New DoD Approach on the Cyber Survivability of Weapon Systems

***Don Davidson*,**
Acting Director Cybersecurity Risk Management
In the Office of the Deputy DoD-CIO for Cybersecurity

CAPT J. Steve Correia
Chief, Cybersecurity Branch
Joint Staff/J-6

Mr. Steve E. Pitcher, GS-15
Cyber Survivability Lead
Joint Staff/J-6

CSE is the Critical Foundation for Ensuring Cyber Survivability is Considered as Part of the Operational Risk Trade-Space

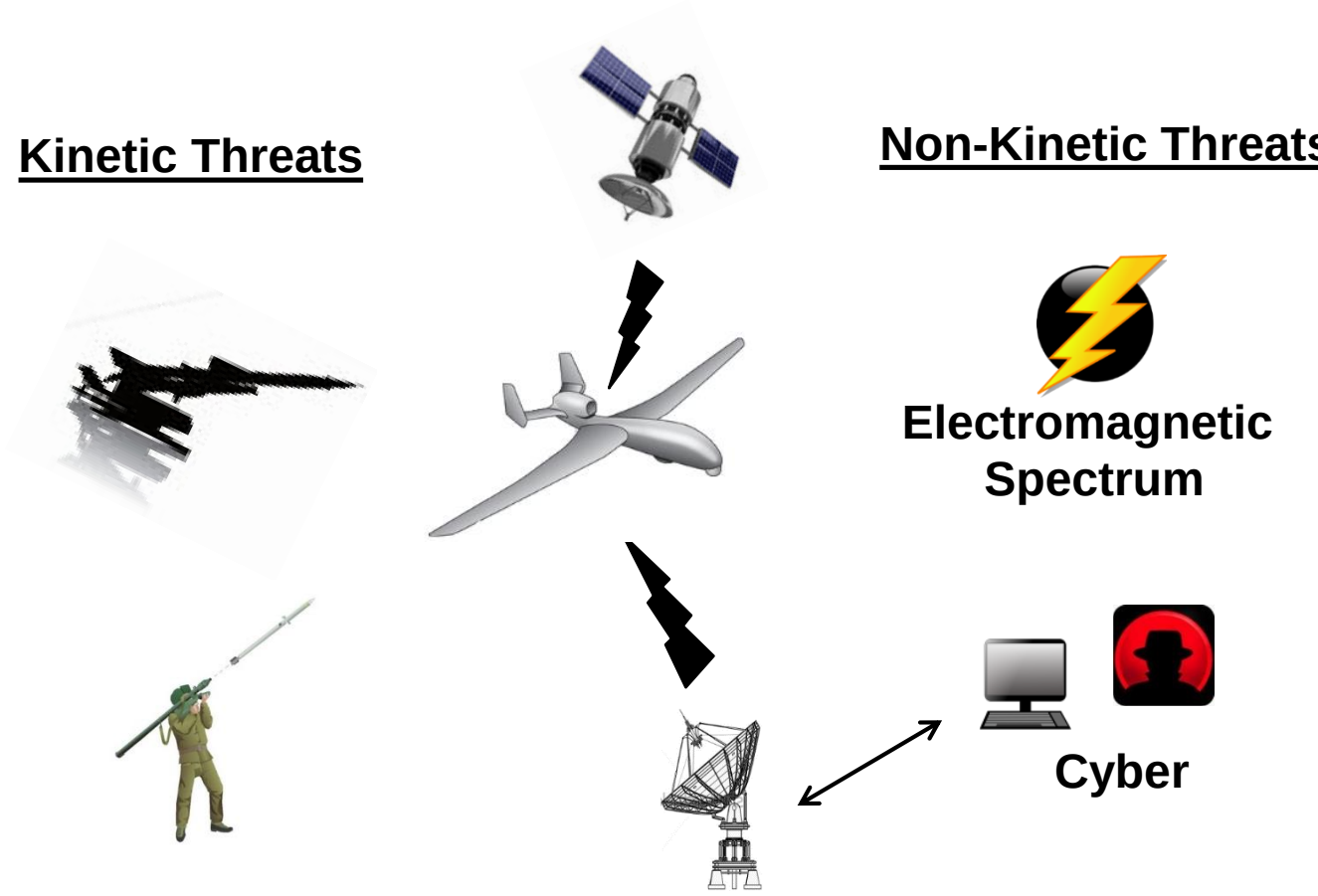
Background

- **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.
  - Known vulnerabilities: continue to be “re”found in operational systems.
  - Cyber security guidance: Program Offices have been unable to maintain compliance at “mission” relevant speeds (IAVAs, Non-IAVAs, STIGs, CTOs, CVEs).

