



# Defense Acquisition University (DAU)

## Cybersecurity Black Card

January 2016

**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.**

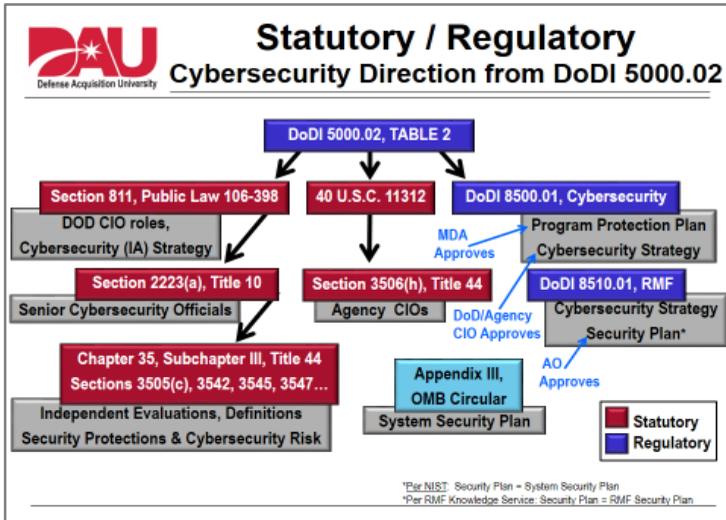
- DoDI 8500.01, 14 Mar 14



<p><b>Confidentiality</b></p> <p>Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.</p>	<p><b>Integrity</b></p> <p>The property whereby an entity has not been modified in an unauthorized manner.</p>	<p><b>Availability</b></p> <p>Being accessible and useable upon demand by an authorized entity.</p>	<p><b>Non-Repudiation</b></p> <p>Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity.</p>	<p><b>Authentication</b></p> <p>Verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.</p>
--	--	---	---	--

### Legislation, Policy and Guidance:

See DoD Cybersecurity Policy Chart: [http://iac.dtic.mil/csiaac/download/ia\\_policychart.pdf](http://iac.dtic.mil/csiaac/download/ia_policychart.pdf)



\*Per NIST: Security Plan = System Security Plan  
 \*Per RMF Knowledge Service: Security Plan = RMF Security Plan

### Operational Resilience - requires three conditions to be met:

1. information resources are trustworthy
  2. missions are ready for information resources degradation or loss
  3. network operations have the means to prevail in the face of adverse events
- DoDI 8500.01, 14 Mar 14

DAU Cybersecurity Website: <http://www.dau.mil/OtherProducts/pages/cybersecurity.aspx>  
 Acquisition Community Connection (ACC) Website: <https://acc.dau.mil/cybersecurity>

### Step 1 - Categorize System

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

### Step 2 - Select Security Controls

Identify and select security controls  
 Develop system-level continuous monitoring strategy  
 Review and approve RMF Security Plan & 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 RMF 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 (RMF Security Plan, SAR and POA&M) to Authorizing Official (AO)  
 AO conducts final risk determination and makes authorization decision

### Step 6 - Monitor Security Controls

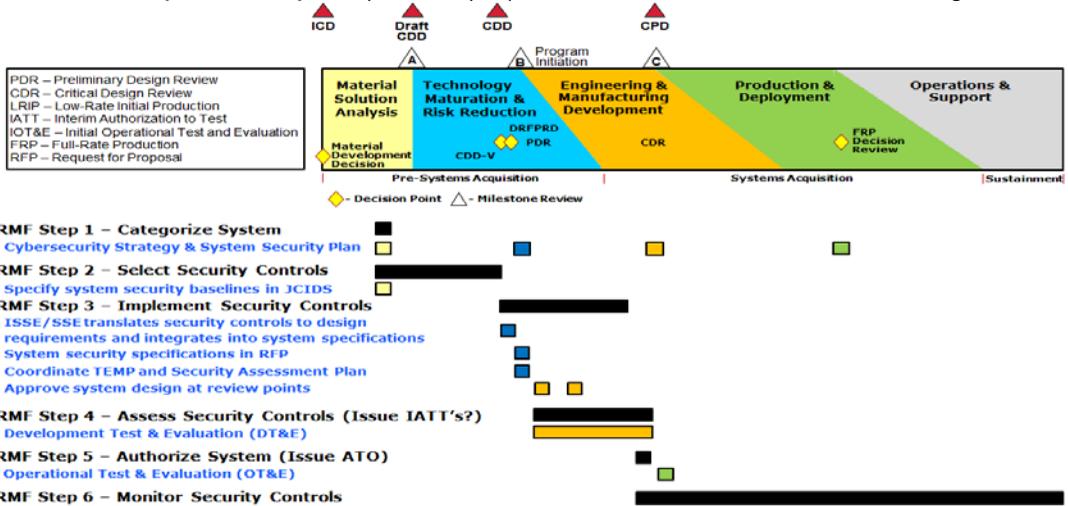
Determine impact of changes to the system and environment  
 Assess selected controls annually; conduct needed remediation  
 Update RMF Security Plan, SAR, and POA&M  
 Report security status to AO for review  
 Implement system decommissioning strategy

## Risk Management Framework Process



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

### RMF and the Acquisition Life Cycle - Cybersecurity requirements must be identified and included throughout



**RMF Step 1 - Categorize System**  
 Cybersecurity Strategy & System Security Plan

**RMF Step 2 - Select Security Controls**  
 Specify system security baselines in JCIDS

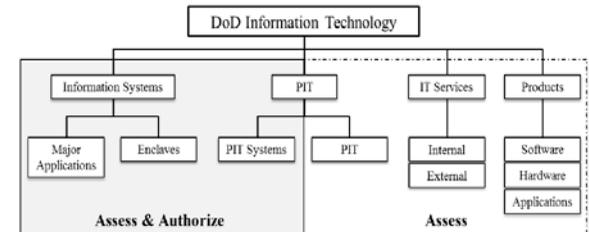
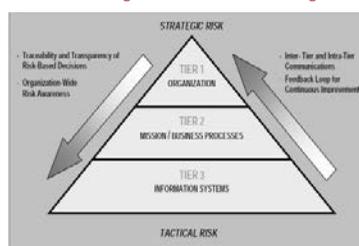
**RMF Step 3 - Implement Security Controls**  
 ISSE/SSE translates security controls to design requirements and integrates into system specifications  
 System security specifications in RFP  
 Coordinate TEMP and Security Assessment Plan  
 Approve system design at review points

**RMF Step 4 - Assess Security Controls (Issue IATT's?)**  
 Development Test & Evaluation (DT&E)

**RMF Step 5 - Authorize System (Issue ATO)**  
 Operational Test & Evaluation (OT&E)

**RMF Step 6 - Monitor Security Controls**

### Multi-tiered Organization-Wide Risk Management



Cybersecurity applies to all IT that receives, processes, stores, displays or transmits DoD information.

- DoDI 8500.01, 14 Mar 14

- NIST SP 800-39, Mar 11

