ITEA
2nd Cyber Security Workshop
"T&E to meet the Advanced Persistent Threat"

Dr. C. David Brown, PE, CTEP
DASD(DT&E) / Director, TRMC

February, 2015

Agenda

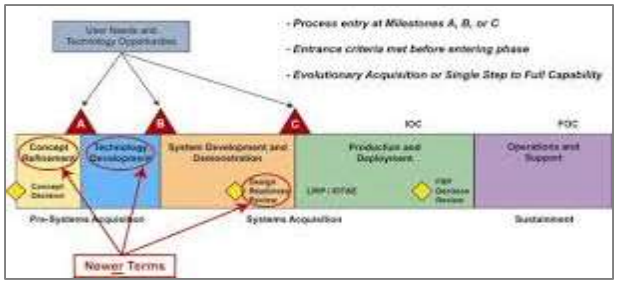
- Inside the Beltway
- DoD Cyber Policy
- AT&L Cyber Guidance and Resources
- Vision and Challenge

Inside the Beltway

New SecDef

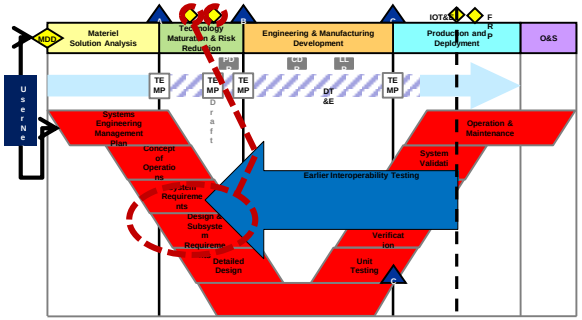
DoD Budget submission

New DoDI 5000.02



BBP 3.0 underway

Shift Left Implementation



Cyber

Better Buying Power 3.0

Achieving Dominant Capabilities through Technical Excellence and Innovation

Achieve Affordable Programs
- Continue to set and enforce affordability caps

Achieve Dominant Capabilities While Controlling Lifecycle Costs
- Strengthen and expand "should cost" based cost management
- Build stronger partnerships between the acquisition, requirements, and intelligence communities
- Anticipate and plan for responsive and emerging threats
- Institutionalize stronger DoD level Long Range R&D Planning

Incentivize Productivity in Industry and Government
- Align profitability more tightly with Department goals
- Employ appropriate contract types, but increase the use of incentive type contracts
- Expand the superior supplier incentive program across DoD
- Increase effective use of Performance-Based Logistics
- Remove barriers to commercial technology utilization
- Improve the return on investment in DoD laboratories
- Increase the productivity of IRAD and CR&D

Incentivize Innovation in Industry and Government
- Increase the use of prototyping and experimentation
- Emphasize technology insertion and refresh in program planning
- Use Modular Open Systems Architecture to stimulate innovation
- Increase the return on Small Business Innovation Research (SBIR)
- Provide draft technical requirements to industry early and involve industry in funded concept definition to support requirements definition
- Provide clear "best value" definitions so industry can propose and DoD can choose wisely

Eliminate Unproductive Processes and Bureaucracy
- Emphasize Acquisition Executive, Program Executive Officer and Program Manager responsibility, authority, and accountability
- Reduce cycle times while ensuring sound investments
- Streamline documentation requirements and staff reviews