JROCM 059-15: approved development of the CSE and encouraged Services to nominate programs as test cases for CSE development

Cyber Survivability Endorsement (CSE)



Sponsors must address the System Survivability KPP and provide specific Cyber Survivability Attributes (CSA) related to the SS KPP which must be met - 18 December 2014 JCIDS Manual, Enclosure D

Where Are Today

- **CSE Implementation Guide Objectives:**

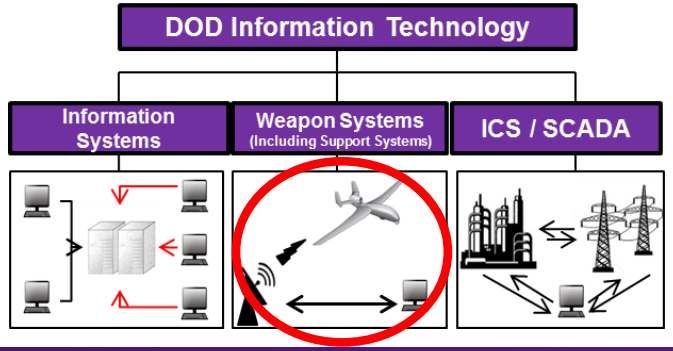
  Joint Staff led effort, with active participation from OSD-CIO, OUSD(AT&L), OUSD(I), DOT&E, DIA, and NSA. Published Jan 2017.

  - **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.

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

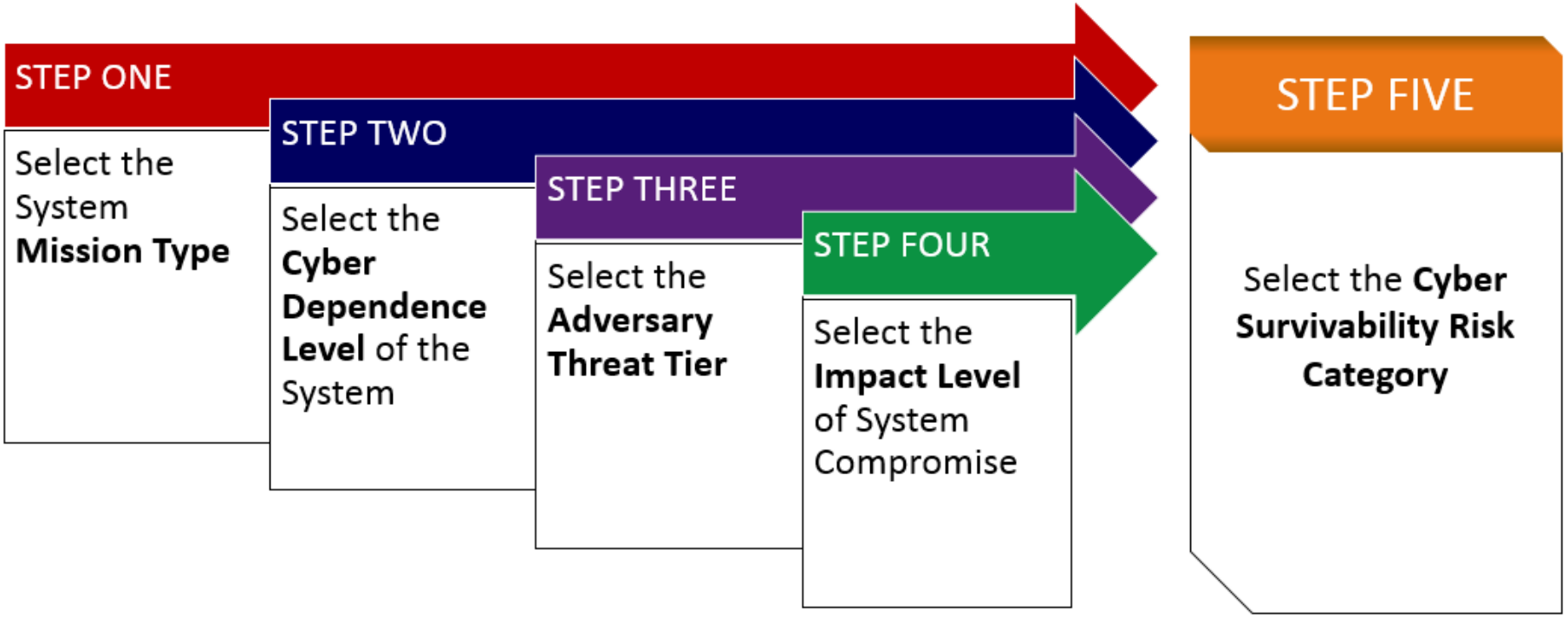
Cyber Survivability Endorsement (CSE)

- **Added Cyber Survivability to the JCIDS System Survivability (SS) Key Performance Parameter (KPP)**
  - Cyber survivability is now part of operational risk trade-space (as of 18 Dec 2014 JCIDS Manual)
- **CSE Implementation Guide: Joint Staff led effort with active participation from DoD CIO, AT&L, DOT&E, OUSD(I), DIA, and NSA.**
  - Provides cyber survivability exemplar statements
  - Includes cyber survivability attributes to aid requirement definition
  - Describes tailoring approach for Capabilities Development Document (CDD) and Capabilities Production Document (CPD) requirements



Build new weapon systems that are cyber survivable commensurate with a risk managed approach to countering a capable and determined adversary

