U.S. ARMY EVALUATION CENTER

Army Cyber Survivability: Shift Left Progress

March 30, 2017

Agenda

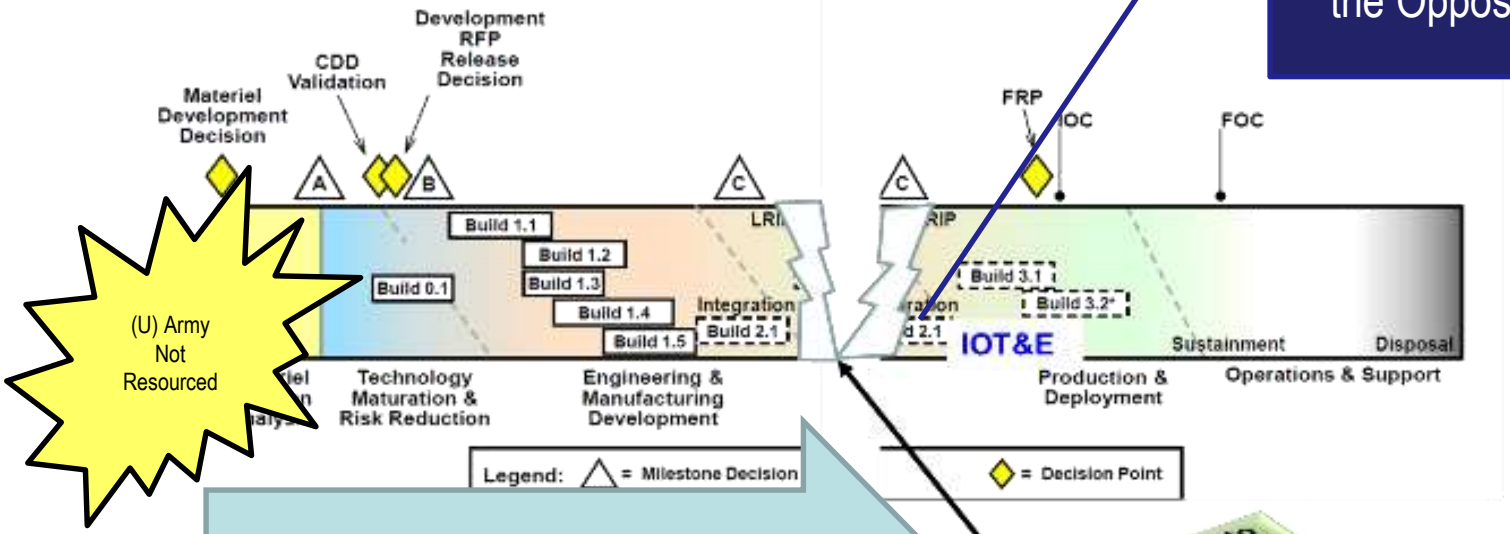
What is “Shift Left”?

How was Shift Left Implemented?

How well did we do?

Why Shift Left?

Only an Adversarial Assessment as part of the Opposing Force



(U) Army Not Resourced

(U) Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) / Risk Management Framework (RMF)

"Must close this gap to enable unity of effort"

