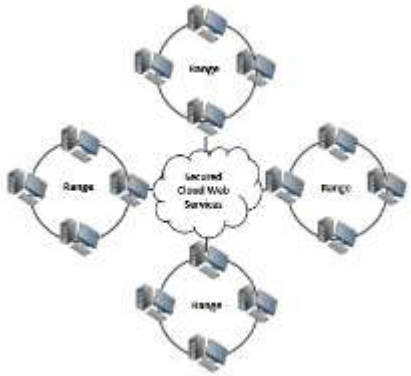
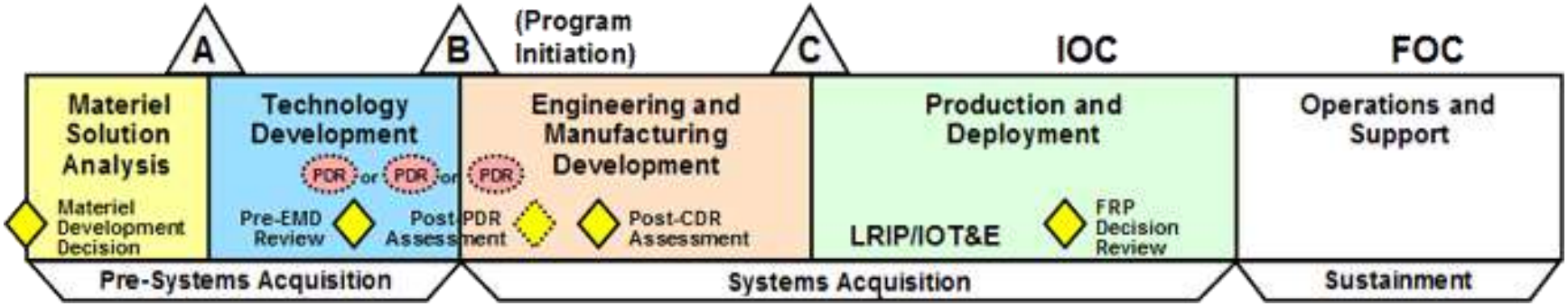
ASA(ALT)
Improving Cybersecurity Across the Lifecycle

March 17, 2016

MG Jon Maddux
Program Executive Office
Simulation, Training and Instrumentation

Mission Assurance / Resilience





Initiatives (1)

Risk Management Framework and Weapon System Prioritization

- Changing the way we develop new and manage legacy systems
- Operational Risk Decision Framework will prioritize weapon systems based on mission criticality and system posture
- Moving Army towards assessing earlier in the acquisition lifecycle with increased emphasis throughout

Acquisition Blue Teams

- Centrally managing and overseeing the execution of blue vulnerability assessment capabilities
- Establishing and managing certification standards and processes
- Providing, in coordination with Program Managers and U.S. Army Evaluation Center, feedback on trends to ASA(ALT) leadership

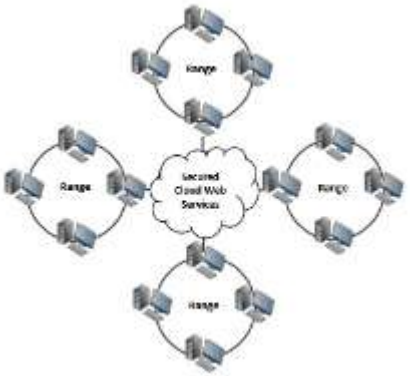
Initiatives (2)

Acquisition Red Teams

- Managing and executing acquisition red team to support Developmental & Operational Test and Evaluation
- Executing red team activities in support of Combatant Command assessments and major exercises
- Providing, in coordination with the U.S. Army Evaluation Center, feedback on trends to (ASA(ALT) leadership

Cyber Ranges

- Providing infrastructure, capabilities and expertise to support test, evaluation, experimentation, and training across Army and DoD
- Working closely with the Army and DoD to define acquisition roles and responsibilities in support of the DoD Cyber Test Ranges and Training Ranges Executive Agents



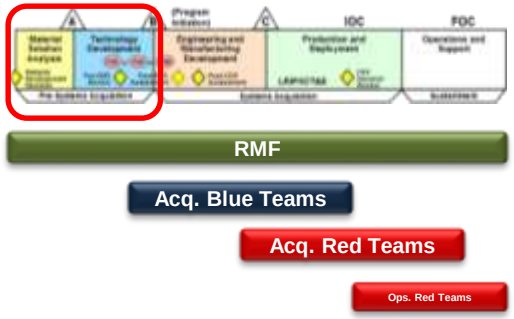
Some of Our Challenges

Talent Management

- Recruiting, hiring and retaining highly skilled cyber personnel
- The threat is constantly evolving and we are increasing our focus on cybersecurity, but we are disadvantaged in the competition for top cyber talent
- Will work with the Army and DoD towards the *Implementation of Recommendations for DoD Civilian Cyber Personnel*

Designing **in Security**

- Current and planned initiatives enhance our cybersecurity posture
- Must improve at defining and incorporating cyber technical requirements into system specifications and contracts
- Must feed catalogued vulnerabilities, tools, exploits and best practices as early and quickly as possible



Questions?