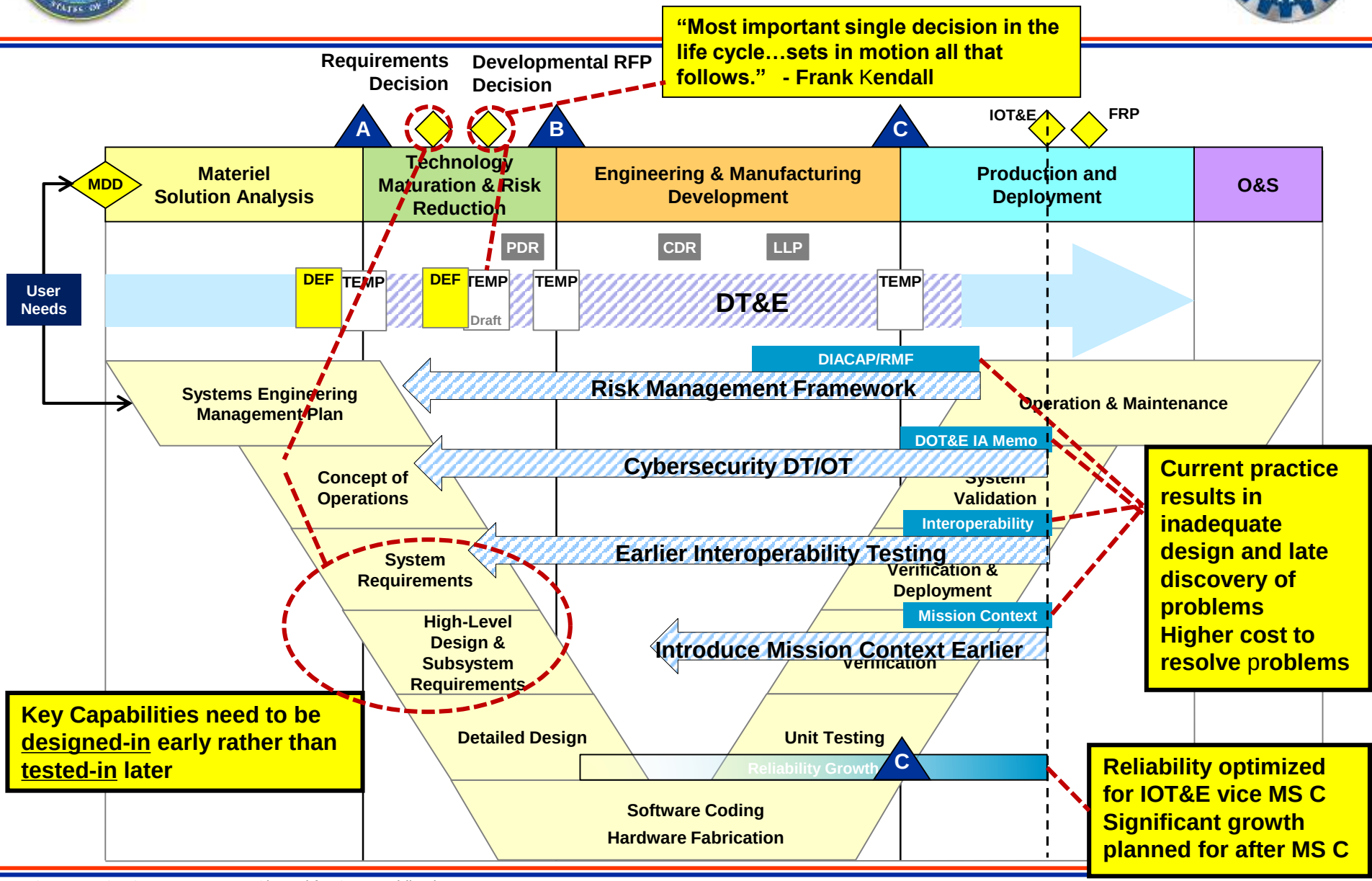
Promote Effective Competition
- Create and maintain competitive environments
- Improve technology search and outreach in global markets

Improve Tradecraft in Acquisition of Services
- Increase small business participation, including more effective use of market research
- Strengthen contract management outside the normal acquisition chain
- Improve requirements definition
- Improve the effectiveness and productivity of contracted engineering and technical services

