

CYBERSECURITY CHALLENGES FOR DOD ACQUISITION PROGRAMS



Steve Mills
Professor of Information Technology
Steve.mills@dau.mil
256.922.8761

www.DAU.mil

Overview

- **Cybersecurity Policy Overview**
- **Questions**
- **Challenge #1 - Cybersecurity Owners and Stakeholders**
- **Challenge #2 - Cybersecurity Performance of DoD Programs**
- **Challenge #3 - Integrating Cybersecurity into the DoD Acquisition Lifecycle**
- **Recommendations**
- **Final Thoughts**
- **How DAU Can Help**

Cybersecurity Policy Overview

DoDI 8500.01 – Cybersecurity

- Signed Mar 14, 2014
- 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 NIST SP 800-53 Security Control Catalog
- Incorporates Cybersecurity early and continuously throughout the acquisition lifecycle

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

- Signed Mar 12, 2014
- 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/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

Cybersecurity & DoDI 5000.02

- **Cybersecurity:** “Prevention of damage, 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 = All DoD IT is included. Not just the network!**
- **Cybersecurity effort spans the entire acquisition process**
- **A “team sport” with impacts to all Acquisition Career Fields**

Cybersecurity in Acquisition Research Efforts

- Defense Science Board (DSB) Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. (January 2013)
- Ongoing DSB Studies on Cybersecurity:
 - DSB Task Force on **Cyber Defense** (Oct 09, 2014)
 - DSB Task Force on **Cyber Deterrence** (Oct 09, 2014)
 - DSB Task Force on **Cyber Supply Chain** (Nov 12, 2014)
- Sponsor of ongoing studies is Mr. Frank Kendall, USD AT&L

Questions

- **“Who in the acquisition workforce needs to be involved in addressing the Cyber threat?”**
- **“How vulnerable and resilient are DoD systems against the Cyber threat?”**
- **“How well is Cybersecurity integrated into the DoD Acquisition Lifecycle?”**



Challenge #1
Cybersecurity Stakeholders

Cybersecurity Stakeholders

J2 - Intel

It's Hacking!

It's Network Defense!

J3 - Ops

PM

SE

J6 - CIO

Cybersecurity is Operational!

It's Electronic Warfare!

It's Program Protection!

Cybersecurity

IT

T&E

LOG

CON





Challenge #2
Cybersecurity Performance
of DoD Programs

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)**

DOT&E FY 2014 Annual Report

- “Cyber adversaries have become **as serious a threat** to U.S. military forces as the air, land, sea and undersea threats represented in operational testing for decades”
- “Program managers worked to resolve vulnerabilities found from cybersecurity testing in prior years, **but FY-14 testing revealed new vulnerabilities.**“
- “Cyber Opposition Forces (OPFOR) portraying adversaries with beginner or intermediate cyber capabilities were able to demonstrate that **many DOD missions are currently at risk from cyber adversaries**”
- “Demand has begun to **exceed the capacity of existing personnel** able to portray cyber threats.”

2 years later – Things are not getting better!!

