

BBP 3.0

3 NEW INITIATIVES FOR CONTROLLING COSTS THROUGHOUT THE PRODUCT LIFECYCLE



George Cash

Professor of Cost Estimating

george.cash@dau.mil



3 NEW INITIATIVES FOR CONTROLLING COSTS

PERSPECTIVE

BBP 3.0 retains many of the “core” initiatives from 1.0 and 2.0, such as affordability caps and should cost targets.

BBP 3.0’s new initiatives focus on our products and their ability to provide military technological superiority.

BBP 3.0

THE LIFE CYCLE COST MISSION AREA

Achieve Dominant Capabilities While Controlling Lifecycle Costs

- **Strengthen and expand should-cost based management**
- **Anticipate and plan for responsive and emerging threats by building stronger partnerships of acquisition, requirements and intelligence communities**
- **Institutionalize stronger DoD level Long Range R&D Program Plans**
- **Strengthen cybersecurity throughout the product lifecycle**



BUILD STRONGER PARTNERSHIPS

**Between Acquisition, Intelligence and
Requirements Communities**





IMPLEMENTING GUIDANCE CRITICAL INTELLIGENCE PARAMETERS

A key aspect linking the A-I-R communities

Communities must work together to identify CIPs

**CIP threshold breach is an indication of adversary's
potential to overcome our capability**

May lead to a change in our requirements

CRITICAL INTELLIGENCE PARAMETERS

WHAT ARE THEY? WHY ARE THEY IMPORTANT?

Key features (parameters) of an adversary's capability to neutralize our own capability

- **CIP thresholds and objectives relate to the level a parameter would need to reach to be of concern**
- **The PM, in partnership with the Intelligence Community (IC), identifies CIPs early on**
- **Setting CIP thresholds and objectives enables the IC to collect and analyze threat data more efficiently**
- **Allows system engineers to reduce the design margins around at-risk components**
- **Reduces cost to the Acquisition Community by avoiding large design margins to account for unknown threat changes**