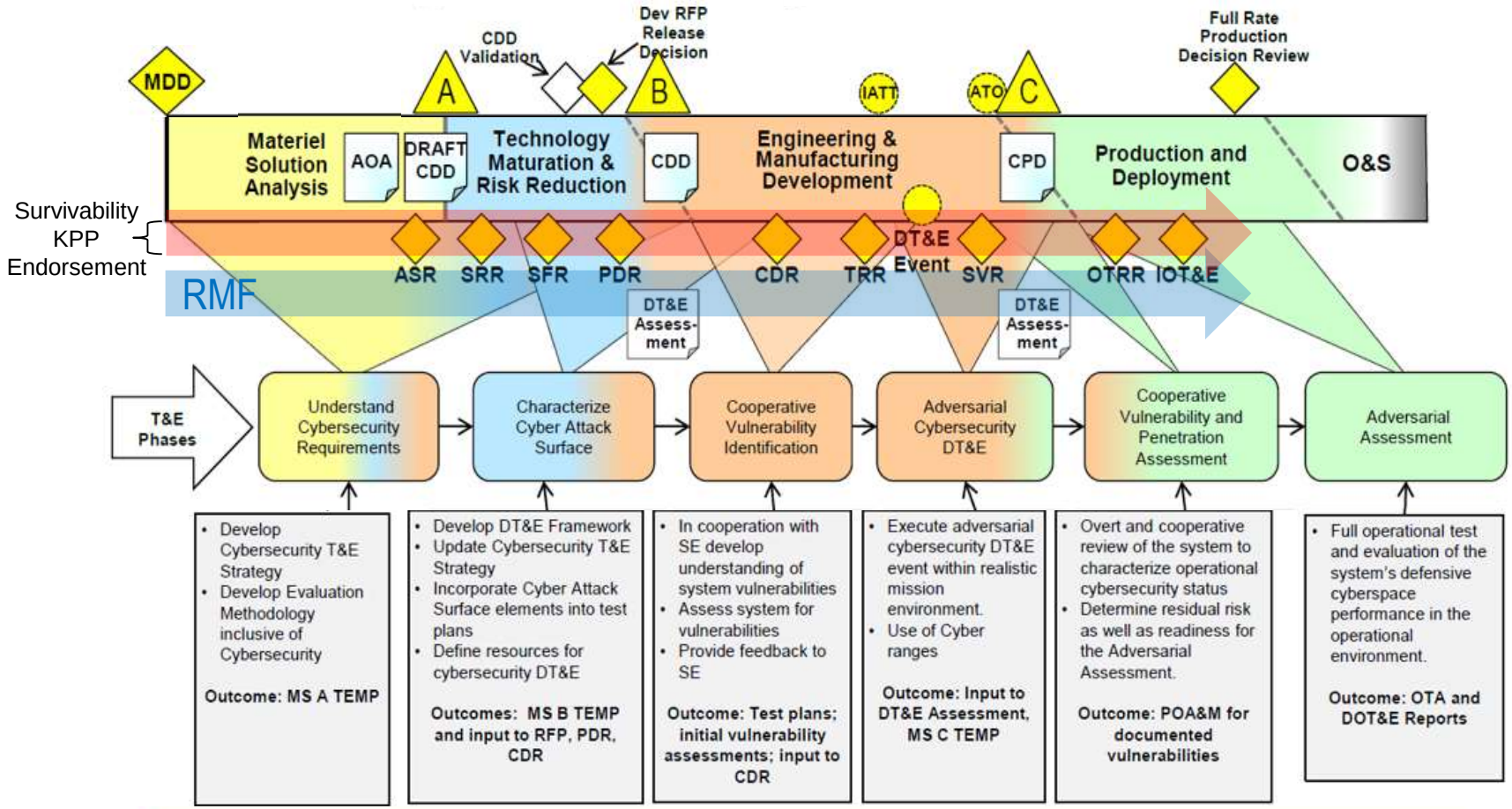
- **"Pre-Milestone A to Retirement"**
  - ❑ **Duration of a System Lifecycle - Continuous Process**
  - ❑ **Establish Security Architecture Early**
  - ❑ **T&E of Major Software Drop in DT and OT**
  - ❑ **Software Changes in Sustainment**
  - ❑ **Underpinned by policy, standards, and disci**

Threat

Shift Left

To discover cybersecurity issues earlier in the acquisition lifecycle

Cybersecurity T&E Process



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

A better cyber survivable system, but that said …

Shift Left Review

- Reviewed Results over two years since implementation of Shift Left (FY2014)
- In order to meet the intent of shift left to be included in the review:
  - System T&E included at minimum the Cooperative Vulnerability Identification (CVI), the Cooperative Vulnerability and Penetration Assessment (CVPA) and the Adversarial Assessment associated with Operational Test
  - The phases above had to have been conducted from Jan 2014 through Jan 2016
  - System had to have completed the operational test agency evaluation reporting (OER).
- **Assessment:**
  - Of the 41 systems reviewed, - 7 met the criteria.
  - Why so few:
    - Acquisition Life cycle had to fall within the two year time span (19 were either assessed before shift left implementation or were only beginning)
    - Another 15 were either rapids program not being networked or were non-oversight programs

5 of the 7 programs were assessed as survivable in the OER

Cybersecurity T&E Trends

The Good News

- **Defenders are Getting Better at all echelons (BDE, DIV, RCC)**
- **Defenders' tools are Improving and making threat movement across the network more challenging**
- **TTPs are developing on protecting "key cyber terrain"**
- **Defense in Depth works both doctrinally and architecturally**

Where Improvement is Needed

- **Defender Manning and Training is always an issue for T&E as it is across the Army**
- **Replicating network defense in depth by echelon and evolving Defender toolkit**
  - **PLT -> CO -> BN -> BCT -> DIV -> CORPS/ACERT**
- **Recurring Cyber Vulnerabilities:**
  - **Exposed or poorly managed credentials**
  - **Systems not configured to identified standards**
  - **Systems not patched for known vulnerabilities**
  - **System/network services and trust relationships that provide avenues for cyber compromise**

Final Thoughts

Shift Left is working

Cyber Survivability T&E complements Compliance (Risk Management Framework)

Hardware and Software in the Network
Network Assessments vice Systems Under Test

- **"Pre-Milestone A to Retirement"**
  - ❑ Duration of a System Lifecycle - Continuous Process
  - ❑ Establish Security Architecture Early
  - ❑ T&E of Major Software Drop in DT and OT
  - ❑ Software Changes in Sustainment
- **Complementary Efforts**
  - ❑ Must have a baseline to enable integration
  - ❑ Defined Cybersecurity Approach Early
  - ❑ RMF
  - ❑ Patch Management
- **Cybersecurity T&E Approach**
  - ❑ Shift Left is producing more survivable systems

Cybersecurity T&E spans the entire materiel life cycle of the program, and each phase builds off the completion of the prior phase. (DODI 5000.02, 2 Feb 2017)