Risk Managed Approach

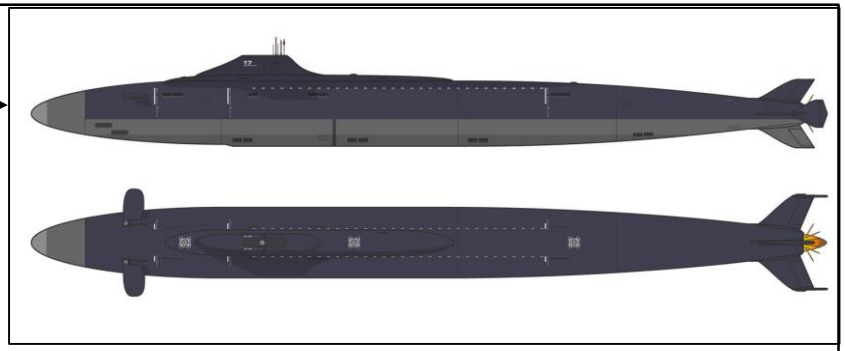


The CSE 5 step risk managed approach takes into account several variables … the resulting CSRC provides consistency between levels of CS requirements, development and testing

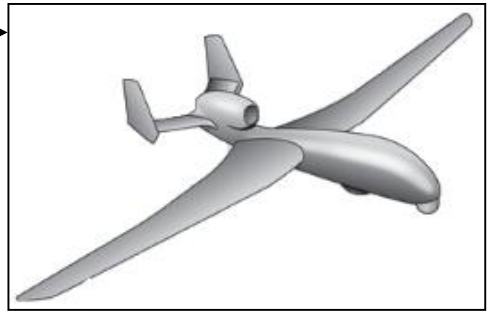
STEP 1: *System Mission Types*

Example

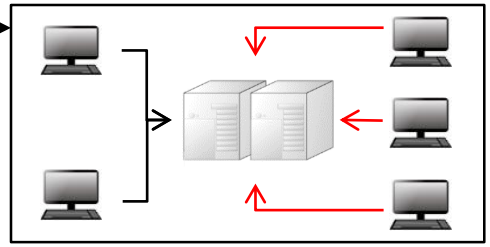
MT 4 – Strategic / National
Systems whose degradation would result in the highest risks to achieving national objectives, require the very best cybersecurity practices



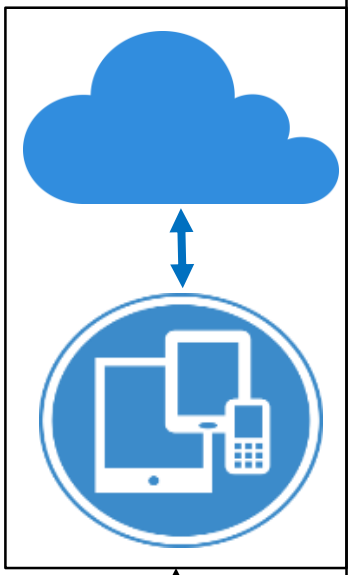
MT 3 – Operational / Tactical
Mission systems, munitions, Command and Control capabilities that require unique DoD protections



MT 2 – Military Critical
Selected high impact systems that ensure near-continuous operation with rapid recovery from failures



MT 1 – Mission Essential
Military and Organizational Support systems; may be hosted within DoD or commercial facilities



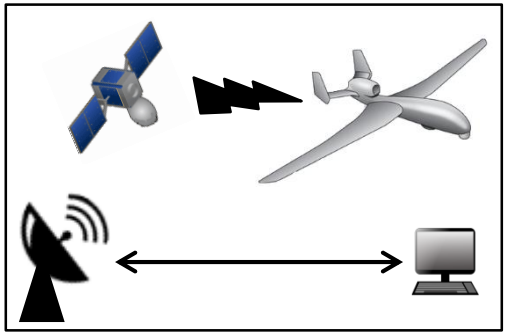
Determining the System Mission Type helps define the required cyber survivability protection for the capability

STEP 2: *Cyber Dependence*

Criticality Analysis provides basis for cyber survivability emphasis for critical functions, components and information exchanges

Example

Determine the Mission Critical Functions of the System



1 – Sustain Flight / Maneuverability

2 – Maintain Internal/External Communication

3 – Perform Offensive / Defensive Activities

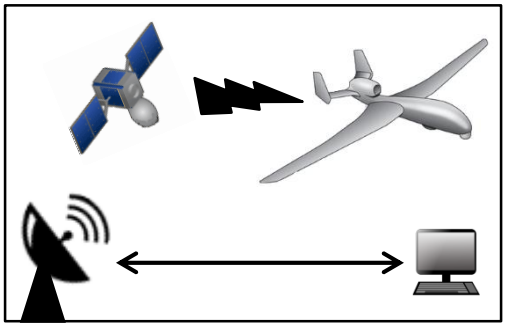
What is a System's Cyber Dependence to Perform its Mission Critical Functions?

