



Cybersecurity as an Integral Part of Systems Engineering

October 26, 2017



Bill Decker
Kim Kendall
Defense Acquisition University
7115 Old Madison Pike
Huntsville, AL 35806
kim.kendall@dau.mil
256-922-8143

www.DAU.mil

Approved for Public Release




Ground rules

- This is a discussion, not a lecture
- Your opinions and viewpoints are welcomed
- There are no right/wrong answers



Agenda

- Introduction
 - Risk Management
 - Technical Risk
 - Cyber
 - Differences/similarities
 - Conclusion
- 

Traditional Risk Management

- Identify potential risks
 - FMEA, team, etc.
- Risk Management
 - Criticality analysis
 - Root cause analysis
 - Potential consequence
 - Document in a risk statement (If-Then)
 - Identify risk reduction efforts (cost – benefit)
 - Track risk mitigation over time
 - Categorize (green, yellow, red) for management



Cyber risk management

- Identify the criticality of the system
- Use to determine which controls are applied
 - Risk reduction?
- Rinse and repeat on a regular basis

Table 6: RMF for DoD IT Activities Throughout the Life Cycle

Life Cycle Event	RMF for DoD IT Activities
ASR	<ul style="list-style-type: none"> • Categorize the information types • Select security control (SC) baseline • SC trace to the preliminary system performance specification • Incorporate SC requirements into the TMRR system performance specification and SOW
SRR	<ul style="list-style-type: none"> • Refine derived SC system-level requirements • Incorporate into specifications for the technical solution
SFR	<ul style="list-style-type: none"> • Tailor the security controls • Allocate tailored SC into system requirements • Ensure the updated tailored SC requirements are included in the system functional baseline • Incorporate CS functional requirements and verification methods into the initial Development RFP
PDR	<ul style="list-style-type: none"> • Tailor and Allocate SC requirements to the hardware and software design • Incorporate tailored SC requirements into system performance specification, SOW, and other contract documents for Development RFP • Align the security assessment plan with the T&E master plan to ensure inclusion of CS testing
CDR	<ul style="list-style-type: none"> • Tailor and Allocate SC requirements to the hardware and software design • Incorporate tailored SC requirements into system performance specification, SOW, and other contract documents for Development RFP • Align the security assessment plan with the T&E master plan to ensure inclusion of CS testing
SVR/FCA, P&D and O&S Phases	<ul style="list-style-type: none"> • Tailor and Allocate SC requirements to the hardware and software design • Incorporate tailored SC requirements into system performance specification, SOW, and other contract documents for Development RFP • Align the security assessment plan with the T&E master plan to ensure inclusion of CS testing

From Defense Acquisition Guidebook CH 9–3.2.2 Risk Management Framework for DoD IT



