DoD's Cyber Survivability Endorsement

JCIDS System Survivability KPP, Cybersurvivability Endorsement (CSE) Implementation Guide v3 (Publicly Releasable), 30 July 2022

Mr. Steve Pitcher, GS-15, CISSP, CEH
JS Senior Cyber Survivability Analyst
Requirements Division, Joint Staff/J6

13 Apr 2023

Things You Will Get From This Brief

- Why Cyber Survivability Endorsement (CSE)
- Hidden Costs/Risks of No System Specific Cyber Requirements
- Challenges: Integration and Long Lifecycle Risks
- Reducing Resource/Mission Risks – Throughout Lifecycle
- Cybersecurity Compliance Necessary, but Not Sufficient
- How to Apply CSE
- Voluntary CSE Adoption
- Way Ahead

How the CSE Framework can provide a holistic approach for describing system specific and threat informed cyber survivability threshold performance requirements (incl. ZT, AI/ML)

Why Cyber Survivability Endorsement (CSE) Created

Joint Staff added CSE to System Survivability Key Performance Parameter (SS KPP) in 2017

- **Trigger:** DepSecDef tasking based on annual operational test (OT) reports highlighting:
  - ❑ Same "dirty dozen" vulnerabilities found every year … in too many weapon systems
  - ❑ These high risk vulnerabilities were well known … should have been fixed before OT
  - ❑ Fixes would now be harder and more costly … since not identified and mitigated early

Probable Root Causes: Legacy systems' only contractual cyber threshold requirement was to get "*enough cybersecurity compliance*" to obtain an ATO. Despite signed ATOs and 40+ DoDIs for cyber, **(1)** no cyber resilience requirements, **(2)** no adapt resourcing to achieve and **sustain** a meaningful cyber risk posture, and **(3)** no actionable cyber threat to justify cyber protections for resource sponsor action…

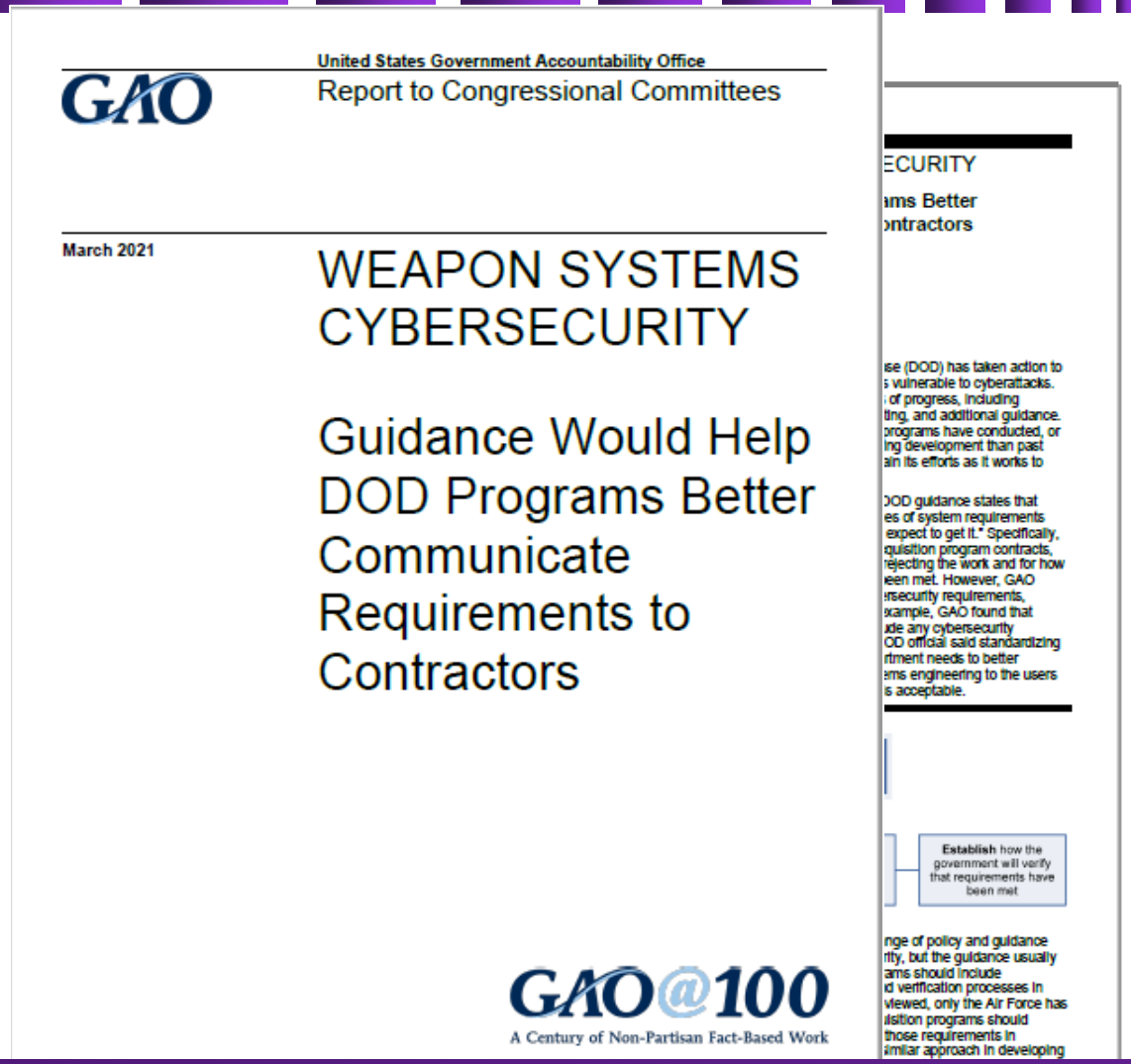
- **Question:** Is a system with 90% RMF cybersecurity compliance more survivable than 70% compliance?
  - ❑ Depends on the risks accepted in each system's move, shoot and communicate functions…

