T&E of Warfighting System Cyber Security Capabilities

Darryl K. Ahner, PhD, P.E.
Director, OSD STAT COE
937-255-3636 x 4708

Bill Rowell, PhD, CISSP, CEH
Cyber Expert, OSD STAT COE
937-255-3636 x 4592
www.AFTT.edu/STAT

Disclaimer

Any opinions or recommendations expressed in this presentation are those of the presenter and do not necessarily reflect the view of the U.S. Air Force or Department of Defense.

Purpose

Provide the T&E community with insights into the cyber security T&E process for warfighting systems via a high-level look at cyberspace, cyberspace operations, and the cyber security requirements process for warfighting systems.

Overview

- Cyberspace
- Cyberspace operations
- Warfighting systems cyber security requirements process
- Key insights

What is Cyberspace?

- Interdependent operations/warfighting domains
  - Physical domains: Land, Maritime, Air, Space
  - Global/non-physical domain: Cyberspace
- Physical Components
  - Many different and often overlapping networks
  - Nodes on those networks
  - System data that support the networks
- Layers of cyberspace domain
  - Physical network
  - Logical network
  - Cyber-persona

What are Cyberspace Operations?

- Composed of **military**, intelligence, and ordinary DoD business **operations in and through cyberspace**
- Employment of cyberspace capabilities
  - By Joint Force Commanders (JFC), their staffs, and supporting and subordinate commanders
  - To achieve JFC objectives **in and through cyberspace**

Cyberspace Operations Objectives

- Provide freedom of maneuver in DoD or other friendly cyberspace
- Deny freedom of action in cyberspace to adversaries
- Accomplish other JFC's cyberspace objectives
- Enable other operational activities

Notes: Maneuver can occur in all layers: physical network, logical network, cyber-persona.

Key terrain in cyberspace (network links & nodes)

