

# CYBERSECURITY CHALLENGES FOR DOD ACQUISITION PROGRAMS



Steve Mills DAU-South

[www.DAU.mil](http://www.DAU.mil)

# Overview

- **Questions**
- **Cybersecurity Owners and Stakeholders**
- **Cybersecurity – Why It Matters to DoD Program Managers**
  - **Defense Science Board Observations**
  - **Cybersecurity Policy Overview**
  - **Cybersecurity in the DoD Acquisition Lifecycle**
- **Sustainment vs Cybersecurity**
- **DAU CyberSecurity Courses**
- **Take Aways**
- **How DAU Can Help**

# Questions

- **“How vulnerable and resilient are DoD systems against the Cyber threat?”**
- **“Should Cybersecurity be treated as a design consideration in DoD acquisition programs?”**
- **“Who in the acquisition workforce needs to be involved in addressing the Cyber threat?”**

# Cybersecurity Owners & Stakeholders

G2 - Intel

It's Hacking!

It's Network Defense!

G3 - Ops

PM

SE

G6 - CIO

Cybersecurity is Operational!

It's Electronic Warfare!

It's Program Protection!

Cybersecurity

IT

T&E

LOG

CON



# 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.”

Source: DoD Defense Science Board  
*Task Force Report: Resilient Military Systems and the  
Advanced Cyber Threat. (January 2013)*

# DoDI 8500.01 – Cybersecurity

- Adopts the term “**Cybersecurity**” in lieu of “**Information Assurance**”
- Extends applicability to all DoD information technology processing DoD information
- 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

# 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**

# 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
- Enclosure 8 defines the timeline to transition from DIACAP to RMF

# 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**

# Cybersecurity & DoDI 5000.02

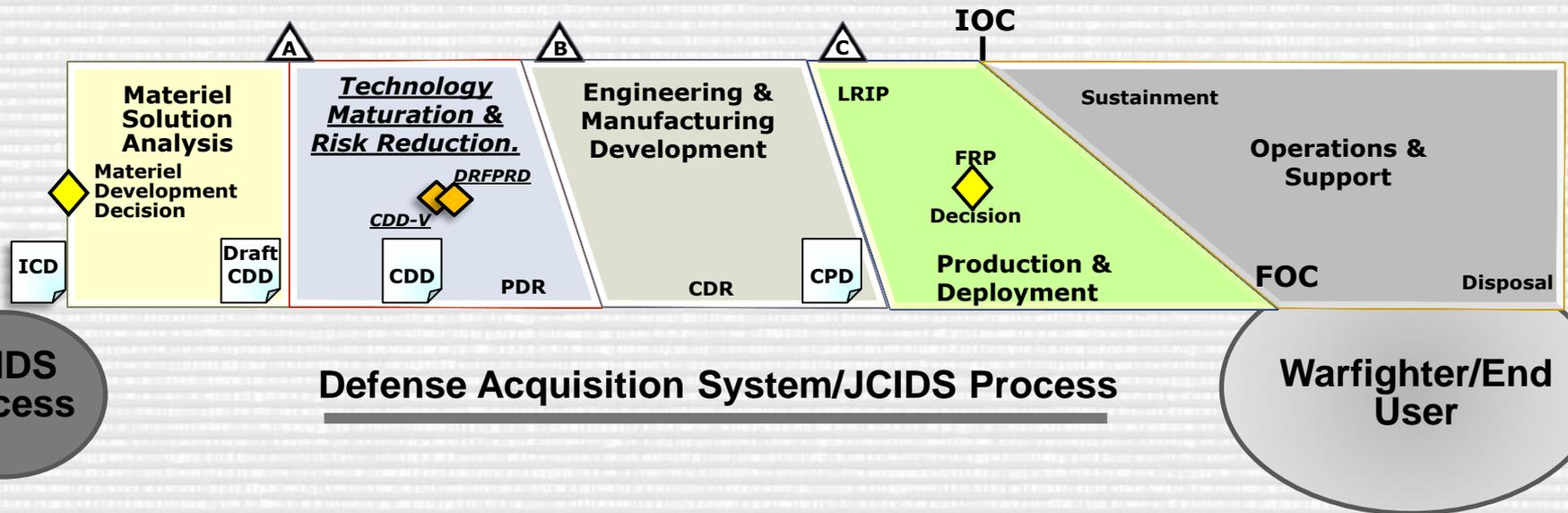
- “**Prevention** of damage to, **protection** of, and **restoration** of computers, electronic communications systems,...wire communication, and electronic communication, including information contained therein...” DoDI 8500.01
- Required by DoDI 5000.02 – Enclosure 11, Section 6. Cybersecurity
  - “All acquisitions of systems containing IT...will have a Cybersecurity Strategy.”
  - “**Beginning at Milestone A**, the PM will submit the Cybersecurity Strategy...”
  - “**STATUTORY for all programs containing IT**, including NSS.”
- Also cited in DODI 5000.02 - Table 9. Clinger-Cohen Act
  - “Ensure that the program has a Cybersecurity Strategy that is consistent with DoD policies, standards and architectures...”

