td>Can be determined by multiple methods: hands-on testing, interviewing key personal, etc.</td>
<td>Multiple methods used: hands-on testing, interviewing key personal, or examining relevant artifacts</td>
<td>Model actions of a defined internal or external hostile entity</td>
</tr>
<tr>
<td>Include a review of operational and management security controls</td>
<td>Feedback to developers and system administrators for system remediation and mitigation</td>
<td>Report at the end of the testing</td>
</tr>
<tr>
<td>Conducted with full knowledge and assistance of systems administrators, owner, and developer</td>
<td>Conducted with full knowledge and cooperation of systems administrators</td>
<td>Conducted covertly with minimal staff knowledge</td>
</tr>
<tr>
<td>No harm to systems</td>
<td>No harm to systems</td>
<td>May harm systems and components and require cleanup</td>
</tr>
</tbody>
</table>
Engineering & Manufacturing Development (EMD) Phase
Aligned to RMF Steps 3, 4, and 5

• Acquisition
  – Design System for Production & Test
  – Conduct Additional Red Team Assessment and Blue team Vulnerability Assessment
  – Develop Capabilities Production Document (CPD)

• RMF
  – Complete Step 3 – Implement Security Controls
  – Complete Step 4 – Assess Security Controls
  – Conduct Step 5 – Authorize System
  – Seek System Initial Authorization to Test (IATT)
  – Seek System Authorization
Production & Deployment Phase Aligned to RMF Steps 4, 5, and 6

• **ACQUISITION**
  – Produce, Test and Deploy System
  – Full Deployment Decision
  – Achieve Initial Operational Capability (IOC) & Full Operational Capability (FOC)

• **RMF**
  – Complete Step 4 – Assess Security Controls
  – Complete Step 5 – Authorize System
  – Conduct Step 6 – Monitor Security Controls
  – Update Security Plan, POA&M, and other RMF artifacts as necessary
Operations & Support Phase Aligned to RMF Step 6

- **ACQUISITION**
  - Support, Sustain and Dispose

- **RMF**
  - Continue Step 6 – Monitor Security Controls
  - Conduct Annual Review
  - Update Security Plan, POA&M, and other RMF artifacts as necessary
Questions Program Managers Can Ask to Determine if Cybersecurity is Integrated into Acquisition Programs

• Is cybersecurity integrated into solution architectures and is it aligned with enterprise/segment/reference architectures?
• Early in the lifecycle during requirements and architecture definition and design, has the developer and/or Chief Engineer/Lead Systems Engineer/SSE tried to model or assess the mission impact of cyber incidents (i.e., estimating mission impact by comparing model measures of effectiveness with and without the effects of different/evolving cyber attacks)?
• Did you appoint, in writing, an ISSM in accordance with the RMF?
• Did you establish a Cybersecurity Working Integrated Product Team (WIPT) during the MSA phase?
• Is the Cybersecurity Strategy coordination maintained and configuration controlled with other governing program documents?
• Have the Cybersecurity Strategy, capability requirements, Acquisition Strategy, and RMF Security Plan informed the RFP throughout the life cycle?
Questions Program Managers Can Ask to Determine if Cybersecurity is Integrated into Acquisition Programs

• Was preference given to the acquisition of COTS cybersecurity and cybersecurity-enabled products, which have been evaluated and validated as appropriate, to be used on systems entering, processing, storing, displaying, or transmitting national security information? Are current cybersecurity threats included in the PPP threat table?
• Is cybersecurity included in the program budget?
• Is software authorized and the current approved version with cybersecurity patches and service packs installed?
• Does the Cybersecurity Strategy describe:
  – The overarching technical approach to secure the system by applying the RMF throughout the acquisition life cycle (and its subsequent implementation)
  – How the program’s cybersecurity requirements are traced through the security controls and into the acquisition baselines and system design
  – How cybersecurity risk will be assessed and managed during the life cycle
  – Collaboration with the Authorizing Official to manage and maintain the system’s cybersecurity risk posture
Summary

• **Risk, Issue, Opportunity Management Process**
  – The cyclical 5 step risk management process provides a useful framework for understanding and dealing with any and all program risks including cybersecurity. It is the overarching risk management process for all DoD acquisition programs.

• **RMF in the DoD Acquisition Lifecycle**
  – The RMF brings a risk-based approach to the implementation of cybersecurity. Transition to the RMF leverages existing acquisition and systems engineering personnel and processes and the artifacts developed as part of existing systems security engineering (SSE) activities. Unlike a compliance-based checklist approach, the RMF supports integration of cybersecurity in the systems design process, resulting in a more trustworthy system that can dependably operate in the face of a capable cyber adversary.

Successful programs will emphasize integrating cybersecurity activities into existing processes including requirements, SSE, program protection planning, trusted systems and networks analysis, developmental and operational test and evaluation, financial management and cost estimating, and sustainment and disposal.
### DAU Cybersecurity Vision

*Enabling the Defense Acquisition Workforce to strengthen cybersecurity throughout the product lifecycle*

<table>
<thead>
<tr>
<th>Foundational Learning</th>
<th>Workflow Learning</th>
<th>Performance Learning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAWIA Career Field Training Courses (PM, IT, ACQ, TST, …)</td>
<td>Ask a Professor, Conferences, Articles, …</td>
<td>Mission Assistance (Existing MA, Business Development)</td>
</tr>
<tr>
<td>Continuous Learning (CLE 074, ISA 220, …)</td>
<td>Web Presence, On-line tools, Videos, …</td>
<td>Includes content consulting and workshops</td>
</tr>
<tr>
<td>Reinforces learning objectives within each competency</td>
<td>Provides timely and immediate information</td>
<td>Applied Subject Matter Expertise</td>
</tr>
</tbody>
</table>

*DAU hired 7 dedicated acquisition cybersecurity professionals beginning in August of 2015 (Enterprise Assets) Currently in the process of hiring an additional 4 cybersecurity professionals.*
Questions?

Derek Duchein
Cybersecurity Professor
Defense Acquisition University
Derek.Duchein@dau.mil

Or
Acquisition.CyberSecurity@dau.mil