Cyberspace Operations Missions

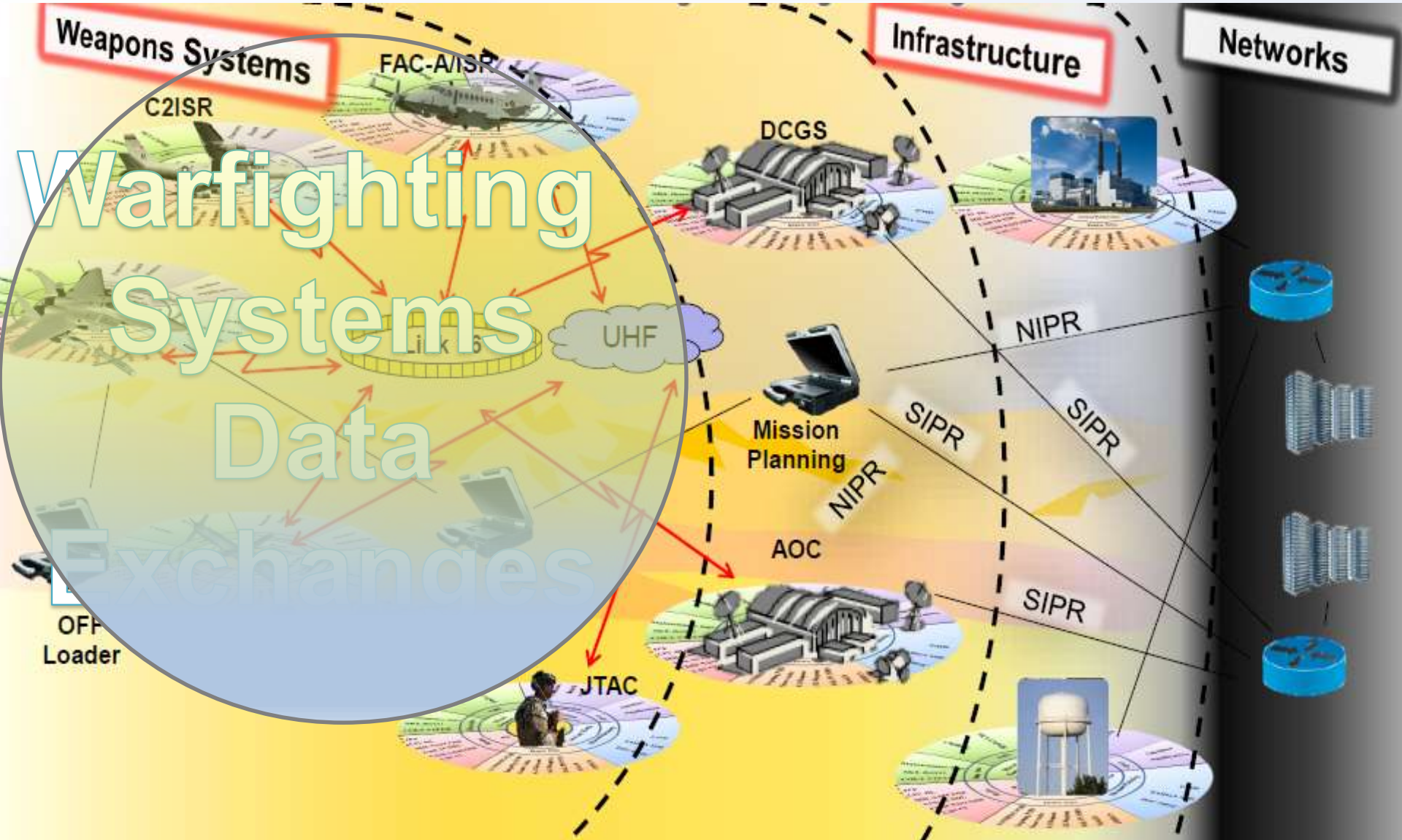
- Defensive Cyberspace Operations (DCO)
  - Defend DOD or other friendly cyberspace
- Offensive Cyberspace Operations (OCO)
  - Project power by the application of force
- DODIN Global Network Operations
  - Design, build, configure, secure, operate, maintain, and sustain **DOD communications systems and networks**
  - Create and preserve **data availability**, **integrity**, **confidentiality**, user/entity **authentication** and **non-repudiation**

Department of Defense Information Networks (DODIN)