**Source: DOT&E FY 2014 Annual Report
(January 2015)**



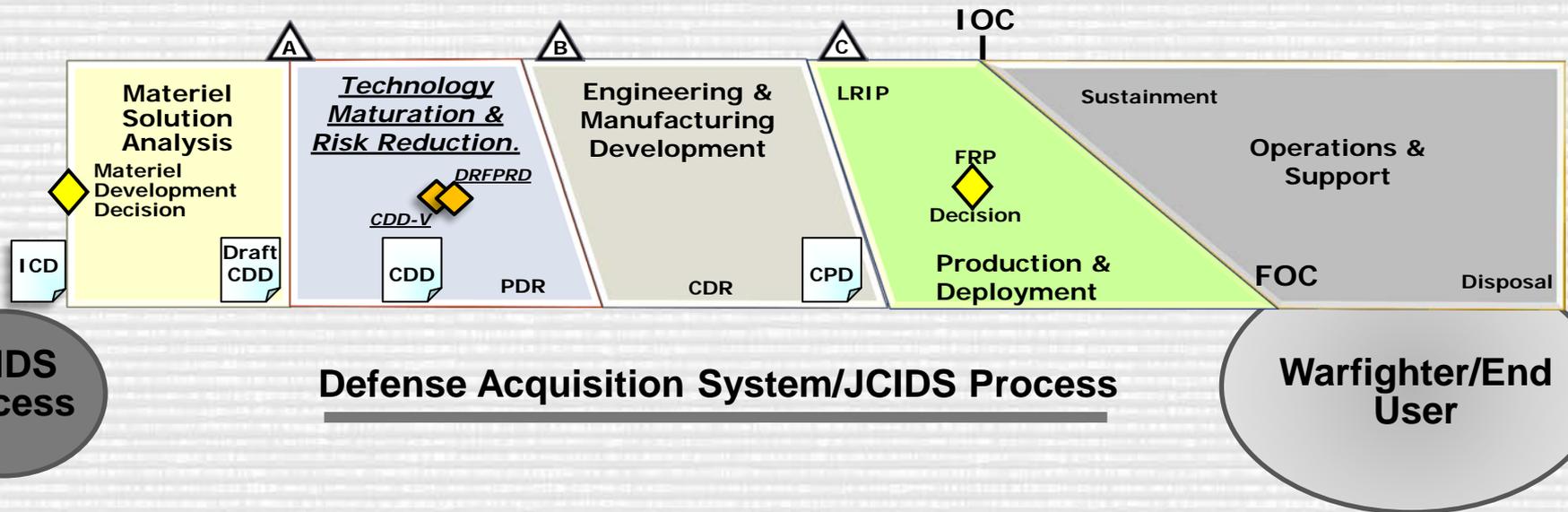


Challenge #3

Integrating Cybersecurity into the DoD Acquisition Lifecycle

Cybersecurity in the DoD Acquisition Lifecycle

Model 1: Hardware Intensive Program

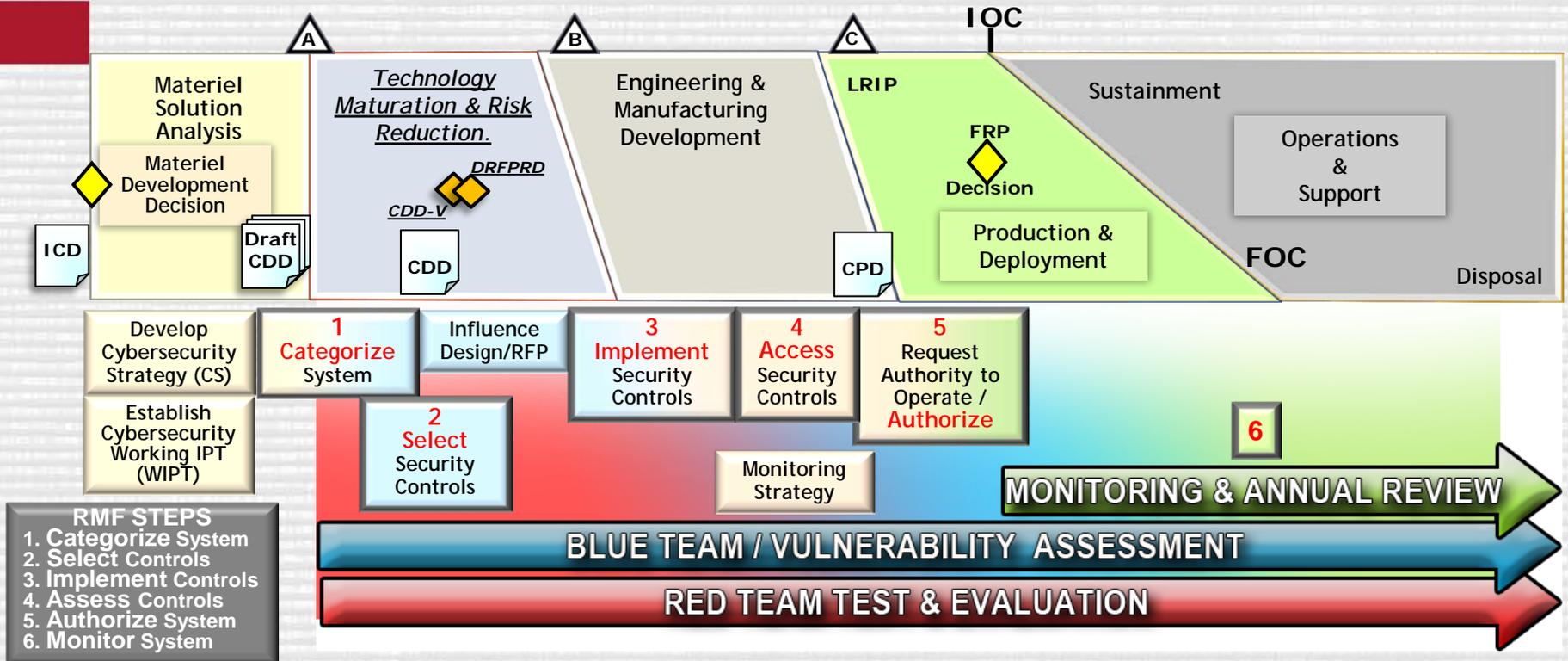


To achieve positive acquisition outcomes,
we must consistently “bake in”
Cybersecurity into our acquisition programs

Measuring Cybersecurity

- “How should Cybersecurity be Measured?”
 - Common Vulnerabilities and Exposures (CVE) approach?
 - Operational Resilience approach?
- How can we “bake in” Cybersecurity into our DoD systems without a standard way to measure it?
 - Linkage exists between measurement and the SE process
- What are the C/S/P impacts of Cybersecurity on our DoD systems ?
 - Many PMs consider Cybersecurity an “unfunded requirement”
 - How important is Cybersecurity to the key stakeholders who have numerous priorities?

Integrating Cybersecurity across the Acquisition Lifecycle



- Effective Cybersecurity in DoD acquisition programs encompasses all of the actions taken to ensure the Confidentiality, Integrity and Availability (CIA) of the system
- PMs should integrate cybersecurity into the system's acquisition lifecycle activities, e.g., SEP, TEMP, PPP, Cybersecurity Strategy and Source Selection processes

Cybersecurity "Shift Left" approach will yield better acquisition outcomes

Recommendations

- DoD needs to develop an accurate way to measure Cybersecurity
 - Cybersecurity KPP?
- Cybersecurity should be treated as a design consideration and recognized as a key component of the System engineering effort
- Cybersecurity must be integrated into the Acquisition Strategy, SEP, TEMP, and LCSP
 - May require some type of forcing function to ensure compliance
