Test and Evaluation Methodology and Principles for Cybersecurity

Andrew Pahutski

Deputy Director; Cyber & Information Systems
Office of the Secretary of Defense (OSD)
Developmental Test and Evaluation (DT&E)

February 26, 2015

Overview

- **Cybersecurity is a challenge for DoD Acquisition Programs**
- **DASD(DT&E) has several initiatives to assist in meeting the cybersecurity challenge**
- **Resources and Points of Contact**

The Cybersecurity Challenge

- **Cybersecurity issues continue to be identified at IOT&E**
  - Fielded Systems continue to experience Interoperability Issues and Cybersecurity Vulnerabilities
  - Too many programs optimize test strategies to deliver data/performance at IOT&E, too late to address without high cost
  - Too many acquisition programs conduct significant and critical DT&E activities after the production decision
  - JCIDS Cybersecurity requirements are poorly articulated
  - OT&E Red Teaming becomes a Cyber Vulnerability Discovery Event
- **During 2014 Combatant Command exercises and acquisition program operational tests, 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.**
  - Systems continue to be fielded with significant cyber vulnerabilities that are only remediated with adverse impact on cost, schedule or performance

DASD(DT&E) Initiatives

- **Shift Left**
- **Developmental Evaluation Framework**
- **Cybersecurity T&E Phases**
- **Cybersecurity Ranges and Support**

DASD(DT&E) "Shift Left" Initiative

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

NOV 13 2012

MEMORANDUM FOR DEFENSE ACQUISITION WORKFORCE

SUBJECT: Better Buying Power 2.0: Continuing the Pursuit for Greater Efficiency and Productivity in Defense Spending

It's been over two years now since Dr. Carter and I issued guidance to the acquisition community to ensure affordability and increase productivity in defense spending to deliver better value to the taxpayer and Warfighter. This guidance was followed by Better Buying Power (BBP) initiatives for increasing efficiencies in order to "do more without more." In these last two years, we've made significant strides, to include institutionalizing many of these initiatives. We are making good progress; we have learned from our experience, but we still have much to accomplish.

Through this memorandum I am introducing a preliminary version of BBP 2.0. After a period of two months for review and comment by stakeholders in industry and government, this will be followed by a more detailed memorandum that will outline the specific goals and requirements for each initiative included in the final BBP 2.0. We will continue to emphasize existing BBP initiatives that are especially important to our success or that require additional refinement, and we will incorporate new ideas and best practices to emphasize that have emerged from the work of the last two years.

As depicted in Attachment 1, BBP 2.0 encompasses 36 initiatives (which are further described in Attachment 2) that are organized into seven focus areas. These include a new focus area that reflects the importance of our total acquisition workforce. The basic goal of BBP, however, remains unchanged: deliver better value to the taxpayer and Warfighter by improving the way the Department does business.

As we move forward with BBP 2.0, let me reiterate that this represents a management philosophy of continuous improvement in our acquisition practices. Improving the productivity of all our contracted work, both products and services, is not an easy task that can be accomplished with a simple set of policy changes. It will require the professionalism and dedication I know I can expect from everyone in the workforce. We are entering an era where resources for the Defense Department are likely to be limited. We must wring every possible cent of value for the Warfighters we support from the dollars with which we are entrusted by the American taxpayers.