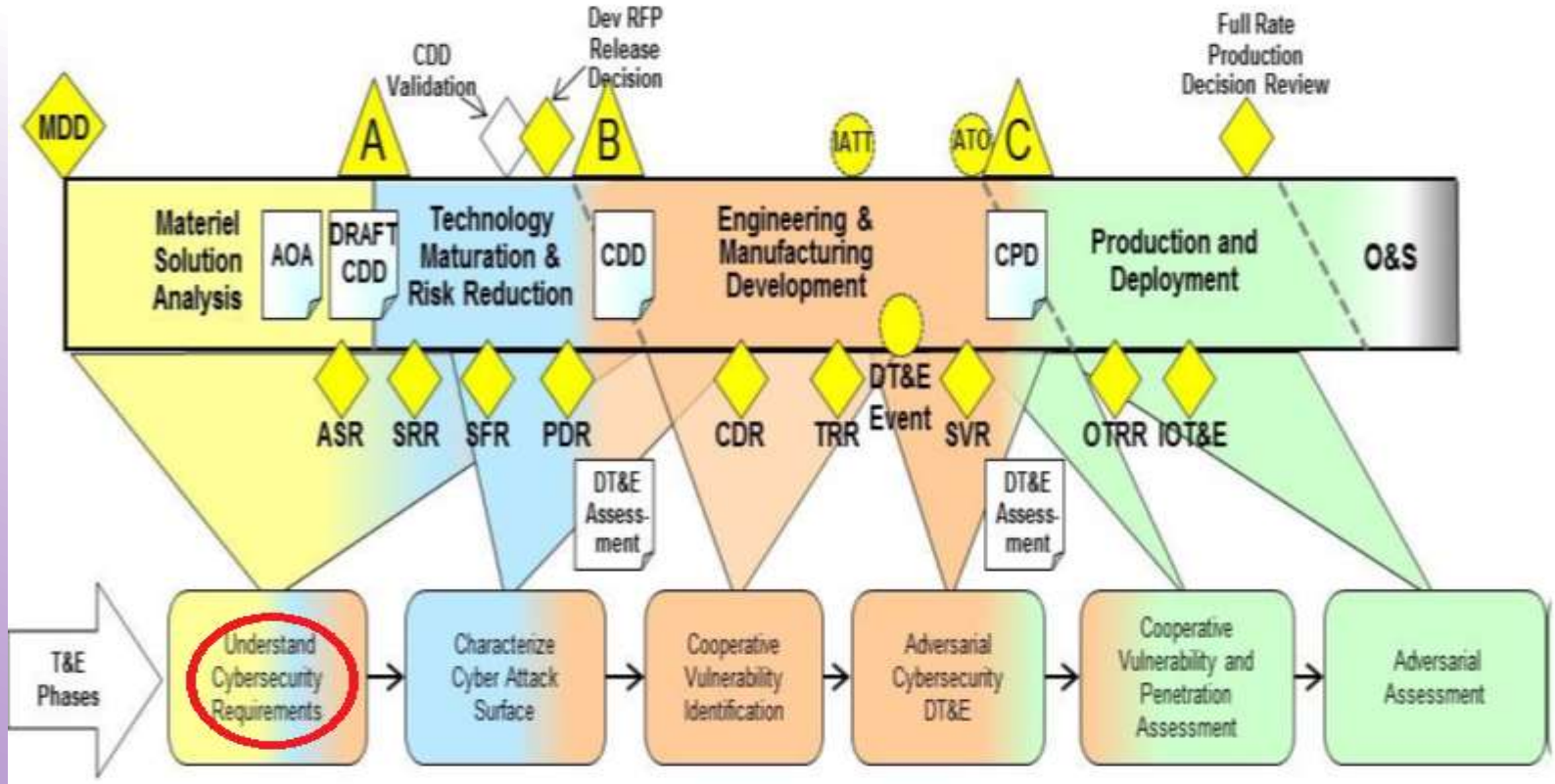
- Globally interconnected, end-to-end set of **information capabilities** for collecting, processing, storing, disseminating, and **managing information on demand to warfighters**, policy makers, and support personnel
- Includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems (NSSs)
- **Enables Cyberspace Operations**

