U.S. ARMY EVALUATION CENTER

Shift Left: Putting the Process Into Action

March 30, 2017

Agenda

The Evaluator's Motivation

Where We Were

Guidance and Policy

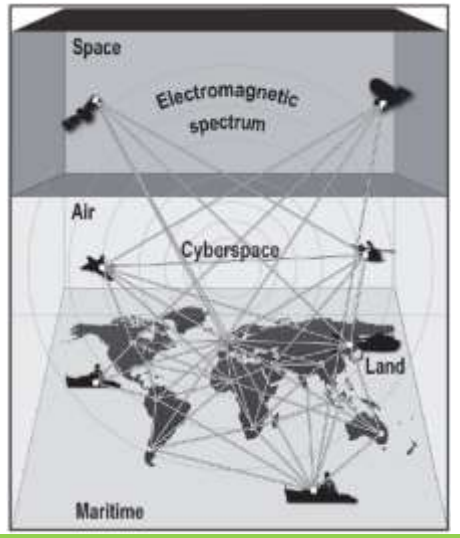
Putting it into Action

The Evaluator's Motivation

What is the Outcome of the T&E Process "Requirements for Cybersecurity/EW"

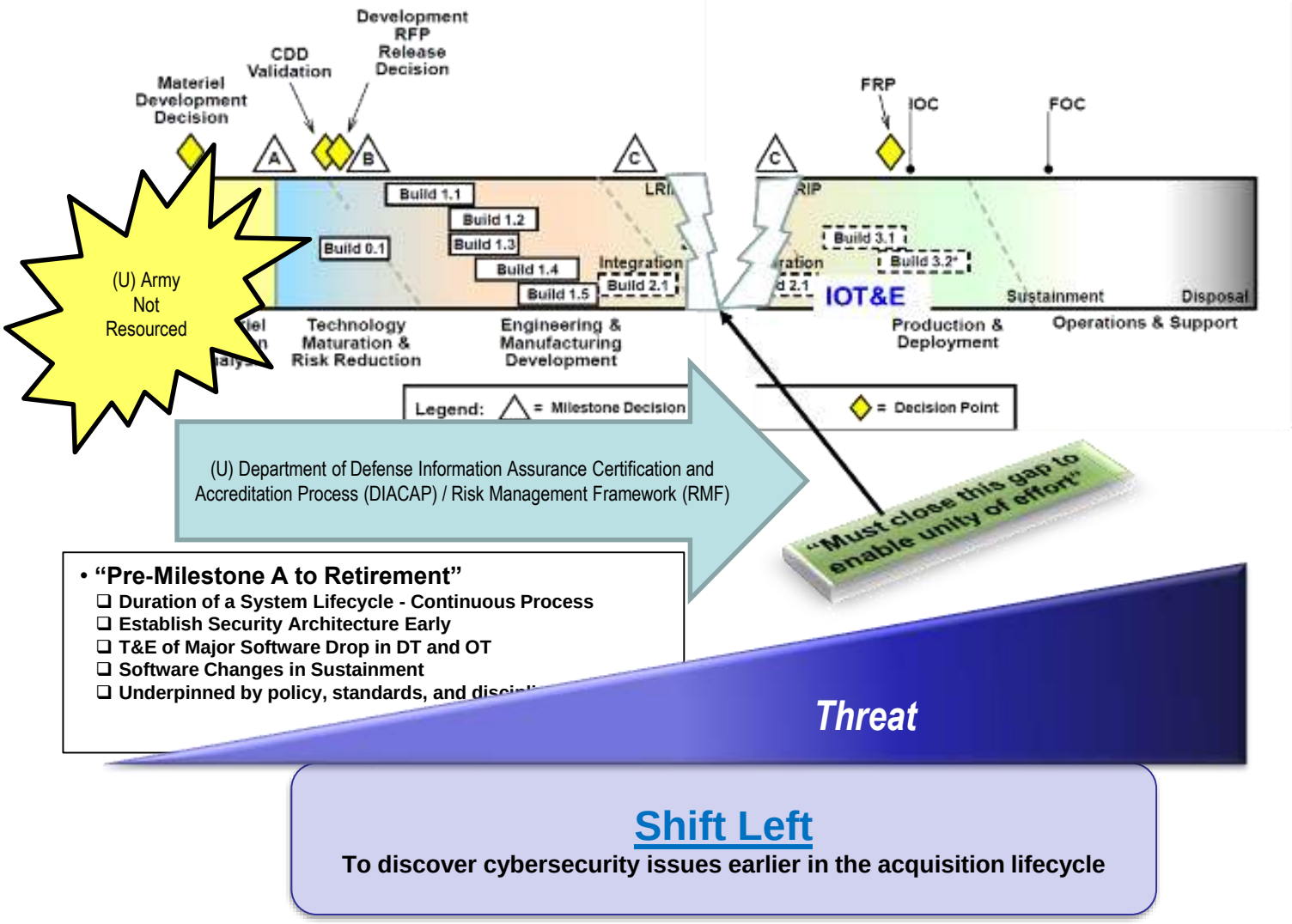
We Owe Decision Makers Key Answers

- Does the system maintain its critical capabilities under applicable threat environments? (Cyber and EW)
- Does the system provide robustness and resiliency against hostile activity?