CSE addresses these root causes and places cyber within the same operational risk trade-space with other system *functionality* (cost, schedule and *performance*)

Why CSE Needed - GAO Report 21-179

GAO 21-179 Findings:

- **DoD has increased use of cyber assessments**
  - MAY help programs identify vulnerabilities earlier.
  - BUT vulnerabilities found in multiple rounds of testing … went unaddressed after first discovered.
- **Guidance would help DoD programs better communicate requirements to contractors**



United States Government Accountability Office

Report to Congressional Committees

March 2021

WEAPON SYSTEMS CYBERSECURITY

Guidance Would Help DOD Programs Better Communicate Requirements to Contractors

GAO@100

A Century of Non-Partisan Fact-Based Work

CSE defines contractually binding cybersecurity and cyber resilience threshold performance requirements … BUT only mandatory for Joint Systems … Not Service, MTA, JUON

Why CSE Focused on Acquisition Performance Requirements

Cyber Survivability Endorsement (CSE)

System's **tailored threshold performance requirements** for both cybersecurity and cyber resilience to **Prevent**, **Mitigate**, **Recover** from and **Adapt** to Cyber Events

JCIDS Manual and DoDI 5000.90 Acquisition Requirements

Cybersecurity Standards

System deemed sufficiently compliant with established standards, by a Risk Acceptance Official

(Not system specific … not threat informed)

Authorized to Operate (ATO)

≠

System Survivable

DoDI 8510.01 Specified Requirements

People
Processes
Tech

Cyber Resilience Engineering

- Trustworthy information resources
- Ready for degradation/loss
- Operations have means to prevail
- Mission focused – not system focused

System Resilience

DoDI 8500.01 Implied Requirements

Mission Assurance

Need to define Success (specific requirement & threat informed performance) … To achieve it

Hidden Costs/Risks – No System Specific Cyber Requirements

% Funds Committed	70% Of Funds Committed prior to Design	85%	95% Of Funds Committed prior to most defects being found …

Data from: Defense Systems Management College

Acquisition Phases	Concept/Reqs	Design	Code	Test	Integration
When are defects introduced?	35%	35%	20%	8%	2%
When are defects found?	1%	2%	17%	46%	34%
Cost to correct	.03%	.3%	2%	35%	62%

Data from: "ROI Analysis of the System Architecture Virtual Integration Initiative", SEI, 2018

90% of Defects Introduced
Early - Result of Poor Cybersecurity and Cyber Resilience Requirements

80% of Defects Found
Too late and too costly to correct … risks potentially unacceptable

97% of Rework Costs
Identified after 95% of funds committed…

Cyber Survivability Threshold Performance Requirements … must be considered at each Acq milestone, flow down to engineering specifications & validated during developmental testing!