Critical Intelligence Parameters in Context

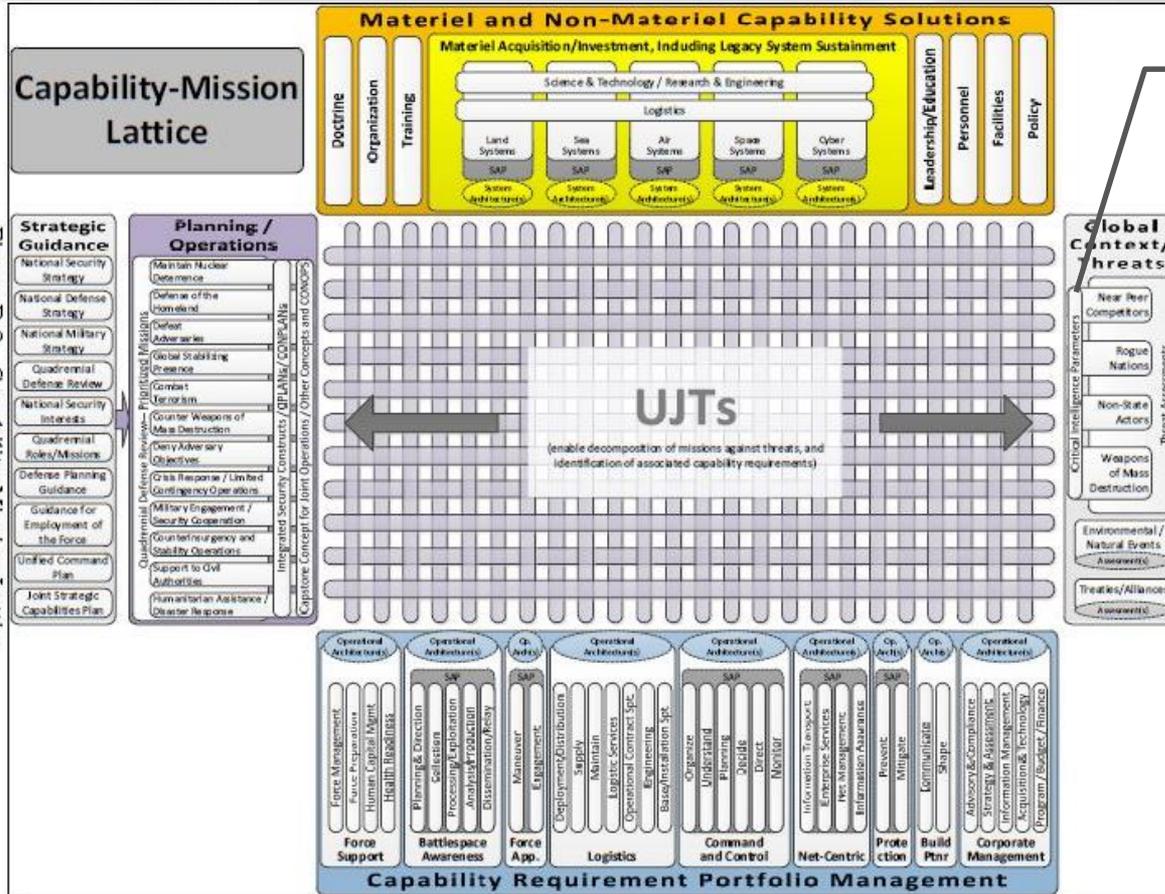


Figure B-2. Capability-Mission Lattice

Critical Intelligence Parameters



CRITICAL INTELLIGENCE PARAMETERS BREACH REVIEW

An assessment of the relationship between a changing CIP and the related performance attributes for one or more of our capability solutions

A risk mitigation team—comprised of program office, capability sponsor, capability developer, FCB representatives, and other stakeholders—conducts the review

If the supporting military Service Intelligence Center determines a CIP has been breached, they will notify the appropriate DoD offices , program office(s) and FCB(s)

The purpose of the CIP breach review is to:

- Determine whether changes in an adversary's capabilities threaten mission effectiveness of current or future capability solution(s)
- Determine if the CIP breach impacts other capability solutions across the capability portfolio
- Determine appropriate responses and/or risk mitigation efforts to balance operational risk and cost and any potential non-materiel and materiel changes

THE PROGRAM MANAGER AND THE IC

MAJOR THINGS TO KNOW

- **Identify an intelligence liaison officer**
- **Request an in-depth briefing on both the threat baseline and on the CIPs for the program**
- **Determine if your program is working off a Validated Online Life-cycle Threat (VOLT) or off of a System Threat Assessment Report**
- **Get involved with the digital threat assessment pilots**

From “Integrating Intelligence and Acquisition to Meet Evolving Threats, Defense AT&L: May-June 2015





Institutionalize Stronger DoD Level Long-Range R&D Plans



INSTITUTIONALIZE STRONGER DOD LEVEL LONG-RANGE R&D PLANS

- **Challenges**

- U.S. faces a potential loss of technological superiority in light of threat investments
- Threats have studied U.S. warfighting strengths and weaknesses and have identified effective countermeasures (e.g., global investments in Anti-Access/Area Denial Capabilities, Electronic Warfare Modernization, etc.)
- Responding symmetrically to threat investments has limited value and imposes significant cost on U.S.
- Current DoD R&D planning is largely focused on mapping investments to critical technology areas; limited, focused investments on high-value game changers that challenge current operational concepts

- **BBP 3.0 Opportunity**

- Initiate a DoD-level long-range plan to provide strategic R&D investment guidance (similar to that conducted in the 1970s) focused on identifying and accelerating enabling R&D that may lead to innovative capability concepts that:
 - Offer significant warfighting advantage over current capabilities
 - Provide asymmetric advantages over potential threat capabilities
 - Allow the U.S. to cost-effectively shape the trajectory of future military materiel competition

DEFENSE INNOVATION INITIATIVE (DII)



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

NOV 15 2014

MEMORANDUM FOR DEPUTY SECRETARY OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
CHIEF OF THE NATIONAL GUARD BUREAU
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: The Defense Innovation Initiative

I am establishing a broad, Department-wide initiative to pursue innovative ways to sustain and advance our military superiority for the 21st Century and improve business operations throughout the Department. We are entering an era where American dominance in key warfighting domains is eroding, and we must find new and creative ways to sustain, and in some areas expand, our advantages even as we deal with more limited resources. This will require a focus on new capabilities and becoming more efficient in their development and fielding.