- Does the system meet all Federal and Department of Defense cybersecurity regulations, guidelines, and best practices?
- Does the system introduce new exploitable cyber vulnerabilities to the systems and networks with which it interoperates?
- Does the system provide the ability to detect the loss of system or data integrity, and to restore the system and data to a known good (trusted) state?



Cyber/EW Survivability as a key element of the mandatory System Survivability (SS) Key Performance Parameter (KPP).

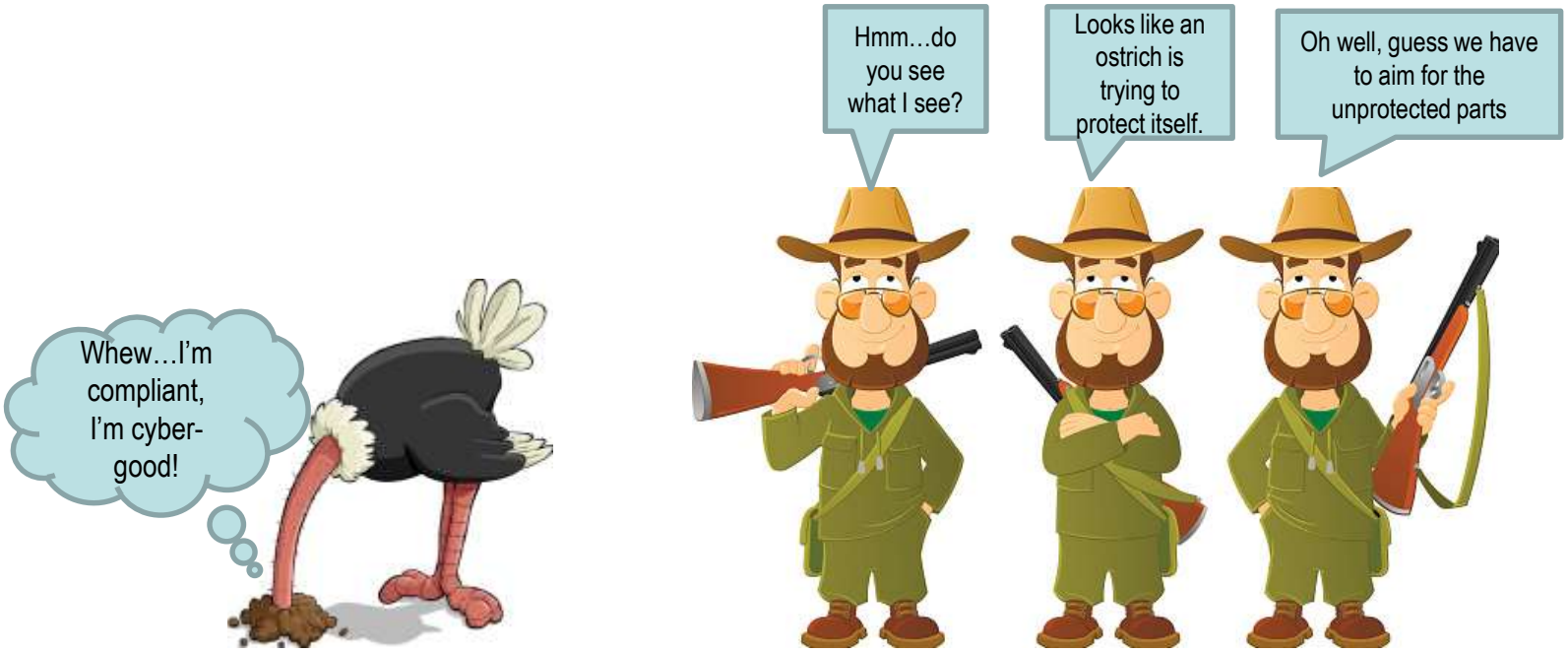
In the Beginning…



Shift Left

To discover cybersecurity issues earlier in the acquisition lifecycle

A Breakdown in the Process?