Hidden Costs/Risks – Loss of Trust and Intellectual Property

Russia: cyber + kinetic
- Disable government, private websites during Russo-Georgian War

2008

China: stealing data
- Exfil technical program data from defense contractors

Stuxnet: digital weapon
- Compromised PLCs of Iranian nuclear centrifuges
- Destroyed > 1000 centrifuges (20% of inventory)

2010

2012

China: critical infrastructure
- Target oil, natural gas pipelines in US

Jeep hack: remote control
- Hackers demonstrate control of a running Jeep from miles away

2015

Russia: cyber + kinetic
- Cyber attack during Ukraine war
- Power outage for 230K people

2017

Maersk: collateral damage
- Russian Cyber attack against Ukraine affects Maersk
- Global operations halted for weeks
- ~$10B in damages to multiple firms

Solar Winds: supply chain hack
- Trojanized IT management software compromised multiple gov't agencies

2020

- ❑ There are few instances of truly "disconnected" systems
- ❑ Many DoD systems use well-known commercial hardware and open source software modules https://www.youtube.com/watch?v=MK0SrxBC1xs for the 2015 Jeep hack
- ❑ See SIPRNet - Navy's "Project B++" destroyer hack https://Intellipedia.intelink.sgov.gov/wiki/B++

This slide stolen (with thanks) from the Navy N2/N6 brief - RO Course

Highlights a few Cyber Exploits taken from Open-Source Information

Anything with a processor is, and HAS BEEN, a potential target

Hidden Costs/Risks – Loss of Warfighting Advantage

Russia

US

China

US

US

China

US

China

This slide stolen (with thanks) from the Navy N2/N6 brief - RO Course

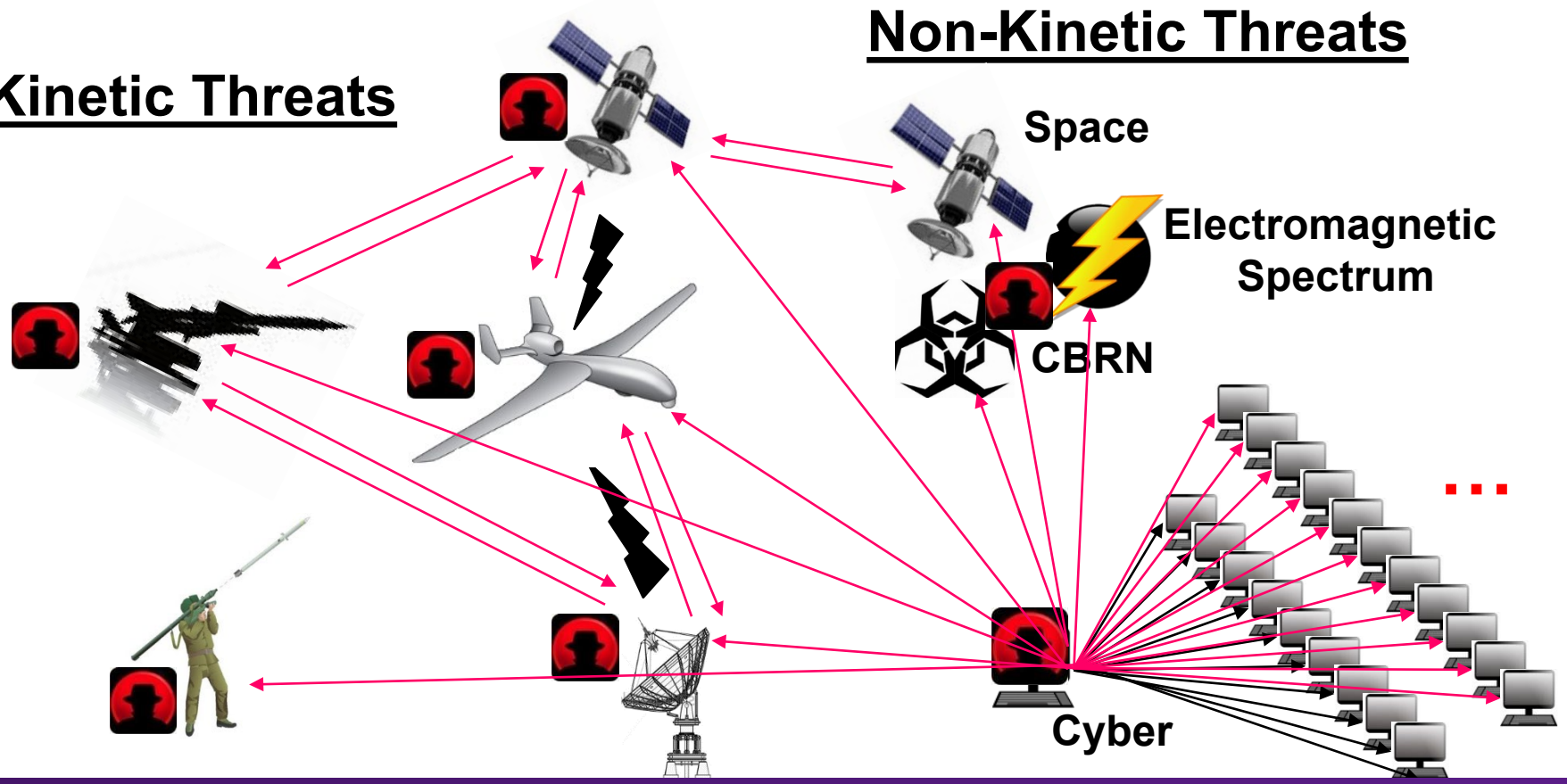
Highlights a few Cyber Exploits taken from Open-Source Information