Frank Kendall

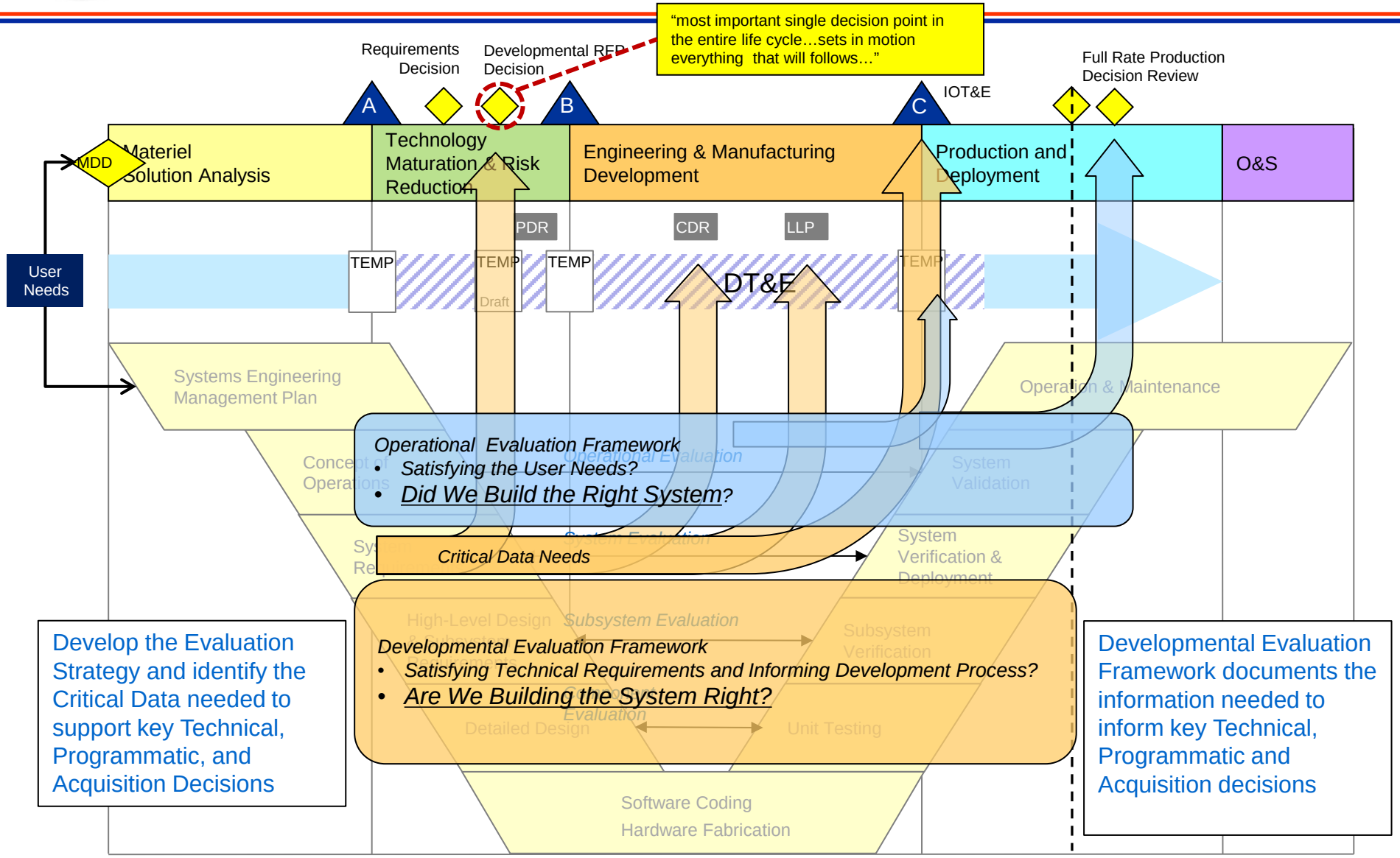
Attachments:
1. BBP 2.0 informational briefing with Focus Areas/Initiatives
2. Description of initiatives

USD(AT&L) Memo
BBP 2.0

"Shift Left" was introduced in FY12 to achieve BBP Objectives and ensure development problems do not become Warfighter or production problems