How DoD is addressing

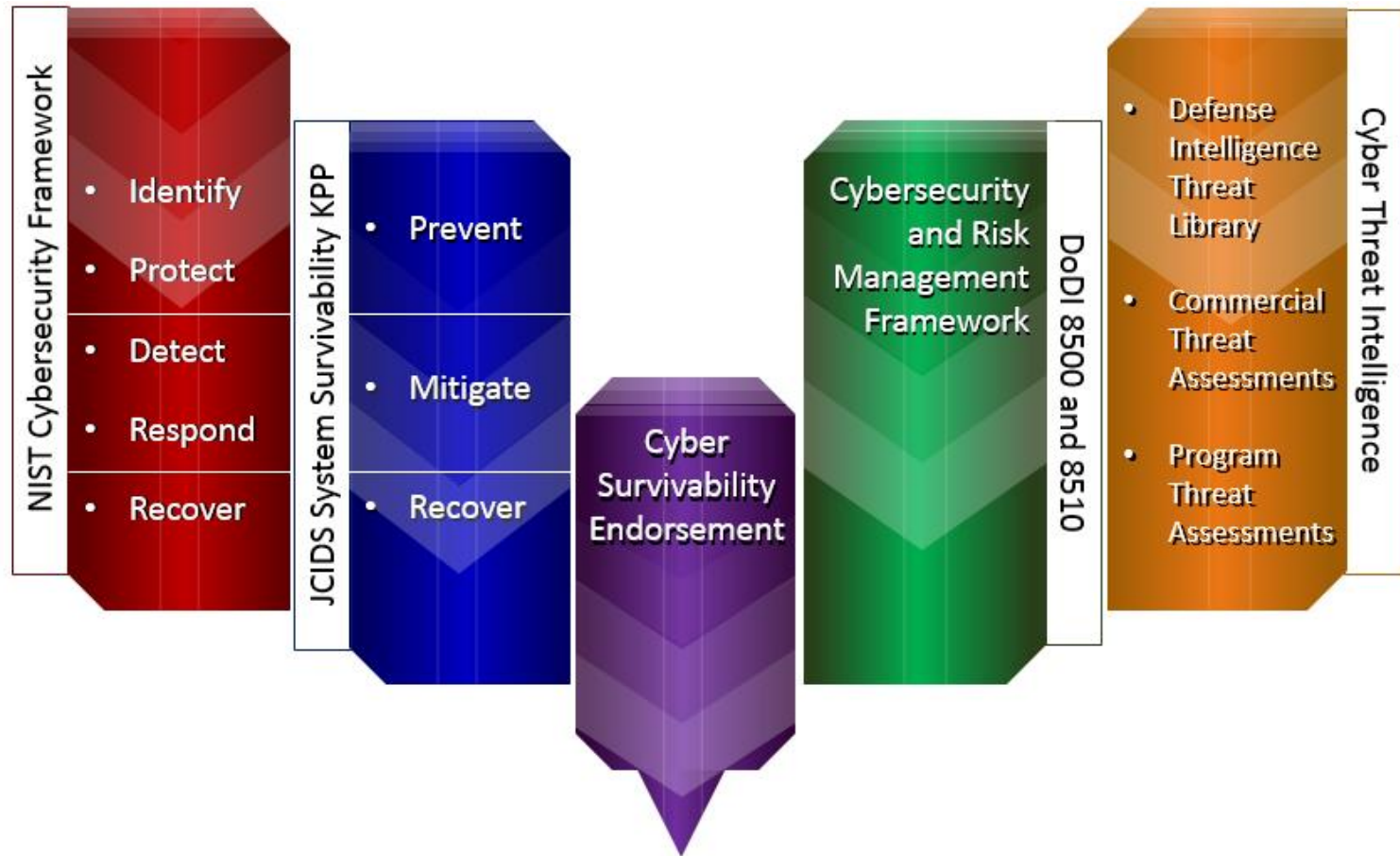
- Next few slides are from an August 2017 briefing by Colonel Dean “Data” Clothier, Chief of the Cyberspace Division, Joint Staff/J-6, title:
“New DoD Approaches on the Cyber Survivability of Weapon Systems”

Background

- **DepSecDef (DSD) directed Joint Staff develop Cybersecurity KPP**
 - Initiated when DSD briefed on DOT&E Cybersecurity Report w/ OUSD(AT&L), OUSD(P), DOD-CIO and VCJCS ... Highlighted multiple weapon systems with vulnerabilities that should have been known and fixed prior to DT&E.
 - Intended to eliminate or sufficiently mitigate known vulnerabilities prior to fielding.
 - Implemented through deliberate design, test and associated DOTmLPF-P in applicable operational environments.
- **Problem:** System survivability requirements not sufficiently articulated for cyber-attack prevention, mitigation and recovery, within requirements documents.
- **Objectives**
 - Drive development of the Joint cyber survivability requirements ... to meet requirements for cyber attack prevention, mitigation and recovery
 - Ensure performance measures are consistent with the threat and consistently applied ... during requirements definition, development and testing
 - Ensure cyber survivability and cybersecurity requirements are considered ... and included as part of the operational risk trade space