STEP 3: *How Select Threat Actors*

What level of cyber actor must the system be capable of withstanding if it is to fulfill its warfighting purposes?

Example

Cyber Threat Actor Capability Level



Tier IV	Advanced
Tier III	Moderate
Tier II	**Limited**
Tier I	Nascent

*NOTIONAL SCORING

IF Insurgent & Irregular Forces, THEN

Determine the Level of Most Capable Cyber Threat Actor to the System

Adversary Threat Tier Taxonomy

There are numerous threat tier models, but we were able to work with DIA and OUSD(I) to gain support for declassifying the following standardized four tier adversary threat model.

ATT 1 – Nascent: Little-to-no organized cyber capabilities, with no knowledge of a network's underlying systems or industry beyond publicly connected open-source information.

ATT 2 – Limited: Able to identify and target-for espionage or attack-easily accessible unencrypted networks running common operating systems using publicly available tools.

ATT 3 – Moderate: Able to use customized malware with better OPSEC practices to conduct wider-range intelligence collection operations, gain access to more isolated networks, and create short-duration effects against critical infrastructure networks.

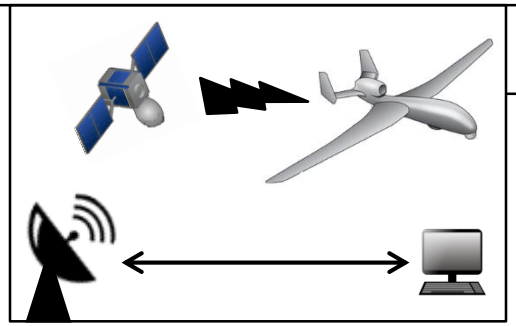
ATT 4 – Advanced: Have the capacity to conduct complex, long-term cyber-attack operations that combine multiple intelligence disciplines to obtain access to high-value networks.

Threat Assessment Reports (TAR) need to include a consistent capability taxonomy that describes specific adversary capabilities and preferred approaches for each step of the cyber kill chain

STEP 4: *Mission Impact*

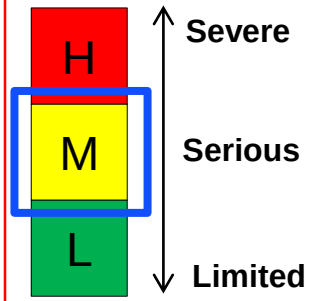
Critical Function I: What is the mission impact of compromised flight or maneuverability due to a cyber attack?

Example

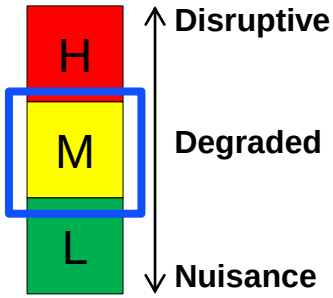


Mission Critical Functions
I Sustained Flight / Maneuverability
II Internal / External Communication
III Offensive / Defensive Capabilities

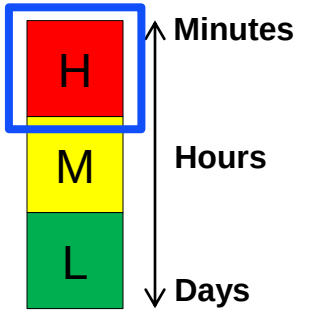
Confidentiality



Integrity



Availability



*NOTIONAL SCORING

- **Confidentiality** – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **Integrity** – Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity
- **Availability** – Ensuring timely and reliable access to and use of information

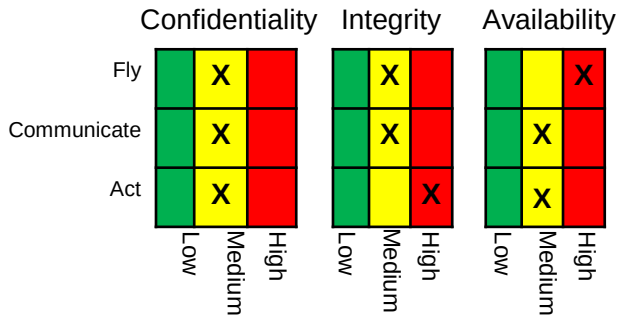
Determine the Mission Impact of Loss For All Mission Critical Functions Due to a Cyber Event

STEP 5: *System Survivability Risk*

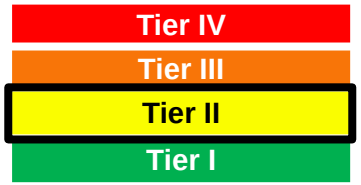
The aggregation of the System Risk and the Threat Actor inform the level of System Security Engineering & Controls applied and the Residual Operational Risk assumed based on the purpose and intended operational environment of the system