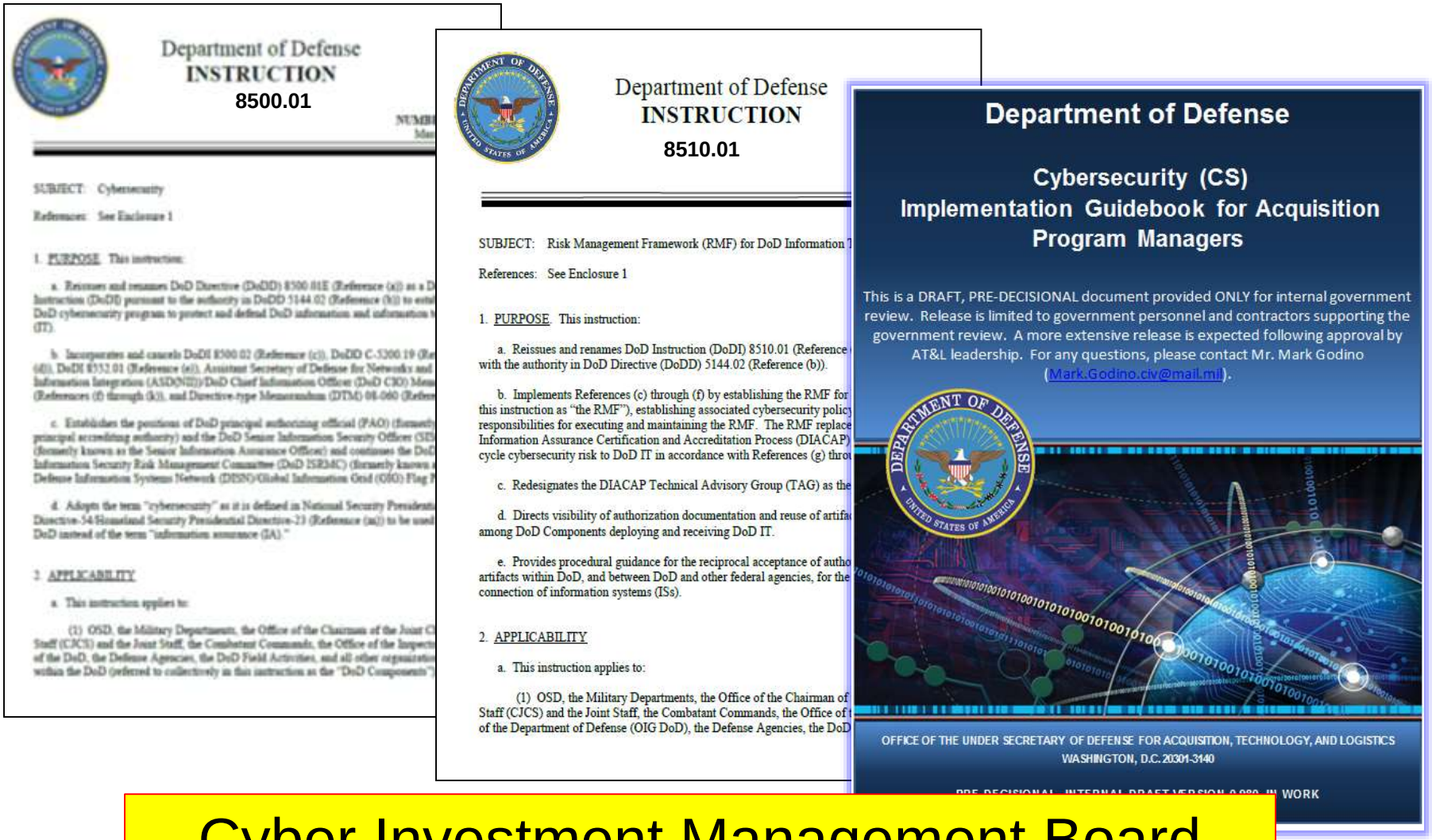
Improve the Professionalism of the Total Acquisition Workforce
- Establish higher standards for key leadership positions
- Establish stronger professional qualification requirements for all acquisition specialties
- Strengthen organic engineering capabilities
- Ensure the DOD leadership for development programs is technically qualified to manage R&D activities
- Improve our leaders' ability to understand and mitigate technical risk
- Increase DoD support for Science, Technology, Engineering and Mathematics (STEM) education