Cyber Survivability is more than Compliance

The threat continues to grow and evolve

Understanding system capability vs. evolving threat as system matures is critical

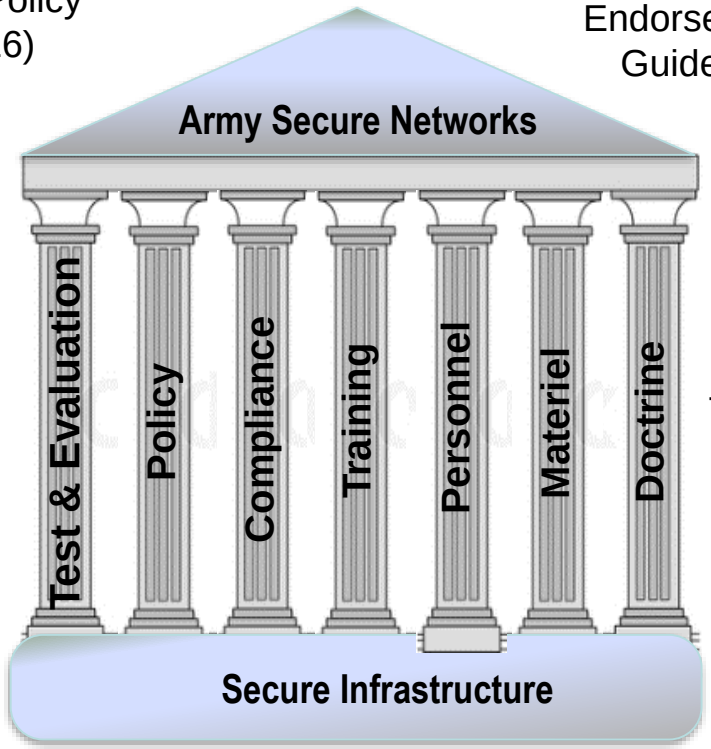
Guidance is Available

DOD Instruction 5000.02, “Operation of the Defense Acquisition System” (2 February 2017)

Army Regulation 73-1 Test and Evaluation Policy (16 November 2016)

Cyber Survivability Endorsement Implementation Guide (26 January 2017)

DOD Program Manager’s Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, version 1.0 (September 2015)



DOD Cybersecurity Test and Evaluation Guidebook, version1.0 (1 July 2015)

OSD Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs (1 August 2014)

DOD Directive 8140 Cyberspace Workforce Management (11 August 2015)

DOD Instruction 8500.01 Cybersecurity (14 March 2014)

Department of Defense Instruction (DODI) 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT) (12 March 2014)

Putting it all Together

DOD Directive 8140 Cyberspace Workforce Management (11 August 2015)

OSD Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs

DOD Cybersecurity Test and Evaluation Guidebook, version1.0 (1 July 2015)