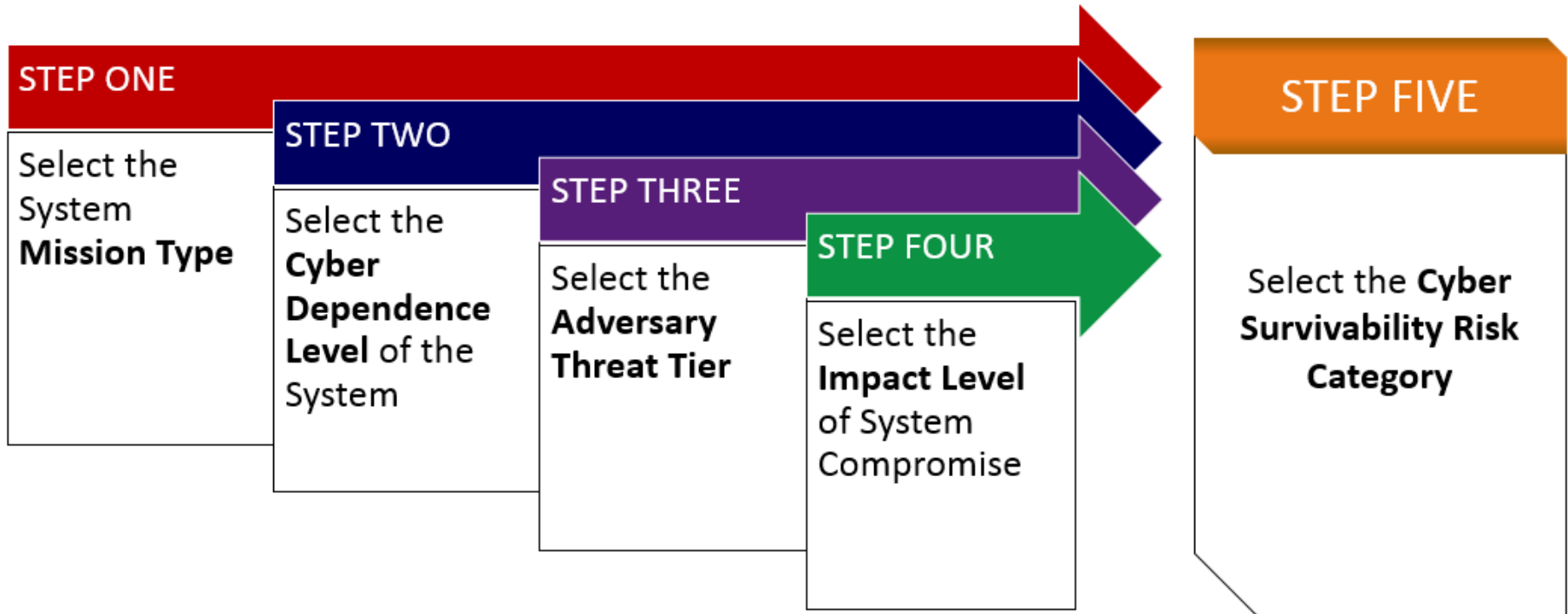
End State: All DoD weapon systems are cyber survivable commensurate with a risk managed approach to countering a capable and determined adversary

Cybersecurity Framework Integration



Risk-Managed, Measureable, Testable, and Implementable Cybersecurity Requirements

Risk Managed Approach



The CSE 5 step risk managed approach takes into account several variables ... the resulting CSRC provides consistency between levels of CS requirements, development and testing

Cyber Survivability Endorsement to the System Survivability KPP

- The Joint Staff and DoD CIO developed Cyber Survivability Endorsement (CSE) criteria to assess requirements for key attributes that increase cyber survivability.

Three Pillars for System Survivability KPP

Prevent

- **Reduced likelihood of being hit**
- Cyber equivalent: Prevent adversary from initiating cyber attack

Mitigate

- **Reduced vulnerability if hit**
- Cyber equivalent: Prevent cyber attack success

Recover

- **Recover critical functions to continue mission**
- Cyber equivalent: Fight through cyber effects, limiting mission harm

Ref: <https://rmfks.osd.mil/rmf/Guidance/RMFRelatedTopics/CybersecurityAndAcquisition/Pages/KeyPerformance.aspx>

Cyber Survivability Attributes to Tailor in the CDD/CPD

SS KPP Pillars (Mandatory)	Cyber Survivability Attributes (CSA) (All are considered, select those applicable)
Prevent	CSA 01 - Control Access
	CSA 02 - Reduce Cyber Detectability
	CSA 03 - Secure Transmissions and Communications
	CSA 04 - Protect Information and Exploitation
	CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels
	CSA 06 - Minimize and Harden Cyber Attack Surfaces
Mitigate	CSA 07 - Baseline & Monitor Systems, and Detect Anomalies
	CSA 08 - Manage System Performance if Degraded by Cyber Events
Recover	CSA 09 - Recover System Capabilities
<u>All 3 KPP Pillars</u>	CSA 10 - Actively Manage System's Configuration to Counter Vulnerabilities

- **Prevent** – Design requirements that protect weapon system's functions from most likely and greatest risk cyber threats.
- **Mitigate** – Design requirements that detect and respond to cyber-attacks; enabling weapon systems functions resiliency to complete the mission.
- **Recover** – Design requirements that ensure minimum cyber capability available to recover from cyber attack and enable weapon system quickly restore full functionality