Continue Strengthening Our Culture of:
Cost Consciousness, Professionalism, and Technical Excellence

"Shift Left"



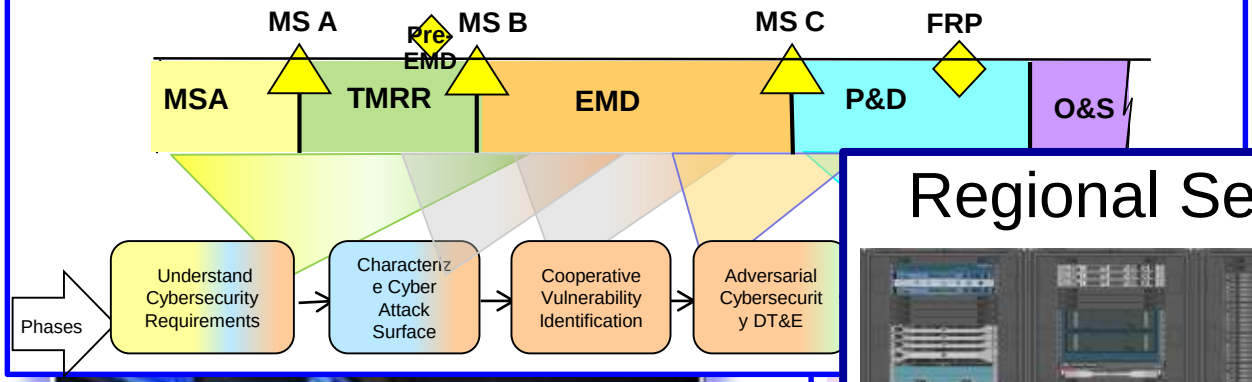
Cybersecurity Policy and Guidance in DoD



Cyber Investment Management Board

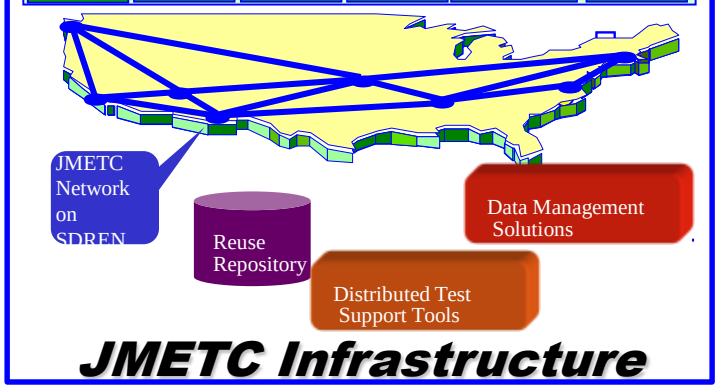
Cybersecurity Guidance and Ranges in AT&L

Cybersecurity T&E Process



National Cyber Range

Regional Service Delivery Point



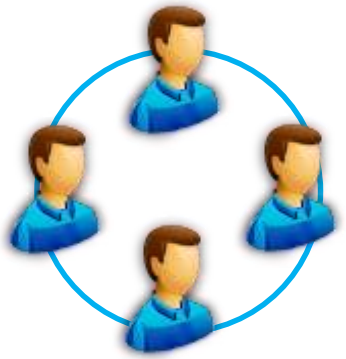
JMETC Infrastructure

National Cyber Range (NCR)