- A Cybersecurity “Champion” is needed to effectively synchronize Cybersecurity efforts across the acquisition lifecycle of DoD programs
 - AMRDEC Cyber Integrator Pilot Program
 - Product Support Manager approach

Cybersecurity – Final Thoughts

- Cybersecurity is not just the network. It is part of the DNA of an acquisition program
- Cybersecurity threats cannot be totally mitigated. You must manage the risk
- Your Cybersecurity effort must be synchronized across your acquisition program (PPP, Cybersecurity Strategy, Security Plan, TEMP & SEP)
- The PM must work the people side – Reward and encourage your Cybersecurity heroes!
- Industry Partners are a critical component of your Cybersecurity efforts. They design and build our products!
- Communicate across systems and functional boundaries. Cybersecurity requires everyone's energy and expertise
- Take every opportunity to educate and train your team – Cybersecurity is a moving target

How DAU Can Help – DAU Cybersecurity Courses

- DAU Course offerings and availability dates:
 - ***Cybersecurity Throughout DoD Acquisition*** (CLE 074)
 - Covers Cybersecurity across acquisition career fields. Available CY15

 - ***Risk Management Framework (RMF) Implementers Course*** (ISA220) - Available CY16

 - Cybersecurity content being incorporated into all career fields

How DAU Can Help (cont.)

- **Contact DAU directly** for :
 - Content Consulting/Tailored Assistance
 - Targeted Training such as:
 - Seminar – Cybersecurity Challenges for DoD PMs
 - Seminar – Risk Management Framework (RMF)
 - Seminar – Cybersecurity Testing in DoD Acquisition
- DAU POCs for Cybersecurity Outreach and Mission Assistance:
 - **Steve Mills (256) 922-8761**
 - **Tim Denman (256) 922-8174**