Example

Systemic Vulnerability



Factor Cyber Threat Actor for the UAV System

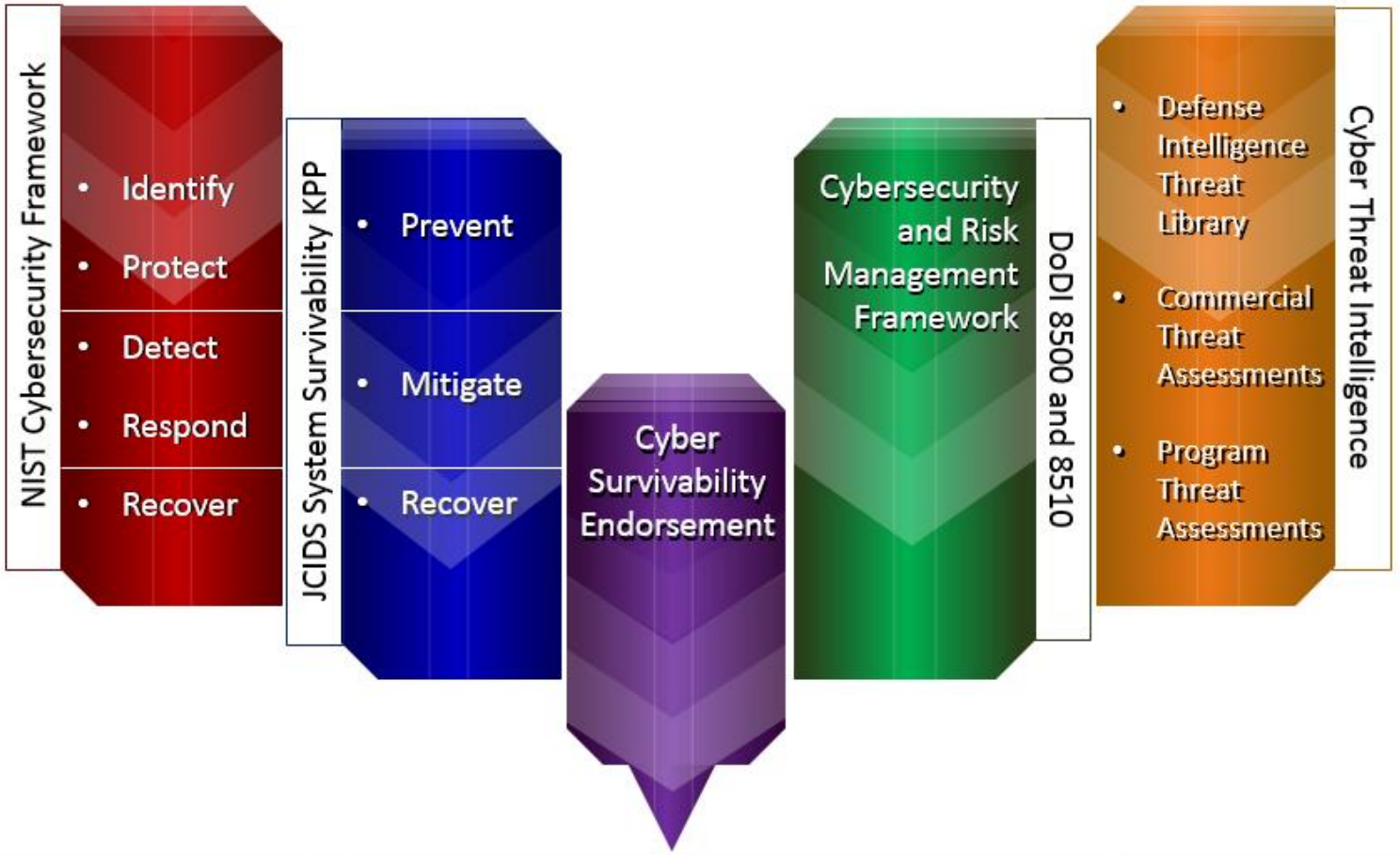


System Survivability Risk

*NOTIONAL SCORING

Vulnerability in the face of Threat Capability yields Survivability Risk

Cybersecurity Framework Integration



Cyber Survivability Attributes and the RMF

- **Reviewed ~800 NIST 800-53 Cybersecurity Technical Controls**
  - Supports the Risk Management Framework (RMF)
  - Consist of 17 Control Families
  - Enable periodic testing of security requirements
  - Vary in specificity and CSE applicability
- **Identified 239 NIST controls potentially applicable to CSE CSAs**
  - 98 Highly Applicable
  - 86 Somewhat Applicable
  - 55 Require Interpretation
- **CSE Implementation Guide - Volumes 2 and 3:** the Joint Staff is working with OSD-CIO and NSA-IAD to develop Volumes 2 and 3. These volumes provide additional detail the Acquisition and Test communities can use to tailor and test recommended cybersecurity technical controls associated with applicable CSAs. The level of cyber hardening acquired and tested is directly related to and consistent with the Cyber Survivability Risk Category selected.