Adversaries are eroding our warfighting advantage through DIB cyber compromises

Challenges: External Integration/Connectivity Risks

Today's more interconnected and cyber-contested environment

Cyber threat is NOW time sensitive, with serious operational risk implications



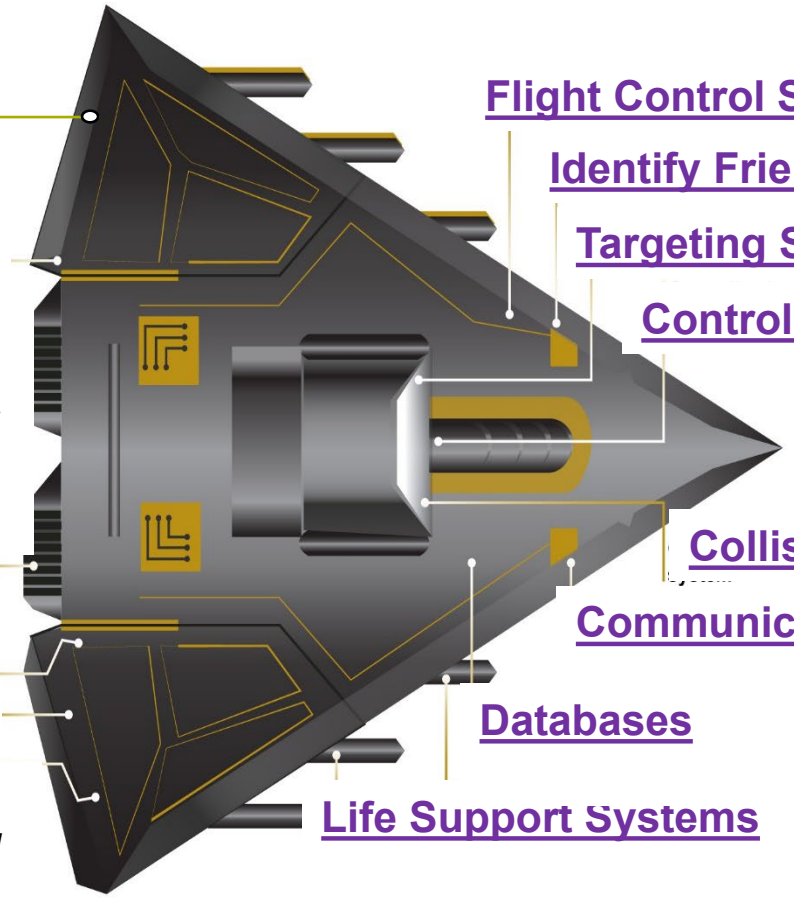
BEFORE: 1++ kinetic bullets needed to achieve 1 kinetic kill

NOW: 1 cyber "bullet" can achieve 1+++ mission kills, IF similarly connected/configured…

*** Buying more systems no longer guarantees resiliency or mission assurance ***

Challenges: Internal Integration/Connectivity Risks

(Pervasiveness represented via fictitious weapon system for classification reasons)



Logistics Systems

Maintenance Systems

(including requirements for uploads of mission tasking, inflight status reports and updates over various communication nets after the mission)

Industrial Control Systems

Microelectronics throughout

Flight Control Systems (rudder, thrust, etc.)