Note: How DODIN/warfighting systems exchange info key to cyber security

DODIN/Warfighting Systems Data Exchanges

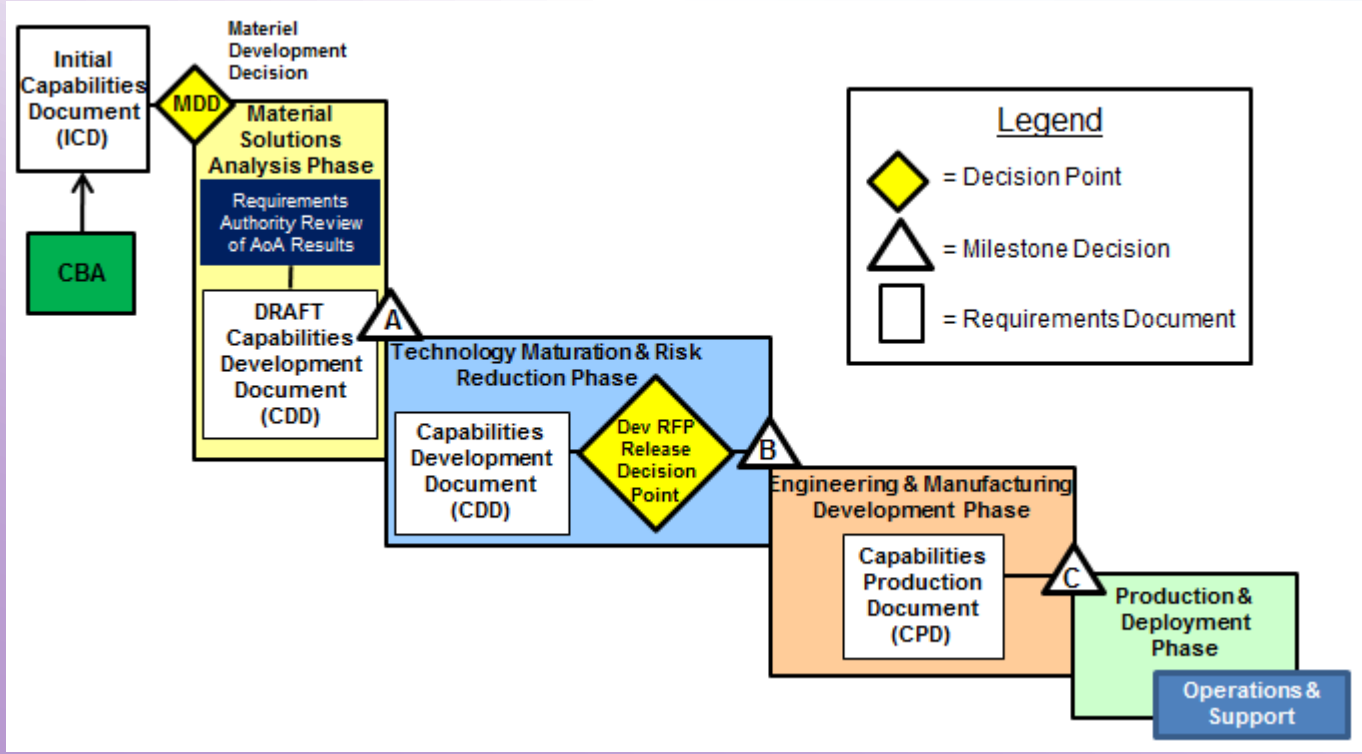


Cybersecurity T&E Phase: Understand Cybersecurity Requirements



Joint Capabilities Integration and Development System (JCIDS) Process

- Objective: Ensure the capabilities required by the **joint warfighter** are identified, along with their associated **operational performance criteria** (requirements), in order to successfully **execute the missions assigned**.
- Integrated JCIDS/Acquisition Process



Requirements Development Process
Performance Attributes as the Bridge

Higher Level (Qualitative)

Strategic Level Mission Outcomes (What, Where, When)

The Sponsor (representing the operators) develops operational system requirements consistent with organizational missions using the **JCIDS process**

- National/Defense Strategy, Defense Planning Guidance & QDR
- Scenarios, OPLANs/Contingency Plans - tasks/conditions/standards
- AF Core Function Planning - force structure and resources

Operational System Requirements (The "What")

- Operational Tasks and Gaps - what we need vs. what we have
- System level Performance Requirements – what it needs to do

- **Performance Attributes, Thresholds/Objectives**

Key Performance Parameter (KPP)/Key System Attribute (KSA)

Technical Requirements (The "How")

- Functional & System Performance Specifications
- Design specifications – system, sub-systems, component
- Product, process, materiel specifications

Lower Level (Quantitative)

The Program Manager and Acquisition Engineering community develop technical requirements and specifications

ICD
CDD
CPD

The "Bridge"

SEP
SRD
RFP

Mandatory System Survivability (SS) Key Performance Parameter (KPP)

- December 2014: System survivability against cyber-attack (non-kinetic) threat added as key element to SS KPP in JCIDS
- Capabilities against threat to system survivability
  - Reduced likelihood of being hit by kinetic or non-kinetic fires. (Prevention)
  - Reduced vulnerability if hit by kinetic or non-kinetic fires, including cyber effects. (Mitigation)
  - Recovery of the overall force to complete the mission despite the loss of individual platforms. (Recovery)