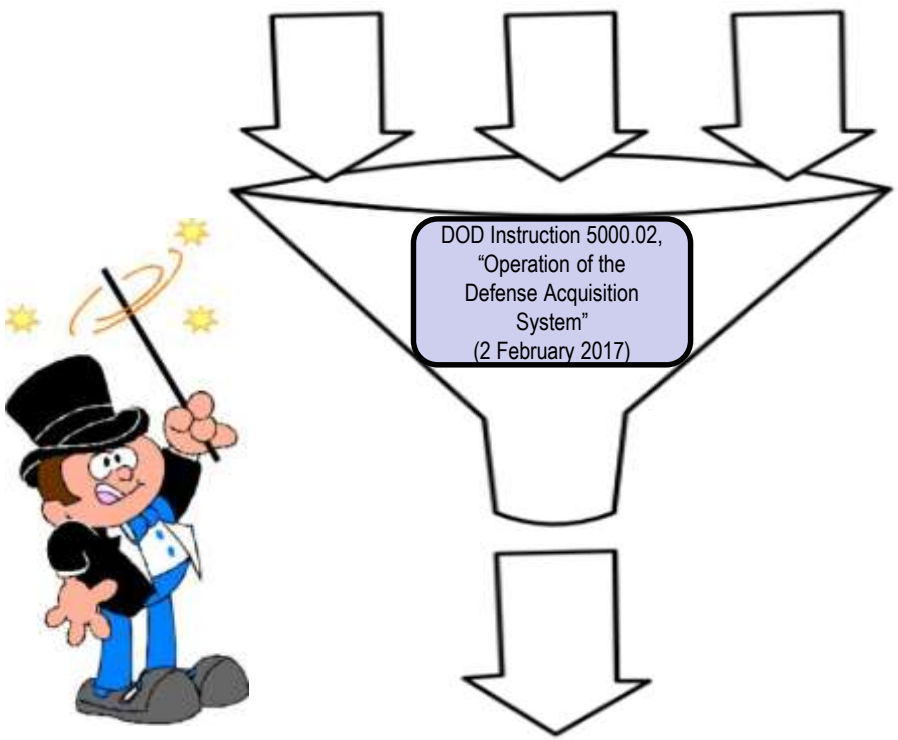
Cyber Survivability Endorsement Implementation Guide (26 January 2017)

DOD Instruction 8500.01 Cybersecurity (14 March 2014)

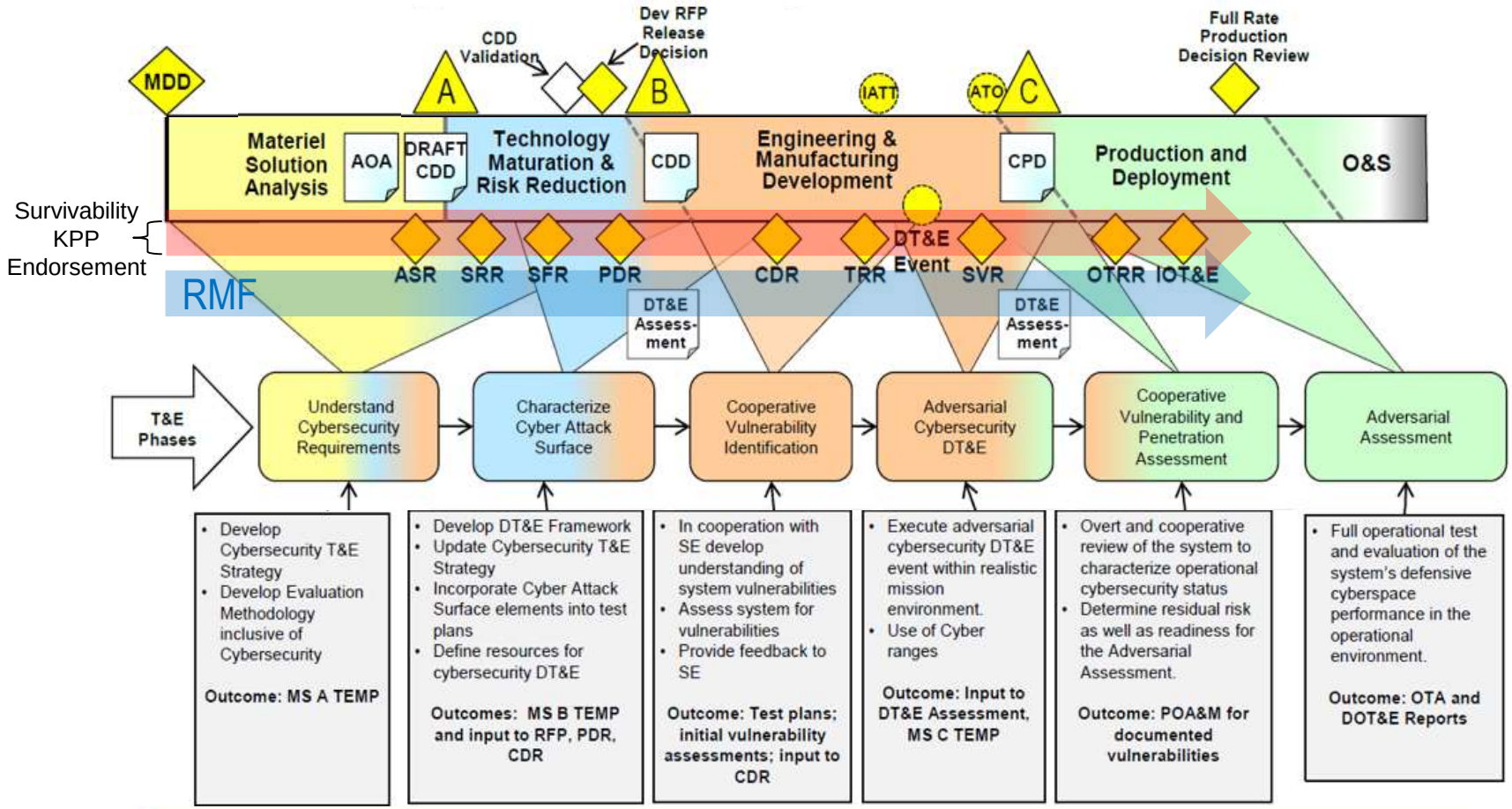
DOD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, version 1.0 (September 2015)