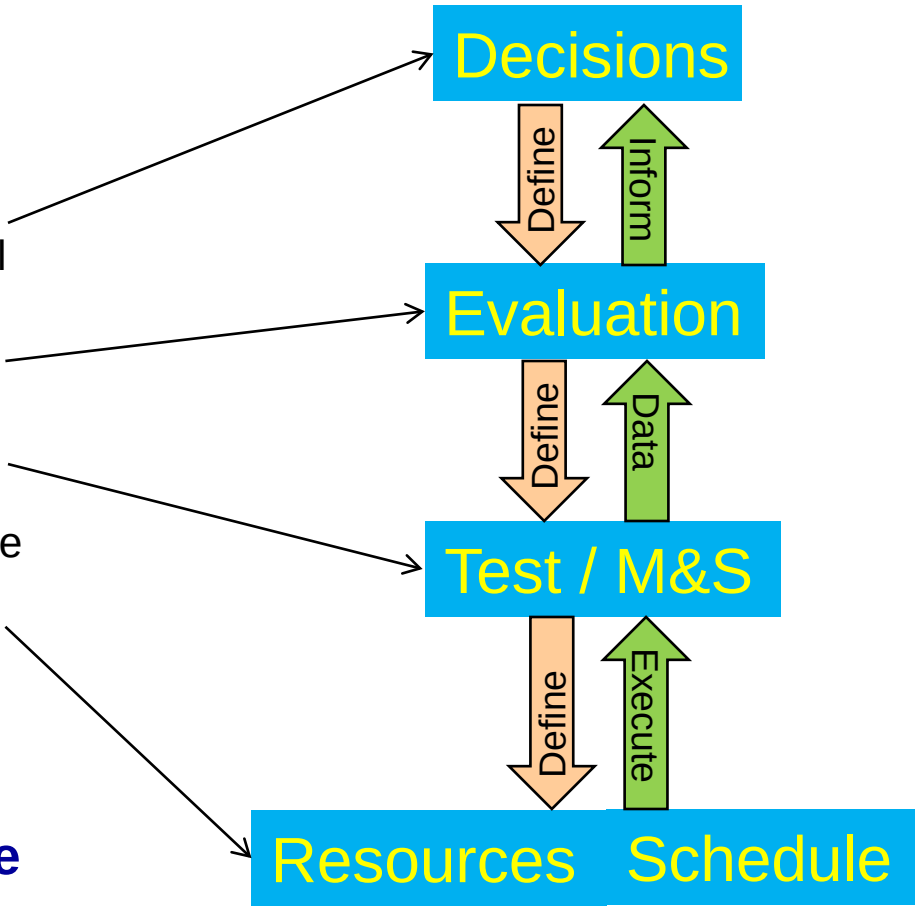
- **Plan for and perform critical DT&E activities earlier in the acquisition life cycle to find and fix problems early**
- **Focus on <u>earlier</u>:**
  - Cybersecurity T&E in a mission context
  - Interoperability T&E
  - System performance
  - Reliability assessments

SE, DT&E, and DoDI 5000.02
Plan for Evaluation, Inform the Decisions



Developmental Evaluation Framework (DEF)

- **DEF articulates a logical evaluation strategy that informs decisions**
  - How acquisition, programmatic, technical and operational decisions will be informed by evaluation
  - How system will be evaluated**
  - How test and M&S events will provide data for evaluation
  - What resources are required to execute test, conduct evaluation, and inform decisions
- **Assists in early test identification (shift left)**
- **Identifies opportunities for reuse / data sharing**