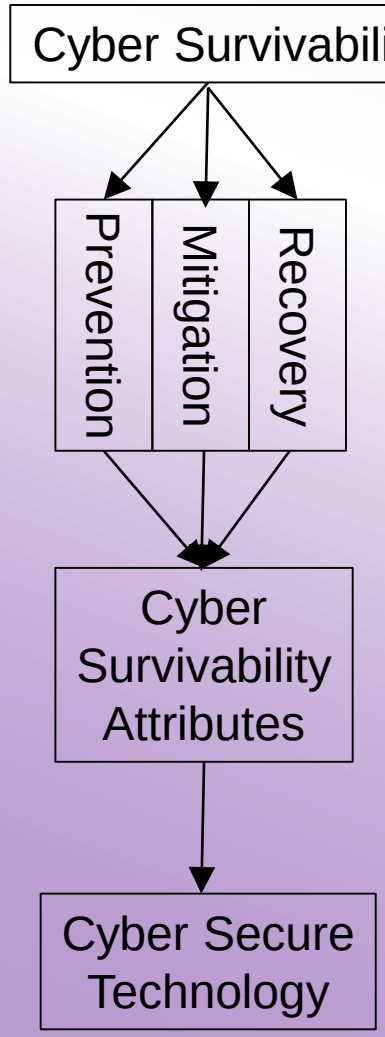
↓

- Cyber Survivability became a warfighting capability requirement for joint warfighting systems!

↓

- June 2015: Joint Requirements Oversight Council initiated development of Cyber Survivability Endorsement process for inclusion in the mandatory SS KPP

Key Cyber Survivability Dependencies for Warfighting Systems



Specific System Survivability Warfighting Capability

Key Operational Capabilities Against a Tier of the Threat Actor Capabilities of Concern to the System

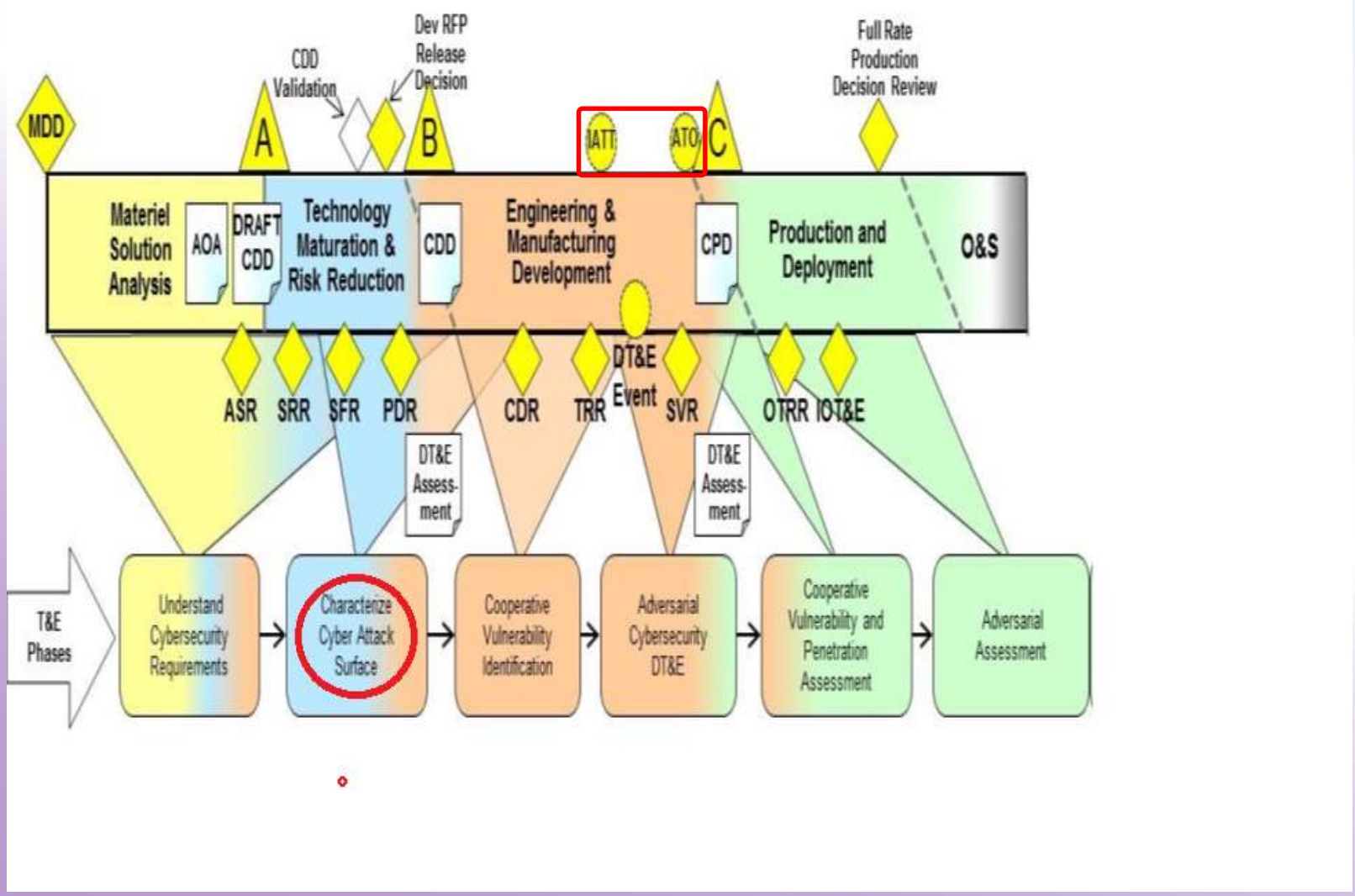
Risk-Managed Performance Measures For SS KPP

