U.S. AIR FORCE

Cyber Security Challenges for RDT&E Systems

Paul Waters
412 TENG Tech Director
Donald.waters.3@us.af.mil

Overview

- Outline
  - Balancing Mission and Cyber Security
  - Incorporating Cyber Security into Range Processes
  - Resource Imbalance
  - Partnerships in RMF

- BLUF
  - Test Ranges need to take ownership of Cyber Security and tailor it to balance Mission and Security

Mission

- Timing is critical
- Flexibility and Agility are essential
- Traditional Cyber Security Confidentiality, Integrity, Availability (C-I-A) balance is different

Cyber Security and Range Processes

- Key Processes should be aligned
  - System Verification
  - Configuration Management
  - Data Security

- Other Processes are Incompatible
  - Continuous Monitoring
  - AF and DoD Software Approval process
  - Firewall Implementation, Virus Updates, Sys Admin Limitations

Resource Imbalance

412 TW

- Unfunded Mandate
  - Requires new people to authorize and accredit
  - Requires new people to validate and monitor
  - Requires new skills to operate and maintain
  - Requires new HW & SW to become compliant
- Requires Culture Shift
  - Need to be more aware of potential risks
  - Need to be appropriately risk tolerant

RMF Partnerships

- Partnering between AO and Ranges
  - Understand “real” risks
  - Understand mission impacts
  - Streamline RMF processes to support agility

- Partnering between Ranges
  - Accept other Range ATOs and ATCs
  - Share RMF control implementation
  - Share updated Range and Cyber Security Processes

QUESTIONS