CSE leverages NIST 800-53 cybersecurity technical controls, to enable easier understanding and implementation by cybersecurity professionals

ICD "CSRC 3" Exemplar:

Integrates Cyber Requirements (black text) *and Threat* (blue text)

The mission's criticality and impact of system compromise requires that the capability must survive and operate in a cyber-contested environment against the span of anticipated adversaries and threat actors that range from the amateurs and unorganized cyber criminals to very sophisticated, persistent, and well-resourced adversaries at a nation state level, capable of advanced cyber trade craft to exploit known and unknown vulnerabilities, as well as the ability to develop and stealthily implant vulnerabilities (includes lower threat tier capabilities). The capability must include sufficient resiliency as appropriate for the mission, and mission profiles supported, to complete the mission in the event of cyber-attacks and effects by the anticipated adversaries. This capability's survivability must include mitigations for C, I, & A compromises of internal and external information flows. Recognizing the adversaries' current and projected cyber threat capabilities and cyber-attack tactics, techniques and procedures, the capability must leverage available DoD cyber protections, to include consideration of protections inherited from the capability's intended operational environment, leverage available DoD developed protection technologies, and as needed, build specific custom protections, countermeasures, and technologies. These protections should include, at a minimum, a defense-in-depth architecture, considering the inherited protections. Cyber Survivability Attributes, which must be assessed for each AoA alternative and tailored for system-specific architectures are:

Cyber Survivability requirement statement *needs to incorporate a high level "projected cyber threat"* … based on the CS Risk Category "template" assessment

Cyber Survivability Attributes to Tailor in the CDD/CPD

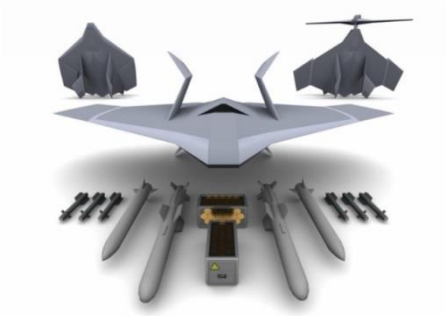
SS KPP Pillars (Mandatory)	Cyber Survivability Attributes (CSA) (All are considered, select those applicable)
Prevent	**CSA 01 - Control Access**
	CSA 02 - Reduce Cyber Detectability
	CSA 03 - Secure Transmissions and Communications
	CSA 04 - Protect Information and Exploitation
	CSA 05 - Partition and 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**
***All* 3 KPP Pillars**	**CSA 10 – Actively Manage System's Configuration to Counter Vulnerabilities**

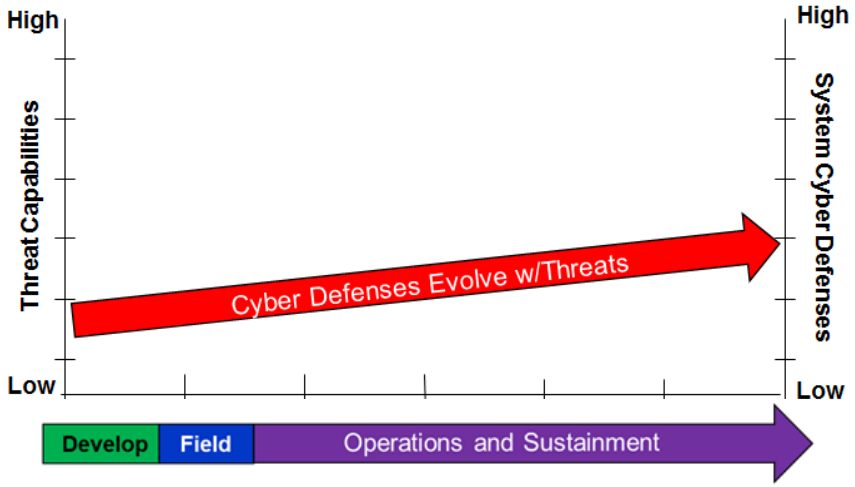
- **Prevent** – Design requirements that protect weapon system's functions from most likely and greatest risk cyber threats.
- **Mitigate** – Design requirements that detect and respond to cyber-attacks; enabling weapon systems functions resiliency to complete the mission.
- **Recover** – Design requirements 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 KKP Pillar

Systemic Ability to Adapt to New Cyber Threats

- Systems must be capable of quickly adapting to new cyber threats
- Sustaining a system's cyber survivability requires elements in the resourcing, design, Life Cycle Sustainment Plans, and Ops & Maintenance procedures