Effective Implementation of Technology

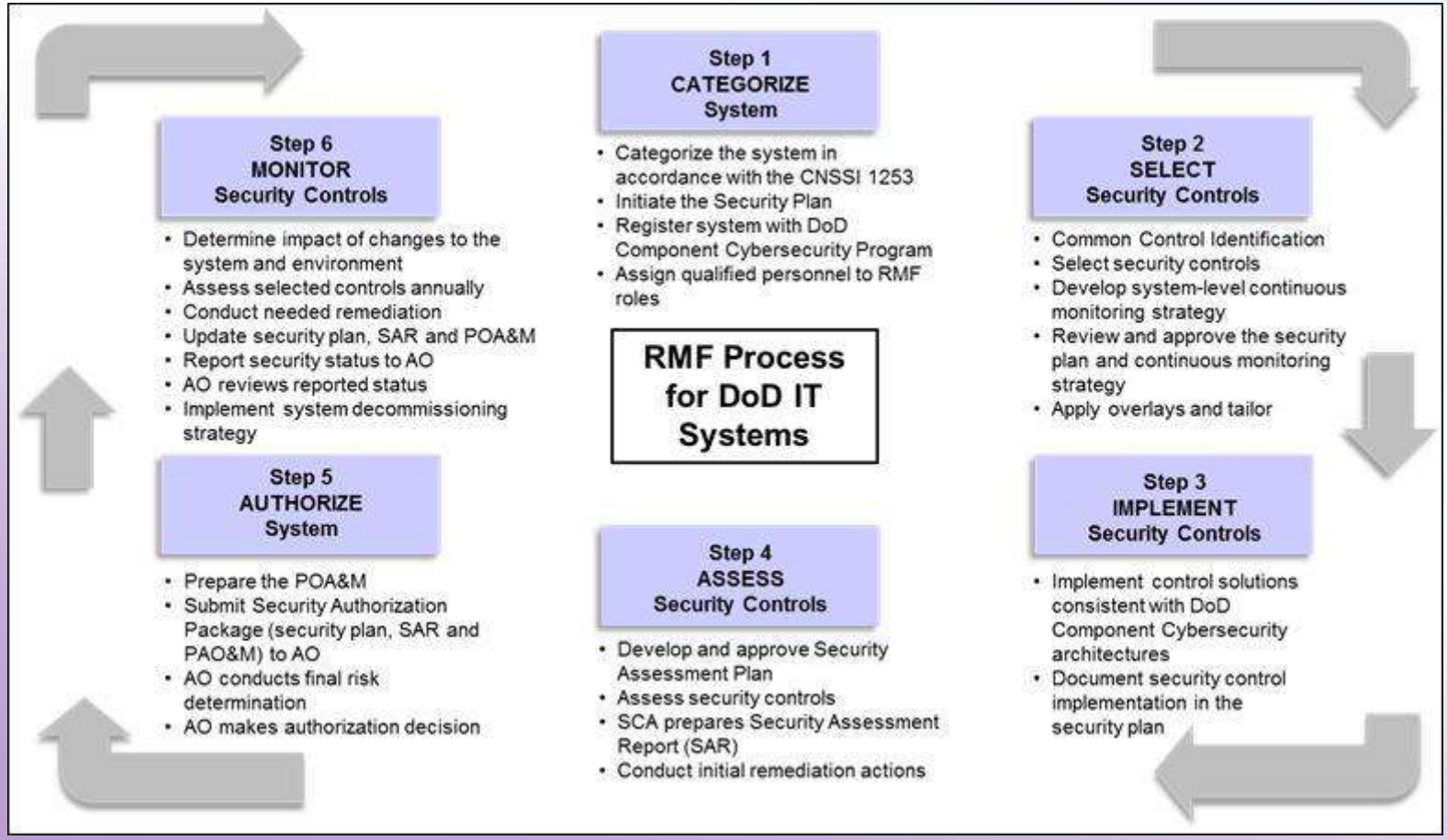
Prevention of Cyber Attack Cyber Survivability Attributes