At a time of constrained and uncertain budgets, the demand for innovation must be Department-wide and come from the top. Accordingly, I am directing Deputy Secretary of Defense Bob Work to oversee this effort. He will report back to me quarterly on progress we have made, and I will remain actively involved in overseeing all aspects of this effort.

We have always lived in an inherently competitive security environment and the past decade has proven no different. While we have been engaged in two large land mass wars over the last thirteen years, potential adversaries have been modernizing their militaries, developing and proliferating disruptive capabilities across the spectrum of conflict. This represents a clear and growing challenge to our military power.

I see no evidence that this trend will change. At the same time, downward fiscal pressure will constrain the way we have traditionally addressed threats to our military superiority and demand a more innovative and agile defense enterprise. We must take the initiative to ensure that we do not lose the military-technological superiority that we have long taken for granted.



OSD013411-14

Secretary of Defense Chuck Hagel's November 15, 2014 memo, "The Defense Innovation Initiative" directs:

"A new long-range research and development planning program will identify, develop, and field breakthrough technologies and systems that sustain and advance the capability of U.S. military power."

BACKGROUND

We've accomplished this before. In the 1950s, President Eisenhower successfully offset the Soviet Union's conventional superiority through his New Look build-up of America's nuclear deterrent. In the 1970s, Secretary of Defense Harold Brown, working closely with Under Secretary – and future Defense Secretary – Bill Perry, shepherded their own offset strategy, establishing the Long-Range Research and Development Planning Program that helped develop and field revolutionary new systems, such as extended-range precision-guided munitions, stealth aircraft, and new intelligence, surveillance, and reconnaissance platforms.

Remarks by Secretary Chuck Hagel
Reagan National Defense Forum
November 15, 2014



LONG-RANGE R&D PLAN (LRRDP) APPROACH

Identify high-payoff enabling technology investments that could:

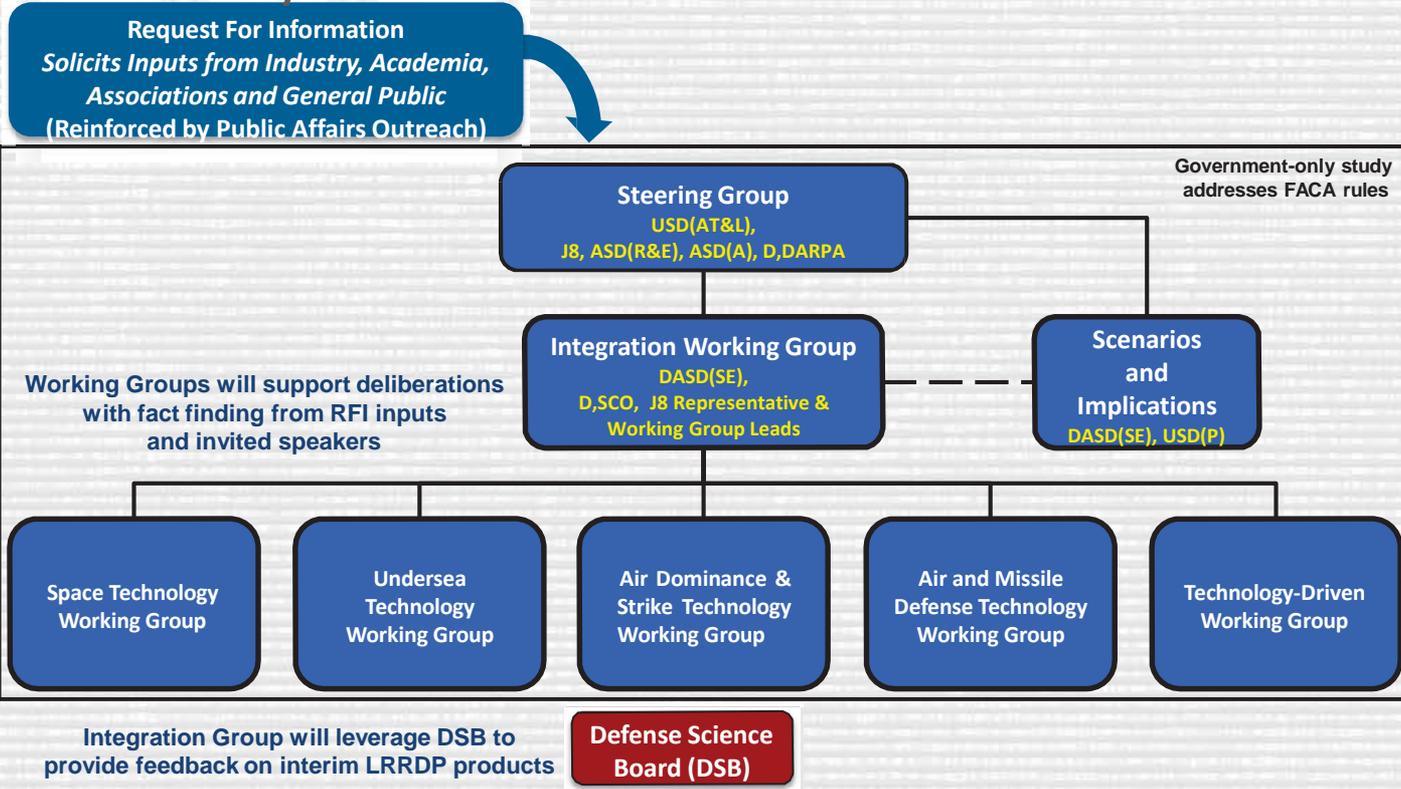
- Provide an opportunity to shape key future US materiel investments
- Offer opportunities to shape the trajectory of future competition for technical superiority, and
- Will focus on technology that can be moved into development programs within the next five years.

<http://www.defenseinnovationmarketplace.mil/LRRDP.html>



LRRDP ORGANIZATION

LRRDP Study Structure



LRRDP RFI APPROACH

- **Five focus areas**

1. Space Technologies
2. Undersea Technologies
3. Air Dominance and Strike Technologies
4. Air and Missile Defense Technologies
5. Technology-Driven Concepts

- **Submissions**

- Abstracts accepted from general public describing specific technologies and use cases or implementation concepts
- Will accommodate both unclassified and classified abstracts

- **Timeline**

- Initial close out 45 days after RFI release
- Monthly rolling close outs every 30 days thereafter until April



JOIN THE BBP 3.0 DISCUSSION

We Want Your Feedback:
<https://www.betterbuying3.com/>

**Better Buying Power
Website for past and
current BBP resource
materials:**
<http://bbp.dau.mil>

Join our conversation:
OSD.ATL.BBP@mail.mil



BETTER BUYING POWER 3.0 CONTROLLING COSTS WITH BETTER CYBERSECURITY



Steve Mills
DAU South Cyber Lead
Steve.mills@dau.mil
256.922.8761

www.DAU.mil

Overview

- **Cybersecurity in DoD Weapons Systems**
- **Controlling Cost through effective Cybersecurity**
 - **Recognize Cybersecurity as a “Design Consideration”**
 - **Integration of multiple complex processes (RMF & DoD Acquisition Lifecycle)**
 - **Other Challenges**
- **DAU’s “Full Duplex” Cybersecurity Support to our customers**