Fundamental to the CSE construct is enabling sponsor to select and articulate CSA choices to achieve each SS KPP Pillar

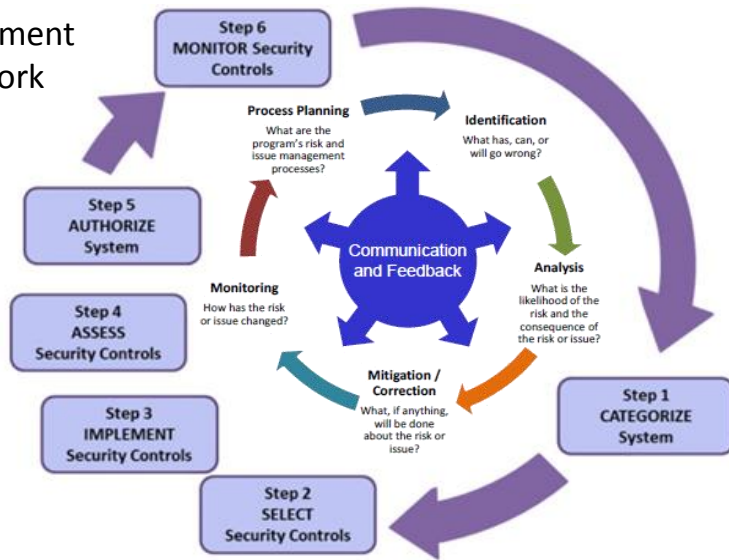
Wrap-Up

- **Problem:** System survivability requirements not sufficiently articulated for cyber-attack prevention, mitigation and recovery, within requirements documents
- **CSE Implementation Guide Objectives:** Joint Staff led effort, with active participation from OSD-CIO, OUSD(AT&L), OUSD(I), DOT&E, DIA, and NSA.
 - **Drives development of Joint cyber survivability requirements** ... to meet requirements for cyber attack prevention, mitigation and recovery.
 - **Incorporates high level cybersecurity exemplar statements** ... prior to the availability of DIA or Service development of system specific threat assessments.
 - **Defines Cyber Survivability Risk Category (CSRC)** ... to enable a consistent approach to cybersecurity requirements, development and testing.
 - **Outlines Cyber Survivability Attributes (CSAs)** ... to be **considered** by requirement sponsors, which can be **consistently** applied, **implemented** by system security engineers, and **tested** by DT&E/OT&E.
 - **Provides Exemplar Requirements and Scorecard** ... support development and assessment and management of requirements.
- **Due out shortly (Fall 2017)**

End State: All DoD weapon systems are cyber survivable commensurate with a risk managed approach to countering a capable and determined adversary

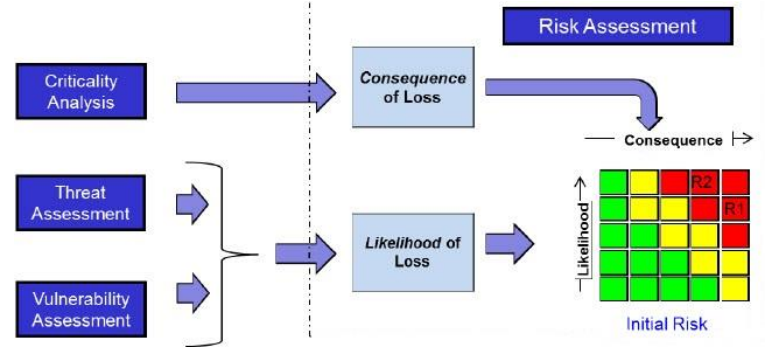
Risk Management Integration

Cybersecurity
Risk
Management
Framework
(RMF)



Risk, Issue, and Opportunity Management

Program
Protection and Trusted Systems & Networks
(TSN)



TSN Analysis

Cybersecurity



Discussion

- Does this help?
- What will be the disconnects?
 - Vocabulary (CSE, controls, etc.)
 - Still delegated to “cyber guy/gal”
- What would be gained (lost) if we used traditional RM processes



Conclusion/recommendations

- Cyber requirements difficult to quantify
 - CSE approach will help – guide coming Fall 2017
 - Vocabulary/processes still not the same for cyber and other threats
 - DoD recognizes the problem
 - Challenge is rationalizing the two systems
 - Debate on whether to use one approach for both
- 