Cyber threats will continue to increase in capability for the foreseeable future

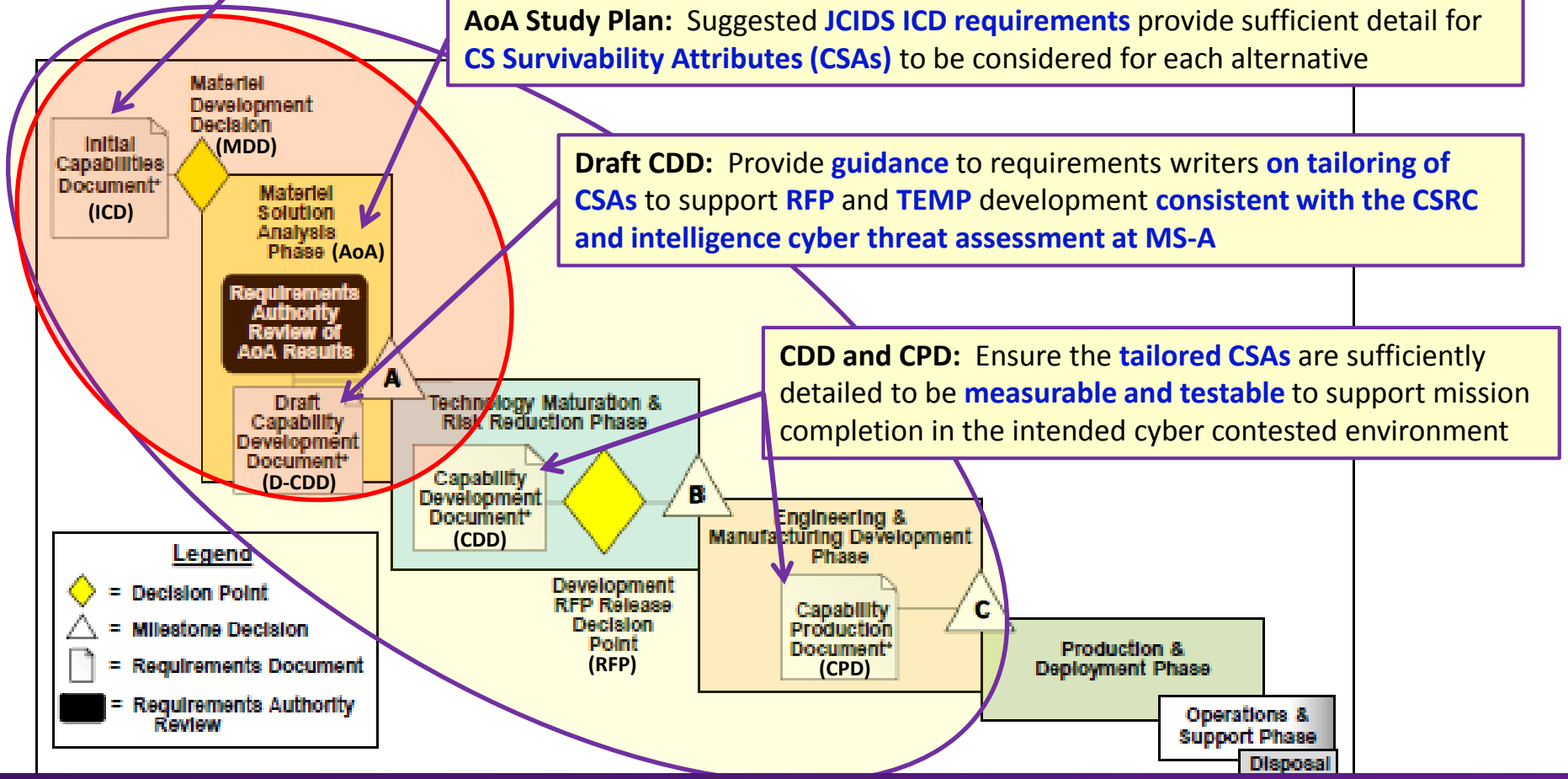
CSE's Greatest Impact Opportunity

ICD: Suggest **"exemplar" Cyber Survivability (CS) requirements** statement incorporates the **"projected cyber threat"** … consistent with the **CS Risk Category (CSRC) assessment**

AoA Study Plan: Suggested **JCIDS ICD requirements** provide sufficient detail for **CS Survivability Attributes (CSAs)** to be considered for each alternative

Draft CDD: Provide **guidance** to requirements writers **on tailoring of CSAs** to support **RFP** and **TEMP** development **consistent with the CSRC and intelligence cyber threat assessment at MS-A**

CDD and CPD: Ensure the **tailored CSAs** are sufficiently detailed to be **measurable and testable** to support mission completion in the intended cyber contested environment



If the ICD and AoA Study Plan addressed cyber survivability, then greater likelihood of identifying preferred solution that meets requirements, is cyber survivable and is cost effective to secure … The CDD/CPD work would also be substantially easier