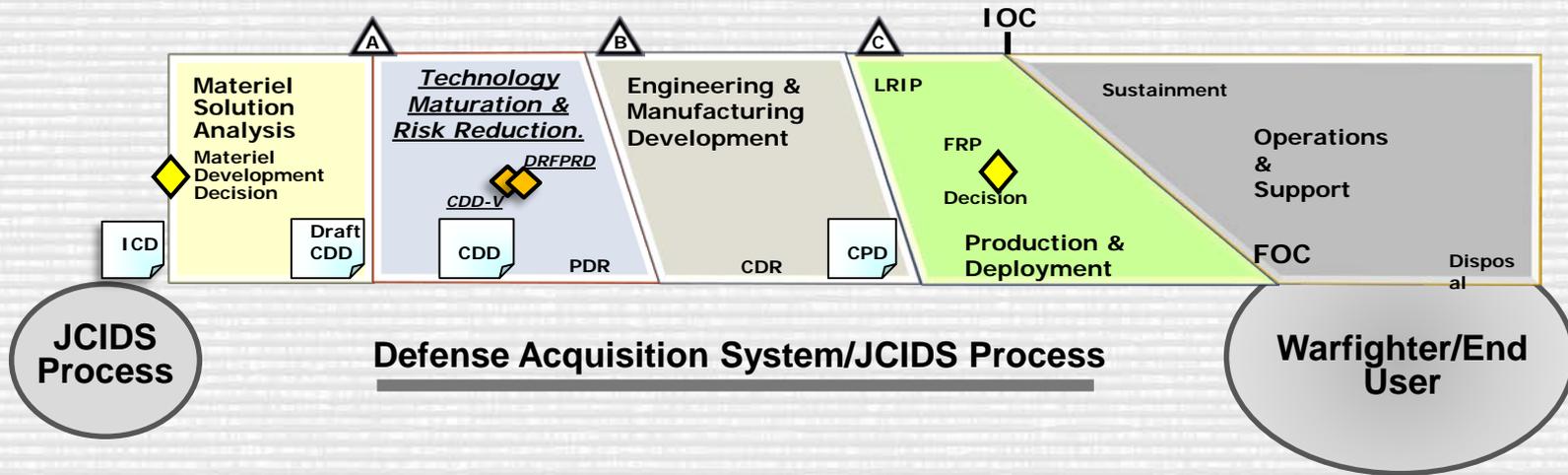


Cost Challenge #1

**Failure to Recognize Cybersecurity as a
“Design Consideration”**

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

Integrating Cybersecurity into our Acquisition Programs

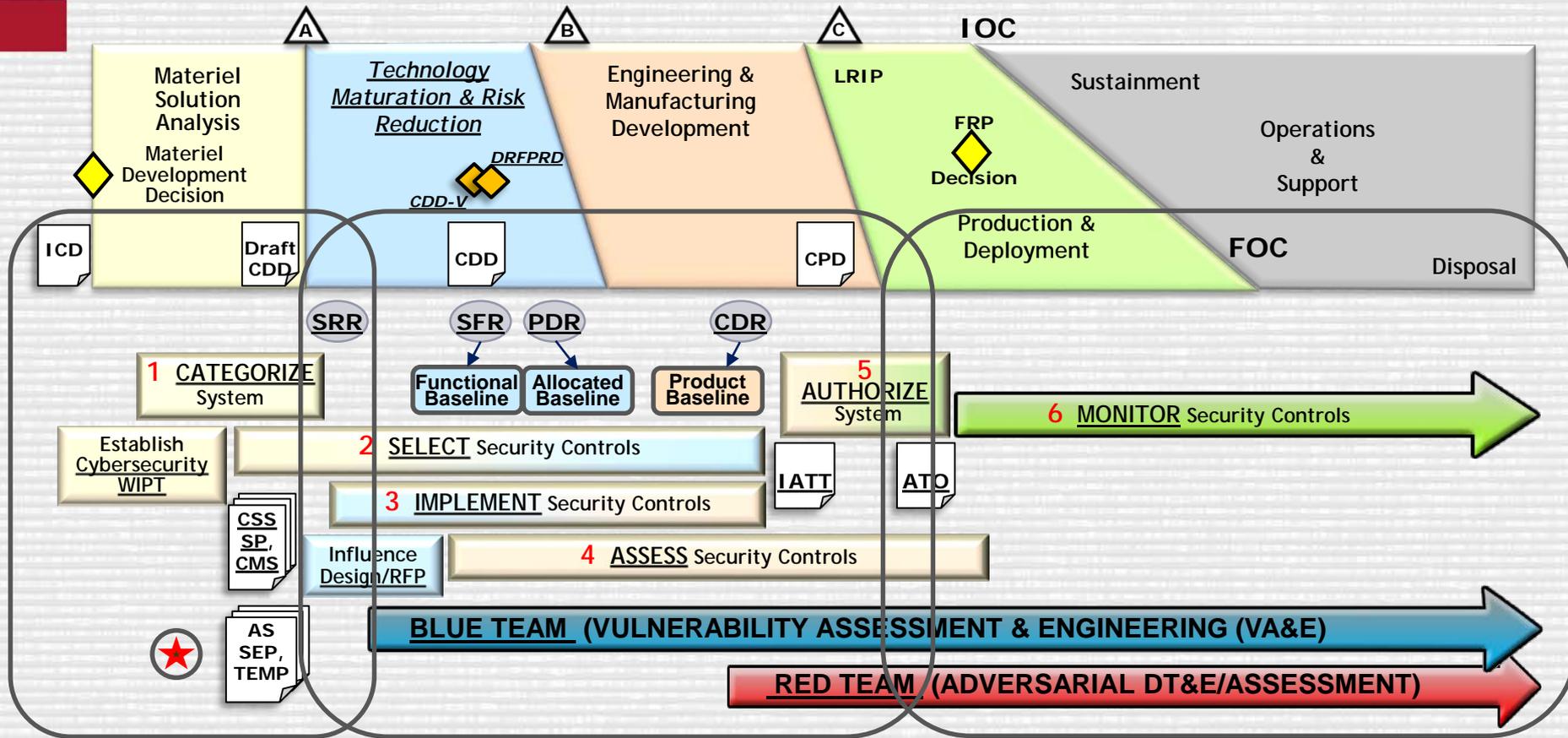
- **How effective has DoD been to date on integrating Cybersecurity into our acquisition programs?**
 - DoD consistently “bolts on” Cybersecurity later in the design process at great cost while achieving marginal results (FY2014 DOT&E Report)
 - Without a new/different approach we can expect similar or worse results
- **Could ensuring Cybersecurity is part of the design process improve results?**
 - Leaders and Team members (Gov’t & Industry) must make this a priority
- **Some keys to success:**
 - Treat Cybersecurity as a true design consideration – “Design for Cybersecurity”
 - This is already done for supportability/sustainability, why not for Cybersecurity?
 - Get leadership on board early – Cybersecurity impacts overall program risk!
 - Get the entire team on board – Cybersecurity is a “team sport”
 - Ensure your Industry Partner(s) have a solid track record on Cybersecurity
 - Use Cybersecurity in the Source Selection process (Past Performance, etc) to help to differentiate among the offerors
 - Develop and incorporate Cybersecurity related contract language to get better results



Cost Challenge #2

Integration of the RMF & DoD Acquisition Lifecycle

Cybersecurity/RMF Integration across the Acquisition Lifecycle



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?



Other RMF Implementation Challenges

- 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
 - # of Cybersecurity workforce
 - Keeping Cybersecurity talent

How DAU Can Help

- **DAU is a “full duplex” organization** – We listen to our customers to ensure we understand your challenges and to learn about how to better meet your needs – This is especially true when it concerns Cybersecurity.
- **Education**
 - Student Centered learning + skilled listening
 - Every customer engagement is an opportunity for DAU to learn
- **Collaboration** - We are members of our local community and pride ourselves in supporting you
- **Execution** – We do Mission Assistance! It one of our core competencies. We help our customers solve their acquisition challenges at the point of need
- **Expertise** – We are investing in our Cybersecurity expertise – Cybersecurity new hires



Questions?

Steve Mills
DAU South Cyber Lead
Steve.mills@dau.mil
256.922.8761