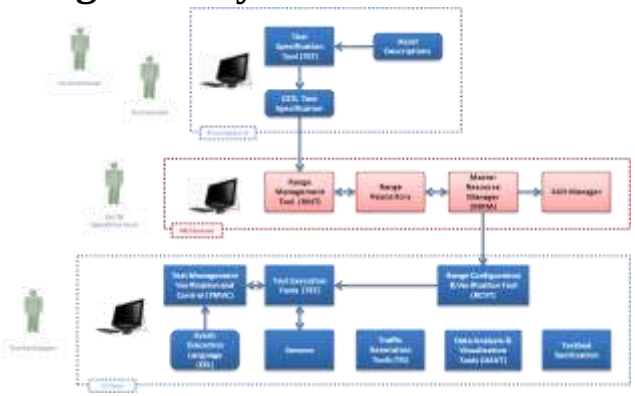
Secure facilities, innovative technologies, repeatable processes, and skilled workforce

Computing Assets/Facility

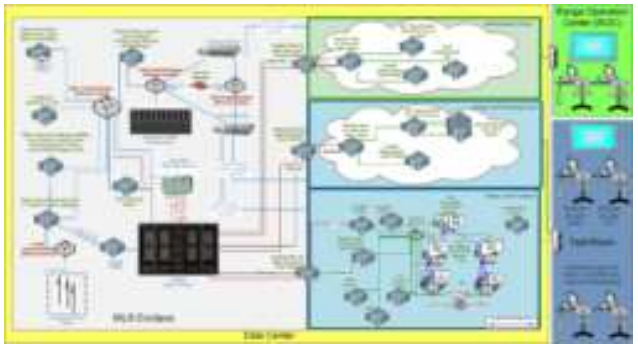
Cyber Test Team



Integrated Cyber Event Tool Suite



Encapsulation Architecture & Operational Procedures



Joint Mission Environment Test Capability (JMETC)

Significant Cost and Time Savings

Risk Reduction

JMETC Now Has Two Networks!

- **JMETC Secret Network (JSN)**
  - Operates on Secret Defense R&E Network (SDREN) since 2007
  - Open network; security agreements good for 3 years
  - Persistently and readily available
  - Primarily serves interoperability testing
  - Secret collateral only
  - NO CYBER OR COALITION
  - 76 sites
  - Supports Rapid Acquisition, Developmental Test, Operational Test, Interoperability Certification