- Control access (01)
- Reduce cyber detectability (02)
- Secure data exchanges within the system and between the system and other systems (03)
- Protect system's information from exploitation (04)
- Protect mission critical functions (05)
- Minimize and harden attack surfaces (06)

Addressing the Prevention Capability



Risk Management Framework Process



Characterize the Cyber Attack Surface Activities

- Identify the cyber-attack surface
- Review RMF artifacts to help identify the attack surface
- Analyze the attack surface
- Understand roles and responsibilities
- Consider host environment
- Formulate test strategy

Example Elements of Cyber Attack Surfaces

Communications

1. Wired
- Coaxial, Fiber, ISDN, Power Line Carrier

2. Wireless
- Wi-Fi (802.11 a/b/g/n), WiMAX (802.16), LMDS, DECT, Ultra-wideband, Bluetooth

3. Cellular
- 3G, 4G, CDMA, TDMA, GSM, UMTS, PHS, HSDPA, SMS

4. Public Switched Telephone Network
- Class 1 (Regional Center), Class 2 (Sectional Center), Class 3 (Primary Center), Class 4 (Toll Center), Class 5 (Local Exchange)

5. Tactical Radio Systems
- HF, HF-ALE, VHF, UHF, SHF

6. Trunked Radios
- TETRA, MPT-1327, APCO, iDEN, GSM-R

7. Satellite Communications
- Broadband Global Area Network, Globalstar, Iridium, Thuraya, VSAT

Software

8. Link & Network Protocols
- IPv4, IPv6, ICMP, MAC, PPP, ATM, SDLC, ARP, HDLC, Frame Relay, X.25

9. Transport & Application Protocols
- TCP, UDP, DCCP, SCTP, VoIP, FTP, HTTP, IMAP, IRC, NTP, POP, SIP, DHCP, SMTP, SNMP, SSH, Telnet, TLS/SSL