- **Cybersecurity = Everything that processes 1's and 0's. This is new!**
- **Cybersecurity effort spans the entire acquisition process**
- **A “team sport” with impacts to all Acquisition Career Fields**



# Cybersecurity in the DoD Acquisition Lifecycle

## Model 1: Hardware Intensive Program

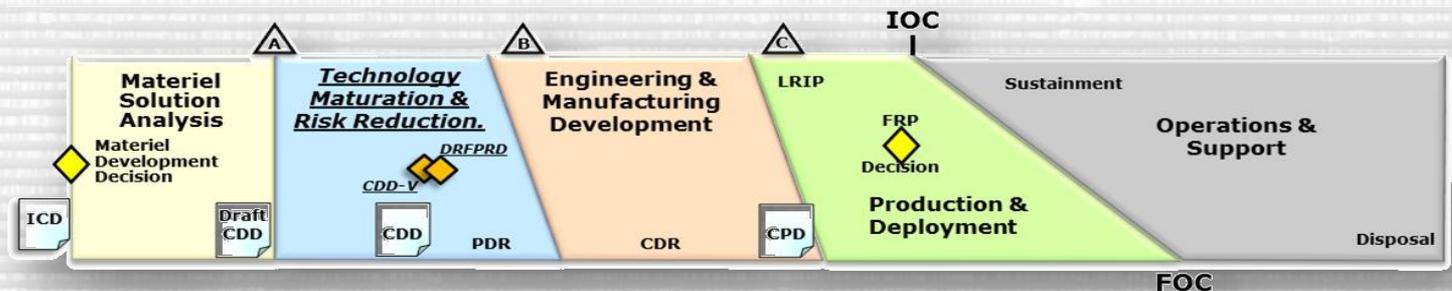


To achieve positive acquisition outcomes, we must consistently “bake in” Cybersecurity into our acquisition programs

# Cybersecurity in the DoD Acquisition Lifecycle

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.

Cybersecurity Integration: Cybersecurity must be fully integrated into system life cycles so that it will be a visible element of organizational, joint, and DoD Component architectures, capability identification and development processes, integrated testing, information technology portfolios, acquisition, operational readiness assessments, supply chain risk management, SSE, and operations and maintenance activities.



# Cybersecurity and BBP 3.0

- Vision Statement for BBP 3.0
  - Achieving Dominant Capabilities through Technical Excellence and Innovation
    - *Cybersecurity is a design consideration and a key enabler of this vision*
- Key BBP 3.0 goals related to Cybersecurity
  - Anticipate and plan for responsive and emerging threats
    - *There is no greater emerging threat to DoD acquisition programs than Cybersecurity*
  - Strengthen organic engineering capabilities.
    - *To be effective, Cybersecurity must be “baked in” as part of the design process*
  - Improve our leaders’ ability to understand and mitigate technical risk.
    - *Cybersecurity can be the greatest technical risk that programs face*

# Sustainment Vs. Cybersecurity

## Sustainment

- Recognized activity spanning the entire acquisition lifecycle
- Represents significant program risk(s)
- Impacts most/all functional areas
- Significant tactical & operational impacts
- Sustainment is a design consideration:
  - Design Interface
  - Sustainment Engineering
- Management Approach
  - IAW with FY 2010 NDAA / PL 111-84
  - Mandated Plan – Life Cycle Sustainment Plan (LCSP)
  - Validated Measurement – Sustainment KPP
  - Mandated Plan Owners
    - Product Support Manager (PSM)
    - Product Support Integrator (PSI)

## Cybersecurity

- Recognized activity spanning the entire acquisition lifecycle – **Not yet!**
- Represents significant program risk(s) – **not being addressed yet by many**
- Impacts most/all functional areas
- Significant tactical & operational impacts
- **Cybersecurity should be a design consideration!**
  - **Design Interface**
  - **Sustainment Engineering**
- Management Approach
  - IAW SEC. 811, P.L. 106-398
  - Mandated Plan – **Cybersecurity Strategy is requirement, but not a “plan”**
  - Validated Measurement – **None**
  - Mandated Plan Owners
    - **No designated owner**
    - **Everyone has a part in cyber**

**Cybersecurity represents a significant gap in the acquisition lifecycle**

# Take Aways

- DSB observations paint a grim picture of our current Cybersecurity posture
- *Cybersecurity applies to all systems or subsystems that process 1's and 0's*
- Cybersecurity is not just the network. It is part of the DNA of an acquisition program
- All acquisition career fields have a piece of Cybersecurity
- Industry Partners are a critical component of your cybersecurity efforts. They design and build our products!
- Cybersecurity is a design consideration which must be addressed throughout the entire acquisition lifecycle

# DAU Cybersecurity Courses

- DAU is developing a Cybersecurity Online Course
  - Covers the RMF and Cybersecurity across acquisition career fields. Available CY15
  
- DAU is developing a 100-level Program Protection (PP) Planning Online Course
  - Cybersecurity one element of PP. Available late CY14
  
- DAU is developing a 200-level PP Planning Classroom Course
  - Cybersecurity one element of Program Protection. Available mid CY15
  
- DAU is developing a 200-level RMF Online Course
  - Available late CY15

# How DAU Can Help

- Ask A Professor (<https://dap.dau.mil/aap/pages/pqsubmit.aspx>) –
- Contact DAU directly for :
  - Tailored Assistance
  - Targeted Training such as:
    - Seminar – Cybersecurity Challenges for DoD PMs
    - Seminar – Risk Management Framework (RMF)
    - Seminar – Cybersecurity Testing in DoD Acquisition
- DAU Capital & Northeast (Ft. Belvoir, VA) Karen Currey (703) 805-4978
- DAU Mid-Atlantic (California, MD) Mike Paul (240) 895-7363
- DAU Midwest (Kettering, OH) Vishnu Nevekar (937) 781-1029
- DAU South (Huntsville, AL) Jack Cain (256) 922-8731
- DAU West (San Diego, CA) Rob Tremaine (619) 524-4811