Department of Defense Instruction (DODI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) (12 March 2014)

Army Regulation 73-1 Test and Evaluation Policy (16 November 2016)



Cybersecurity T&E Process



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

A better cyber survivable system, but that said …

An Evaluator's Thoughts

Policy and guidance provide strong foundation for a strong program

Descriptive vs. Prescriptive

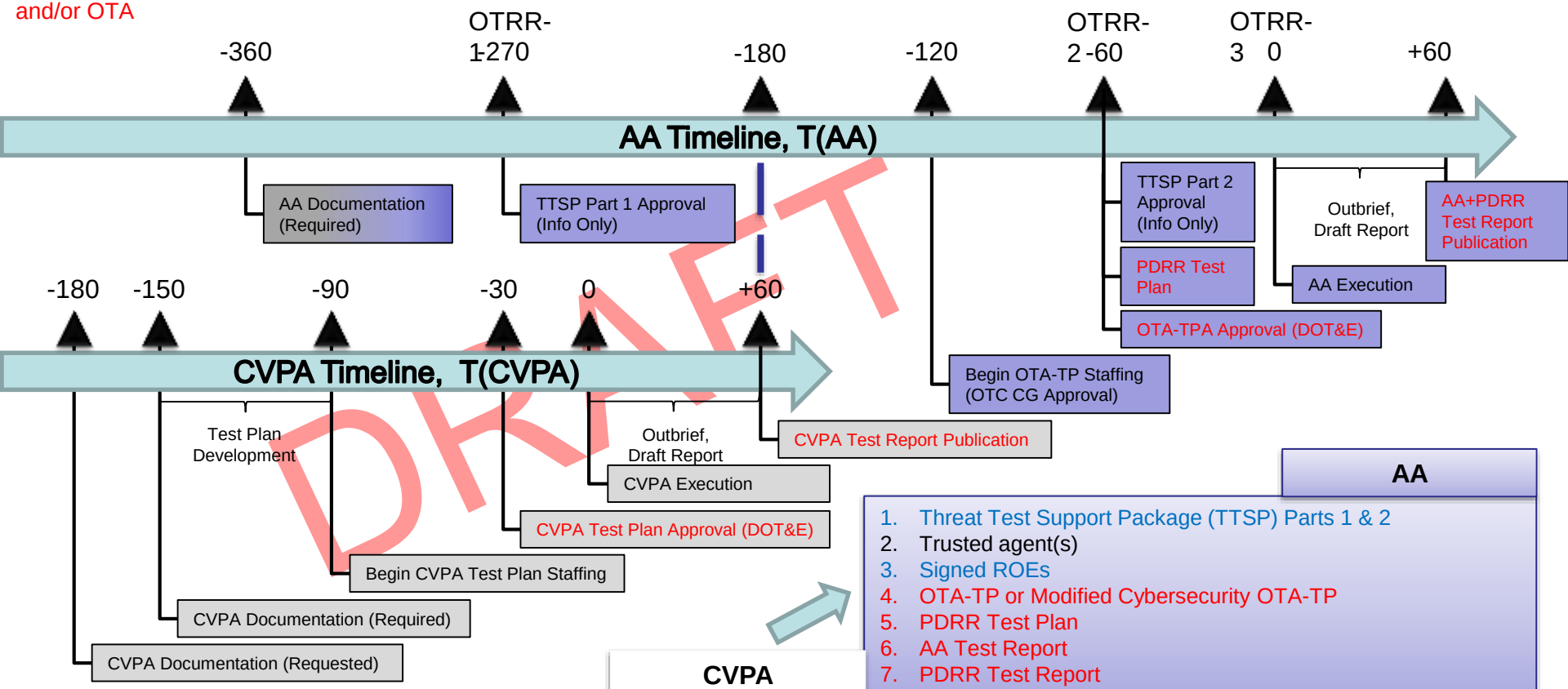
Recommendations:

- Language in RFP beyond compliance and accreditation
- Plan and design to the intended contested environment
- Develop DODAF views of intended network architecture, logical and physical connections and interfaces
- Identify security aspects required for any system to integrate, embed, or connect to your system
- Embed cybersecurity SMEs—architecture, process, hacker mentality—with Systems Engineering Team early in the design process
- Engage Research, Development and Engineering Centers to assist with design
- Conduct Cybersecurity Table Top Exercise prior to Preliminary Design Review

GOAL: A cyber survivable system by Milestone C
Corrections are costly to implement closer to production

Red Text = Products generated by test providers (ARL/SLAD, TSMO) and/or OTA

OT Cybersecurity Documentation Timeline



AA

1. Threat Test Support Package (TTSP) Parts 1 & 2
2. Trusted agent(s)
3. Signed ROEs
4. OTA-TP or Modified Cybersecurity OTA-TP
5. PDRR Test Plan
6. AA Test Report
7. PDRR Test Report

CVPA

1. Security Classification Guide
2. Test timeframe, location, unit
3. Test and Evaluation Master Plan
4. System Evaluation Plan (SEP) and Data Source Matrix (DSM)
5. Statement of Work, Initial Capabilities Document (ICD), CDD, CPD, ONS/JUONS
6. Concept of Operations (CONOPS)
7. DODAF Views
8. Physical and Logical Architecture Diagrams
9. Systems Engineering Plan (SEP)
10. Program Protection Plan (PPP)
11. User (Technical and Operator's) Manuals
12. Preliminary Design Review (PDR) and/or Critical Design Review (CDR)
13. Interface Control Document (ICD)
14. System Threat Assessment Report (STAR) / VOLT and Information Operations Capstone Threat Assessment (CTA)
15. Risk Management Framework (RMF) Artifacts
16. Previous Test Reports and/or Scheduled Test Plans
17. Most recent vulnerability scans
18. DOD Ports, Protocols, and Services Worksheet
19. HW & SW list/inventory
20. IP list (white/blacklisted)
21. Unit SOPs
22. IRP, COOP, and DRP (Unit and SUT)
23. PDRR Scoping Questionnaire
24. User role provisioning forms for System Under Test (SUT)
25. On-site support and classified storage requirements document
26. Copy of approved Radio Frequency Authorizations (RFA)
27. CVPA Test Plan
28. CVPA Test Report

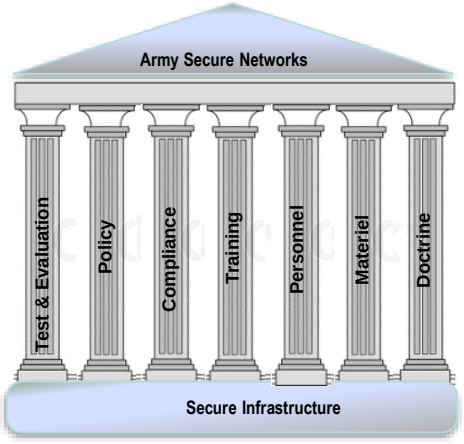
Final Thoughts

A cyber survivable system can be built—Guidance is there; execution is key

Build cyber survivability into the system from the initial concept

- "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
- Unity Of Effort
  - ❑ Must have a baseline to enable integration
  - ❑ Defined Cybersecurity Architecture and Standards
  - ❑ Discipline – "Centralized Management of Continuous Integration"
- Cybersecurity T&E Approach

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



Do not find vulnerabilities in operational systems that should have been discovered early and designed out during system development.