10. Datalink Messages & Formats
- VMF, Link-16, Link-11, USMTF, SCDL, UTH-Gold, JREAP-C, MADL, IFDL

11. Operating Systems
- Linux, Windows, INTEGRITY, LynxOS, iOS, Android

12. Host Server & Control Software
- Cisco IOS, JunOS, RTOS, Unique DCS software, router/switch software

13. Service-Oriented Architecture (SOA) Services
- SOAP, REST, CORBA, WCF, DDS

Hardware

14. Local Devices
- Removable media, flash drives

15. Local Ports
- USB, RS-232, Firewire

16. Components & Subsystems
- Processors, network controllers, encryption devices

Mitigation of Cyber Attack Cyber Survivability Attributes

- Baseline and monitor systems and detect anomalies (07)
  - Monitor cybersecurity configuration baseline for anomalies
  - Support timely response to anomaly's effects to minimize damage and preserve minimum essential functions needed for mission completion
  - Facilitate operator intervention to sustain functions
- Manage system performance if degraded by cyber events (08)
  - Maintain minimum performance required from the system before unacceptable mission consequences occur.
  - Avoid sudden, unrecoverable or catastrophic failures
  - Enable mitigations of cyber-attack effects
  - Continue to perform mission critical functions

Recovery from Cyber Attack Cyber Survivability Attribute 09

- Applies to overall force rather than individual system
- Focus on completing the mission while under attack
- Accomplish mission-by-mission
- Solution may be outside of cyberspace
  - Tactics, Techniques, and Procedures
  - Alternate systems
- Challenges
  - Developing capability requirements & associated contractual language
  - Implementing and executing test scenarios

Warfighting Systems Cyber Resiliency

- Built into Prevention
- Mitigation includes the resiliency to complete the mission
- Recovery includes the resiliency to recover to a state that enables the warfighting system to fight another day
  - Restored to the fully operational configuration defined prior to the mission
  - Restored to a state that adds mitigation for threats encountered during the previous mission **or**
  - Restored to a risk managed level accepted by the Commander to send it out on another mission

Key Insights

- DODIN cyberspace operations critical to providing info needed by warfighting systems to perform their mission
- Cyber Survivability is becoming a top-level requirement for warfighting systems
- Understand Cyber Survivability key operational capabilities of Prevention, Mitigation, Recovery
- Understand how Cyber Resiliency is included in Prevention, Mitigation, and Recovery

Questions

BACKUP SLIDES

Cyber Attack Surface View

- Minimize (minimize cyber attack surface) vulnerabilities during development through effective System Engineering
- Protect (identify cyber attack surface) against vulnerabilities through developed controls (Select, Implement, Assess Controls)
- Ensure (monitor cyber attack surface) systems engineers understanding
- Develop process and procedures for addressing cyber attack.
- Analyze the impacts of exposed cyber attack surface (resiliency and recovery)

References

Joint Publication 3-12 (R) Cyberspace Operations, 5 Feb 2013

The Joint Force Commander's Guide to Cyberspace Operations, Joint Force Quarterly, 2014, 2nd Quarter

Air Force Civilian Cyber Fundamentals Course

Joint Capabilities Integration and Development System Manual, 18 Dec 2015

DoD Cybersecurity Test and Evaluation Guidebook, 1 Jul 2015

DoDI 5000.02 Operation of the Defense Acquisition System, 2 Feb 2017

AFMC/A3 Short Course: Test and Evaluation of Cyber Capability Requirements in Aircraft & other Weapons Systems

NIST Special Publication 800-59, Guideline for Identifying an Information System as a National Security System

Joint Chiefs of Staff. October 2016. Cyber Survivability Endorsement Implementation Guide. Draft, version 1.0 (UNCLASSIFIED//FOR OFFICIAL USE ONLY).

National Security Systems Criteria for Federal Agencies

- Any **information system** used or operated by an agency or by a contractor, or other organization on behalf of an agency
  - Intelligence activities
  - Cryptologic activities related to national security
  - Command and control of military forces
  - **Equipment that is an integral part of a weapon or weapons system**
  - Critical to the direct fulfillment of military or intelligence missions
  - **Not used for routine administrative and business applications**