DT&E story thread: decision – evaluation– test & resources

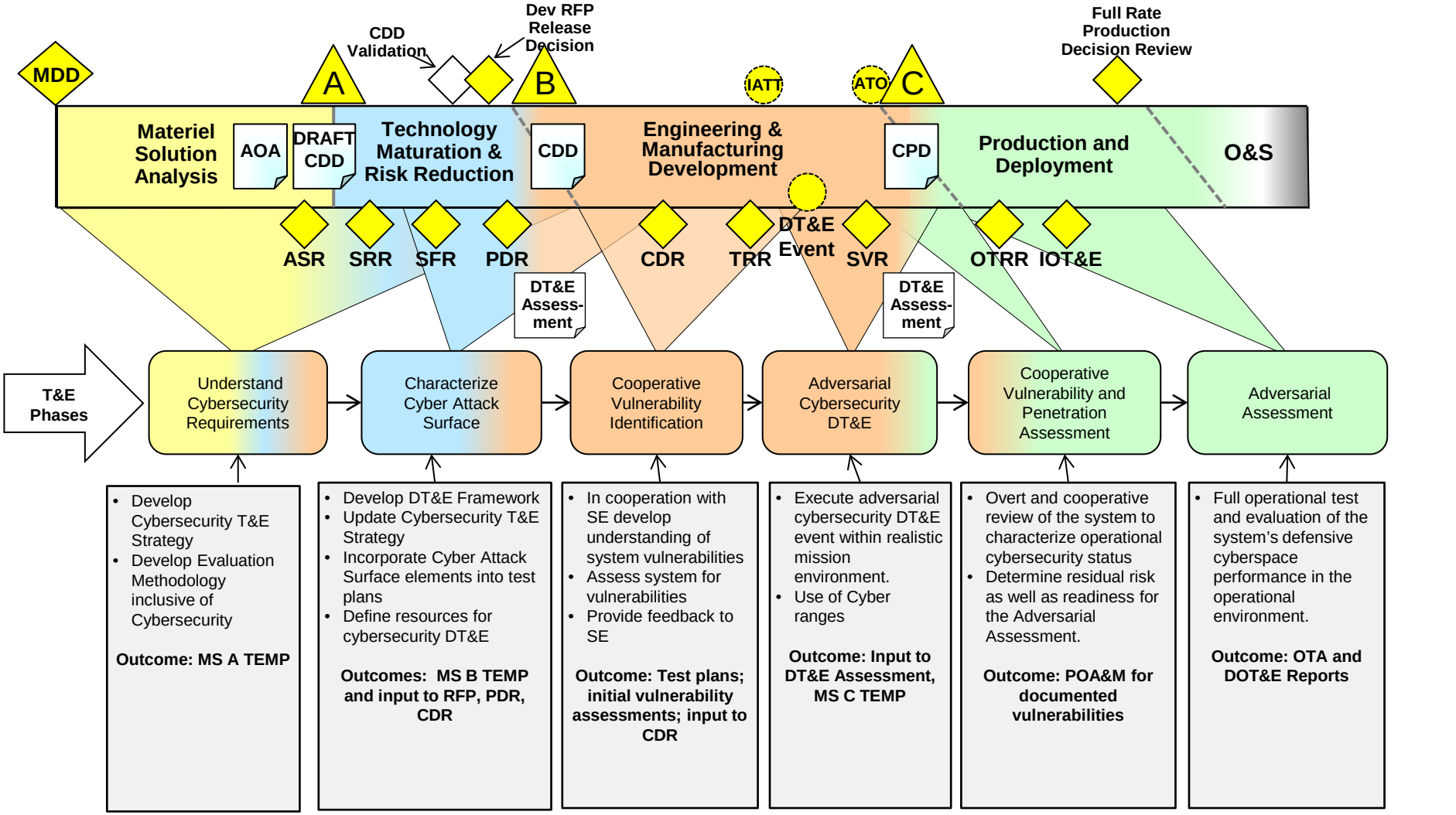
How System is evaluated

- **Requirements appropriate, implemented and tested.**
  - Test to requirements; not every system needs to be tested to nation state threat portrayal, levels of threat
  - RMF starts with categorization of protection needs and impact of failures
- **Tools used for compliance validation and known exploits**
- **How well does system protect?**
- **How does the system detect?**
  - Are notifications useful for cyber staff?
- **How does the system react?**
- **How can the system be restored?**

How Program is evaluated

- Cybersecurity “baked in”
- Requirements complete and appropriate
- Test events planned and resourced
- Test organizations identified
- End user involved
- Developer accountable, including for reuse of testing
- TEMP is primary document for test planning

Cybersecurity T&E Phases



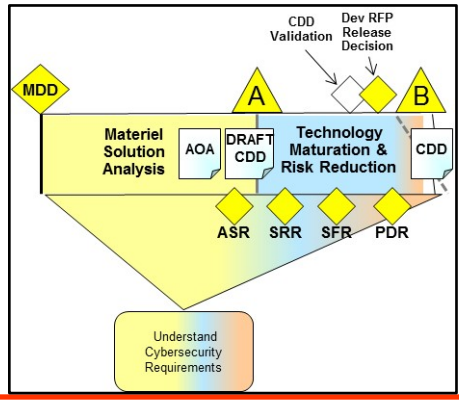
Phases are iterative and executed as part of the Acquisition continuum.

