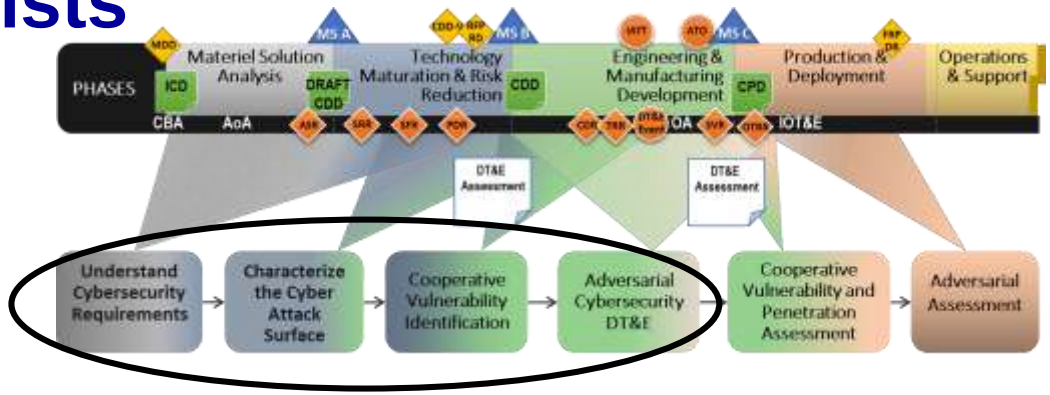
Developmental Test and Evaluation (DT&E) Cyber Test Planning

2016 ITEA Symposium

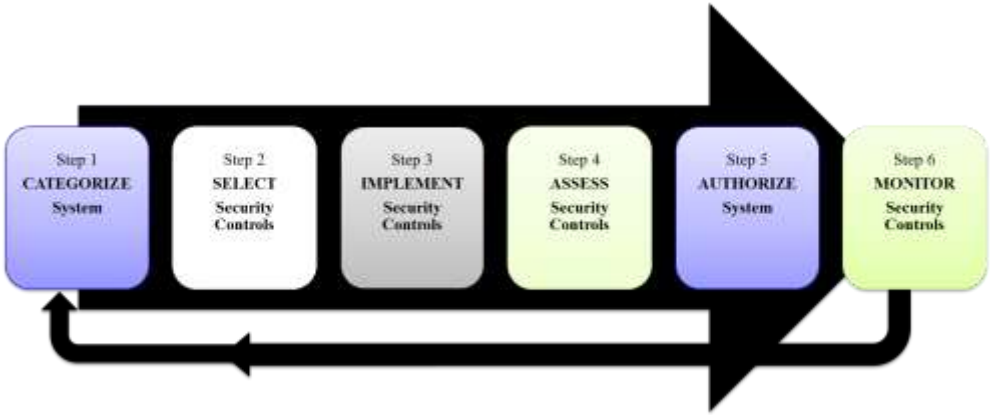
Sarah M. Standard
Cybersecurity/Interoperability Technical Director
Deputy Assistant Secretary of Defense (DT&E)
October 4, 2016

Cyber DT&E and the Risk Management Framework (RMF)

- **Cyber DT&E consists of four *phases***
  - Iterative
  - Mission focus



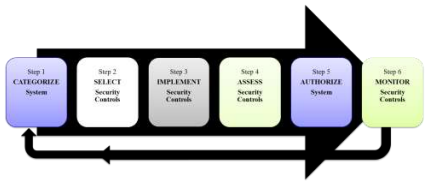
- **RMF is a six step process**
  - Designed in
  - Compliance



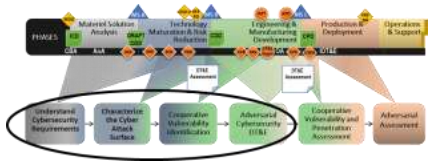
NOT TIGHTLY COUPLED – THIS IS NOT A MARRIAGE
THEY INFORM EACH OTHER – IT IS A FRIENDSHIP

Why do Both?

RMF		Cyber DT&E
Derived cyber requirements	⟺	Performance assessment
Authorization to Operate (ATO)	⟺	Verification and validation of system resiliency



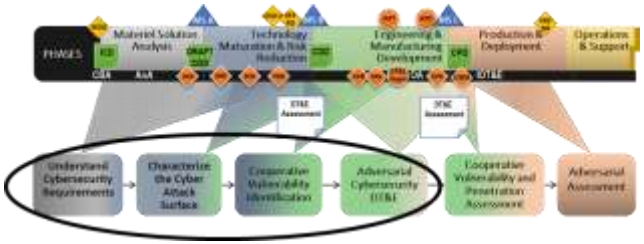
RMF Step 4 ≠ Cyber DT&E



BOTH IMPROVE AND INCREASE SYSTEM CYBER RESILIENCY

Planning and Implementing the Cyber DT&E Phases

- **Read the guidebook**
- **Program must stand up a Cyber Working Group**
- **Program must partner with a Cyber DT&E team**
- **Adequately resource Cyber DT&E**
- **Perform mission based cyber risk assessments (CRAs) or cyber table tops (CTTs)**



START EARLY TO FINISH BEFORE MILESTONE C

SHIFT LEFT TO DESIGN RIGHT!

Mission Based Cyber Risk Assessments

- **Many methodologies**
  - Vary in complexity, effort, participants and duration
- **Assess mission impact and likelihood**
  - Threats and system vulnerabilities
- **Actionable information for cyber DT&E**

DETAILED UNDERSTANDING OF ARCHITECTURE, OPERATION AND THREATS IS CRITICAL

Questions?