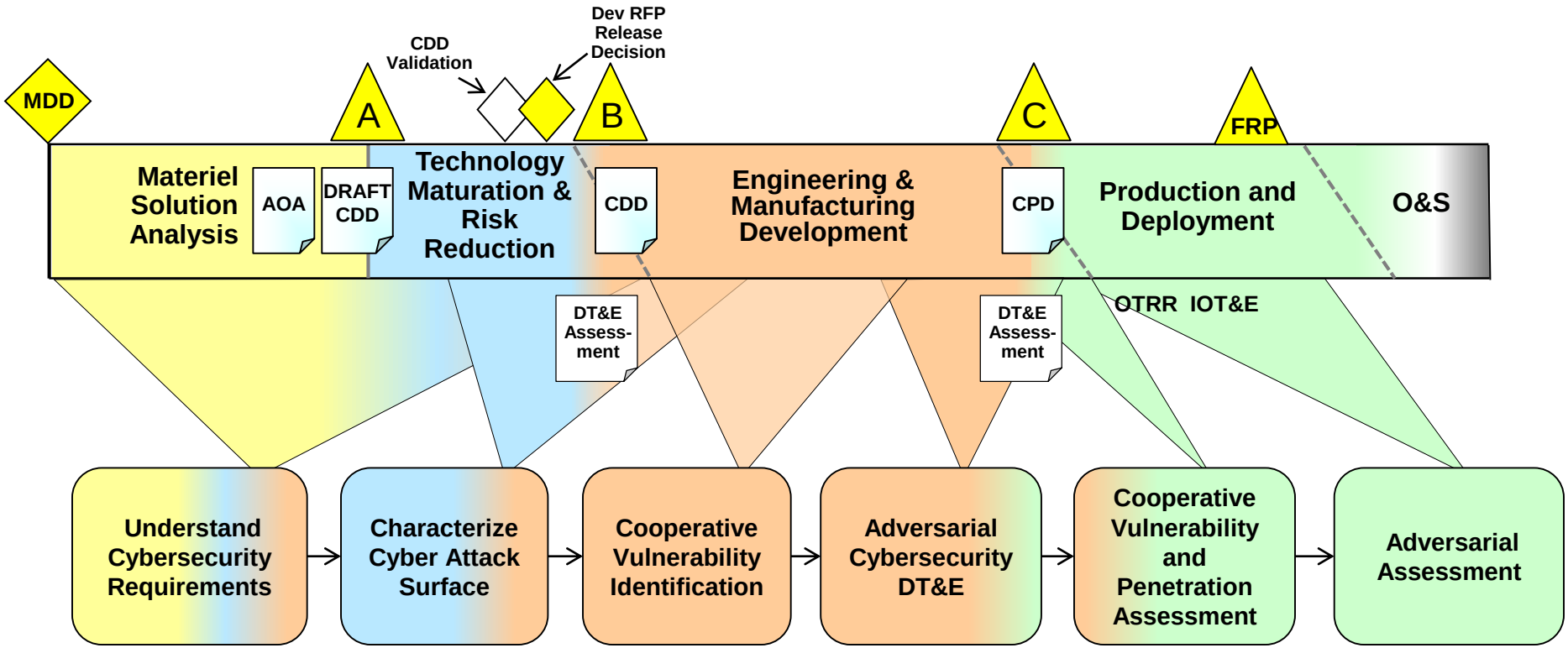
- **JMETC MILS Network (JMN)**
  - Operated on the DREN
  - Requires security agreements for each event
  - Multiple independent levels of security
  - Accredited by DIA up to TS/SCI in June 2014
  - Working SAP/SAR accreditation
  - Includes compute and storage capability
  - Capable of supporting conventional and cyber testing
  - Capable of supporting events with coalition

Regional Service Delivery Points (RSDPs)

- **The RSDPs reside on the JMETC MILS Network**

- **They will:**
  - provide increased **capacity and scalability** to create persistent, representative cyber-threat environments
  - provide **common range services** (i.e. traffic generation, simulation, instrumentation, visualization, and integrated event management)
  - be **flexible and adaptable** to evolving users requirements
  - leverage the latest technology to deliver **cost and performance efficiencies**
  - **Eventually there will be about seven, distributed across the U.S.**

Cybersecurity 6-Step T&E Process
Mapped to the Acquisition Lifecycle



Triton UAS Cybersecurity Pilot
5 month OSD Study

- **Executed by Northrup-Grumman & Navy PM**
- **Exercise the Cybersecurity process**
- **Use the NCR: Resiliency of Triton to representative Cyber Attacks**

Question: **How does the system behave in response to realized Cyber Threats?**

Air Force F-16 Cyber Study

- Focus on the Cyber T&E Process
- Study Complete
- Results expected at TRMC in mid-March

Vision

- Cybersecurity T&E of our weapons systems is essential to meeting warfighter requirements

- Systems must be:
  - Engineered to be secure in a Cyber-contested environment
  - Resilient when vulnerabilities are exploited

- Cybersecurity must be engineered in from the beginning

And it must be informed by DT&E
Cyber testing in OT is TOO LATE!

I need your help!

- Testers:
  - Work closely with your Systems Engineering counterparts to ensure Cybersecurity requirements are understood
  - Ensure T&E planning & execution adequately verify/validate requirements
  - Ensure adequate T&E resources
- Requirements / Resource Sponsors:
  - Ensure CDDs include Cybersecurity requirements
  - Ensure CONOPS includes detailed description of Cyber environment
- Program Managers / PEOs:
  - Engage early up your Service chain of command and across the services to facilitate early Cyber engineering and testing
- Contractors / Primes:
  - Cybersecurity must be the foundation of your system

YOU can help improve Cybersecurity!

Questions