Phase 1 – Understand Cybersecurity Requirements

Understand the program's cybersecurity requirements and develop an initial approach and plan for conducting cybersecurity T&E

- **Early in the acquisition process, the Chief Developmental Tester and T&E WIPT**
  - Identify cybersecurity requirements and ensure they are complete and testable.
  - Review cybersecurity requirements in the System Requirements Document, PPP, technical documents, RMF artifacts, and RFPs.
  - Review threat documents to understand the cyber threats to the system.
- **Based on the requirements review, the T&E WIPT constructs a T&E strategy to address the cybersecurity requirements and threat profiles.**
- **This phase will be performed iteratively, as system development proceeds.**

The Chief Developmental Tester and T&E WIPT will ensure that system cybersecurity requirements are identified and testable

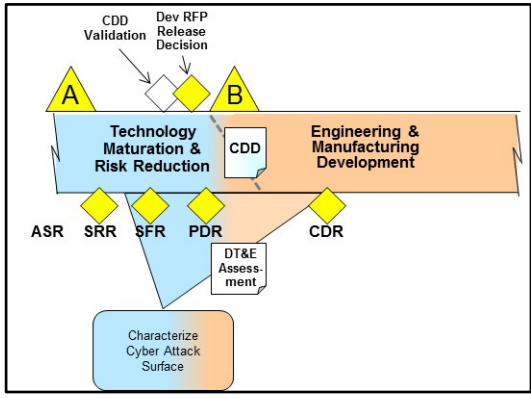


Phase 2 – Characterize Cyber Attack Surface

Identify opportunities an attacker may use in order to plan testing to evaluate whether those opportunities continue to allow exploitation.

- **The attack surface is the system's exposure to reachable and exploitable cyber vulnerabilities, including reliance on supporting / underlying infrastructure.**
- **Characterizing the cyber-attack surface is executed in collaboration with the systems security engineering process.**
- **RMF artifacts such as the Security Plan and Security Assessment Plan are used to identify additional components that constitute the system's attack surface.**

Characterization of the cyber-attack surface provides input into subsequent test planning



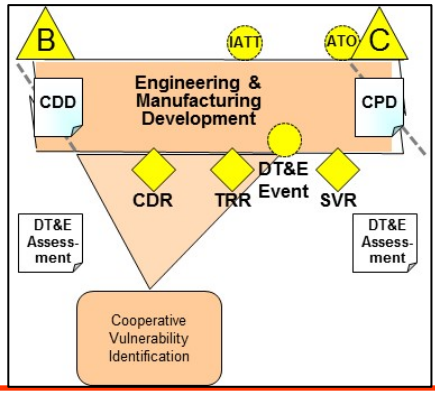
Phase 3 – Cooperative Vulnerability Identification

Analyze and evaluate potential vulnerabilities to determine measures to improve resilience (cyber range or lab)

- **Develop initial concept for cyber security testing activities at the component and subsystem level**
  - Identify test opportunities to conduct cybersecurity testing in a system of systems context (such as JITC interoperability testing)
  - Identify and integrate RMF security controls assessment activities into unit testing. Functional testing, etc.
  - Evaluate early RMF artifacts
- **Perform a vulnerability assessment using a Blue Team, to determine likely avenues of cyber attack and the most likely threat exploits**
  - Include or emulate the CNDSP
  - Analyze the kill chain
  - Enumerate discovered vulnerabilities
  - Provide feedback to SE

T&E informs Decision Makers

Vulnerability Testing will be integrated, to the extent possible, with other system test events

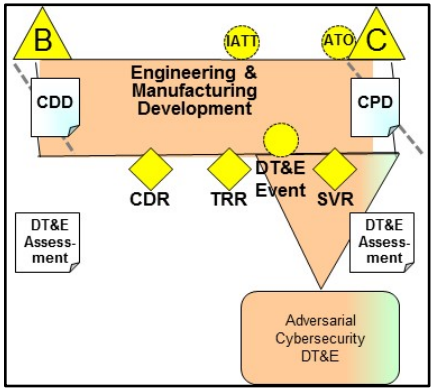


Phase 4 – Adversarial Cybersecurity DT&E

Evaluation of the system's cybersecurity in a mission context, using realistic threat exploitation techniques, while in a representative operating environment.