Wrap-Up

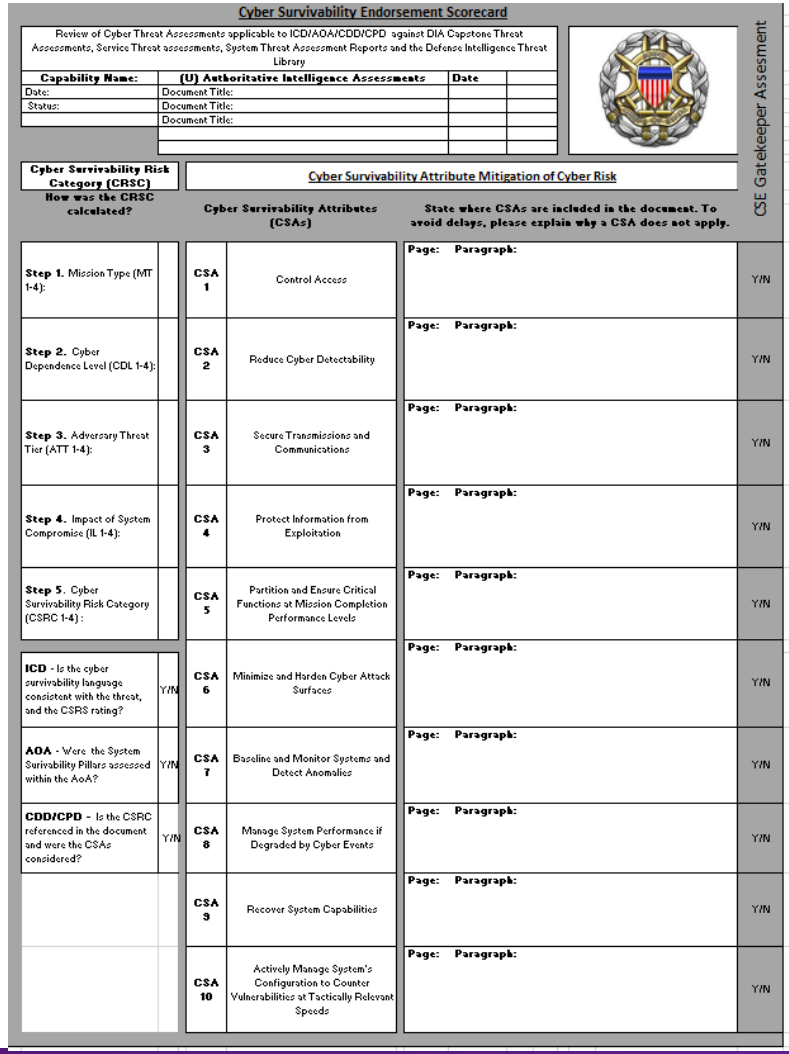
- **Problem:** System survivability requirements not sufficiently articulated for cyber-attack prevention, mitigation and recovery, within requirements documents
- **CSE Implementation Guide Objectives:** Joint Staff led effort, with active participation from OSD-CIO, OUSD(AT&L), OUSD(I), DOT&E, DIA, 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.

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

BACKUP

CSE Scorecard Assessment Process

- **Requirement Sponsors** use the Cyber Survivability Scorecard to document that appropriate CSAs have been considered, and where they are articulated within requirement's documents.
- **CSE analysts** use the Cyber Survivability Scorecard to review ICDs, and assess CDDs and CPDs entered into KM/DS with JROC Interest, JCB Interest, or qualify as Joint Integration.
- **CSE assessment** occurs during the 21 day Document Review and commenting stage within the JCIDS deliberate staffing process.



Cyber Survivability Endorsement Scorecard

Review of Cyber Threat Assessments applicable to ICD/AOA/CDD/CPD against DIA Capstone Threat Assessments, Service Threat assessments, System Threat Assessment Reports and the Defense Intelligence Threat Library

Capability Name:	(U) Authoritative Intelligence Assessments	Date	
Date:	Document Title:		
Status:	Document Title:		
	Document Title:		

CSE Gatekeeper Assesment

Cyber Survivability Risk Category (CRSC) How was the CRSC calculated?		Cyber Survivability Attributes (CSAs)		Cyber Survivability Attribute Mitigation of Cyber Risk: State where CSAs are included in the document. To avoid delays, please explain why a CSA does not apply.	
Step 1. Mission Type (MT 1-4):		CSA 1	Control Access	Page: Paragraph:	Y/N
Step 2. Cyber Dependence Level (CDL 1-4):		CSA 2	Reduce Cyber Detectability	Page: Paragraph:	Y/N
Step 3. Adversary Threat Tier (ATT 1-4):		CSA 3	Secure Transmissions and Communications	Page: Paragraph:	Y/N
Step 4. Impact of System Compromise (IL 1-4):		CSA 4	Protect Information from Exploitation	Page: Paragraph:	Y/N
Step 5. Cyber Survivability Risk Category (CSRC 1-4) :		CSA 5	Partition and Ensure Critical Functions at Mission Completion Performance Levels	Page: Paragraph:	Y/N
ICD - Is the cyber survivability language consistent with the threat, and the CSRS rating?	Y/N	CSA 6	Minimize and Harden Cyber Attack Surfaces	Page: Paragraph:	Y/N
AOA - Were the System Survivability Pillars assessed within the AoA?	Y/N	CSA 7	Baseline and Monitor Systems and Detect Anomalies	Page: Paragraph:	Y/N
CDD/CPD - Is the CSRC referenced in the document and were the CSAs considered?	Y/N	CSA 8	Manage System Performance if Degraded by Cyber Events	Page: Paragraph:	Y/N
		CSA 9	Recover System Capabilities	Page: Paragraph:	Y/N
		CSA 10	Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds	Page: Paragraph:	Y/N

CSE Scorecard is a management tool to help guide requirements development, and streamline review process to ensure CSAs are logically considered and articulated