- **Verify/Exercise Critical Missions through an adversarial, Red Team-type exercise**
- **ID exposed vulnerabilities/mission impact**
- **Develop DT&E Assessment, including**
  - How critical mission objectives will be impacted if the data required to execute the mission objectives is altered due to cyber-attack and/or exploitation
  - How critical mission objectives will be compromised if required data is unavailable
  - How critical mission objectives will be compromised if mission data is exploited in advance of mission execution.

The goal of the cybersecurity DT&E event is to discover critical vulnerabilities and determine their impacts



New DoD Cybersecurity Test & Evaluation T&E Policy and Guidance

- **Policy**
  - DoDI 5000.02, Operation of the Defense Acquisition System, January 2015
  - DoDI 8500.01, Cybersecurity and 8510.01 RMF, March 2014

- **Implementation Guidance**
  - DOT&E Memo, Procedures for OT&E of Cybersecurity in Acquisition Programs, August 2014
  - DAG Chapter 9 (T&E), Paragraph 9.6.5 (Cybersecurity T&E)
  - Cybersecurity T&E Guidebook
  - DOD Cybersecurity Guidebook for Acquisition Program Managers
  - DOT&E Cybersecurity Assessment Program

- **Training**
  - DAU TST courses now include cybersecurity module/ Cybersecurity T&E phases, DAU 102, 204, 303

*In development

Challenges

- **Stove piping of PORs across System of Systems**
  - Requirements and scope of testing are a recurring source of disagreement
  - Cybersecurity testing of critical data exchanges with other systems may not be possible until Interoperability testing and certification activities late in the lifecycle
- **Cyber threat portrayal is required early and throughout the process**
  - STARs are currently inadequate for cyber threat portrayal
  - Threats should drive the engineering of Cybersecurity countermeasures and priorities for remediation; requires coordination with SE
- **Addressing embedded systems and Platform IT as well as "classic" IT**
- **Increased Workforce Demand**
  - Service/Components Penetration Test resources (Red Teams)
  - Service/Components Vulnerability Test (Blue Teams)
  - Cyber Ranges

Resources: Cyber Ranges

C4 Assessment Division (C4AD), Suffolk, VA Contact E-Mail: JS.DSC.J6.MBX.C4AD-operations@mail.mil	Conduct assessments of existing and emerging Command, Control, Communications, and Computers (C4) capabilities in a persistent C4 environment.
DoD Cybersecurity Range, Quantico, VA Contact E-Mail: IARangeCMT@ITSFAC.com	Provide a persistent environment to support T&E, exercise support, training, and education.
Joint IO Range (JIOR) Norfolk, VA Contact Phone Numbers: (757) 836-9787 or (757) 836-9848	A flexible, seamless, and persistent environment (infrastructure) that enables Combatant and Component Commanders to achieve the same level of confidence and expertise in employing information operations (IO) weapons that they have in kinetic weapons.
National Cyber Range (NCR) Orlando, FL Contact E-Mail: osd.pentagon.ousd-atl.mbx.trmc@mail.mil	Provide realistic, quantifiable assessments of the Nation's cyber research and development technologies. Includes agile setup of Multiple Independent Levels of Security (MILS) sanitized Unclassified, Secret, or SCI environments for Program of Record testing.
Joint Mission Environment Test Capability (JMETC) Test Resource Management Center (TRMC) Contact E-Mail: osd.pentagon.ousd-atl.mbx.trmc@mail.mil	JMETC provides the persistent, robust infrastructure (network, integration software, tools, reuse repository) and technical expertise to integrate Live, Virtual, and Constructive systems for test and evaluation in Joint Systems-of-Systems and Cyber environments.

Points of Contact

- **Andrew Pahutski, DASD(DT&E), andrew.j.pahutski.civ@mail.mil**

- **Cyber Resources:**
  - Cyber Ranges (JIOR, NCR, DoD Cyber Range, & C4 AD)
  - Cybersecurity center of excellence, Ft. Gordon
  - Blue team/Red team SMEs**
    - Navy NIOC
    - Army TSMO
    - Army Ist IO Command
    - Air Force 177th IO Squadron

** Please email me directly for specific POCs

Questions?