Identify Friend or Foe Systems

Targeting Systems

Controller Area Network (CAN) Bus

Collision Avoidance System

Communications Systems

Databases

Life Support Systems

Source: *GAO-19-128 Report: "Weapon Systems Cybersecurity, DoD Just Beginning to Grapple with Scale of Vulnerabilities"*

Source: GAO analysis of Department of Defense information. | GAO-19-128

Cyber Attack Surface is too expansive to be supported by a few Cyber Critical Intelligence Parameters (CIPs)

Functionality **designed for good can also be used for evil – must protect critical** ***functions (move, shoot and communicate)*** **… which** ***must be segregated*** **to complete mission**

Challenges: Long Lifecycle Risks

F-35 Lightning II - Joint Strike Fighter

1993	1996	2001	2006	2009	2015	2022	2050+
Studies for JSF Program begin	2 Contractors Develop prototypes	Contract awarded to Lockheed Martin	First Flight of JSF	**Alleged Chinese espionage**	Entered Service	**Halted Delivery [Chinese alloy in component]**	Replace Fleet

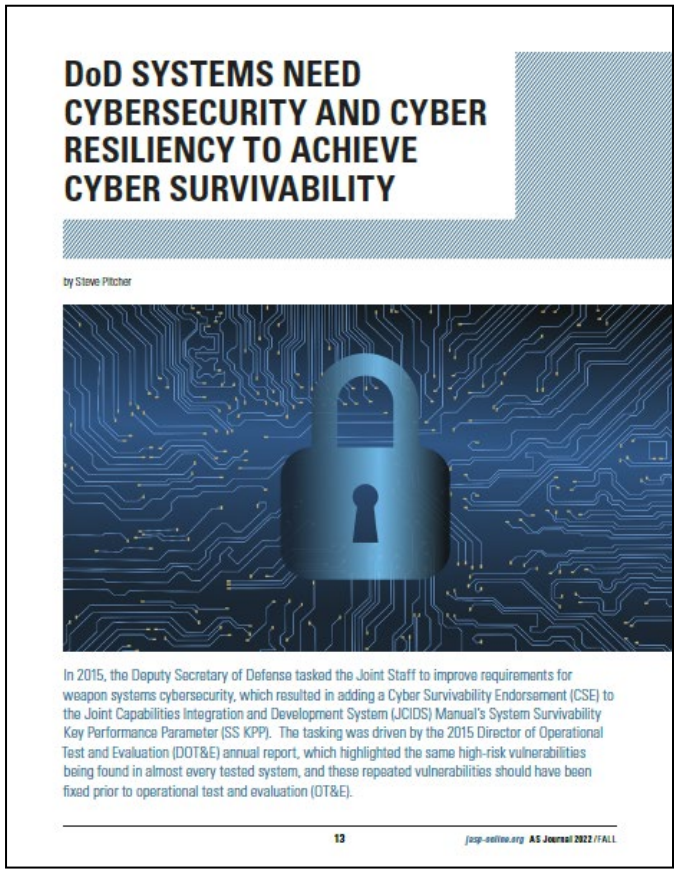
Strategy and Concepts → **Development** → **Acquisition** → **In-Service and Disposal**

Define/Engineer *Cyber Threshold Performance Requirements … With* ***Adapt*** *Component*

Validate Achieving *Cyber Threshold Performance Requirements (DT) and Operational Effectiveness (OT)*

Sustain *Cyber Threshold Performance Requirements … With* ***Adapt*** *Component*

DoD Needs Cyber Survivability for Mission Assurance



DoD SYSTEMS NEED CYBERSECURITY AND CYBER RESILIENCY TO ACHIEVE CYBER SURVIVABILITY

by Steve Pitcher

In 2015, the Deputy Secretary of Defense tasked the Joint Staff to improve requirements for weapon systems cybersecurity, which resulted in adding a Cyber Survivability Endorsement (CSE) to the Joint Capabilities Integration and Development System (JCIDS) Manual's System Survivability Key Performance Parameter (SS KPP). The tasking was driven by the 2015 Director of Operational Test and Evaluation (DOT&E) annual report, which highlighted the same high-risk vulnerabilities being found in almost every tested system, and these repeated vulnerabilities should have been fixed prior to operational test and evaluation (OT&E).

13 jasp-online.org AS Journal 2022 /FALL

Fall 2022 – Aircraft Survivability Journal

https://www.jasp-online.org/asjournal/fall-2022/dod-systems-need-cybersecurity-and-cyber-resiliency-to-achieve-cyber-survivability/

Is there any operational requirement more crucial than surviving long enough to accomplish a mission, or safely return to base for restoral?

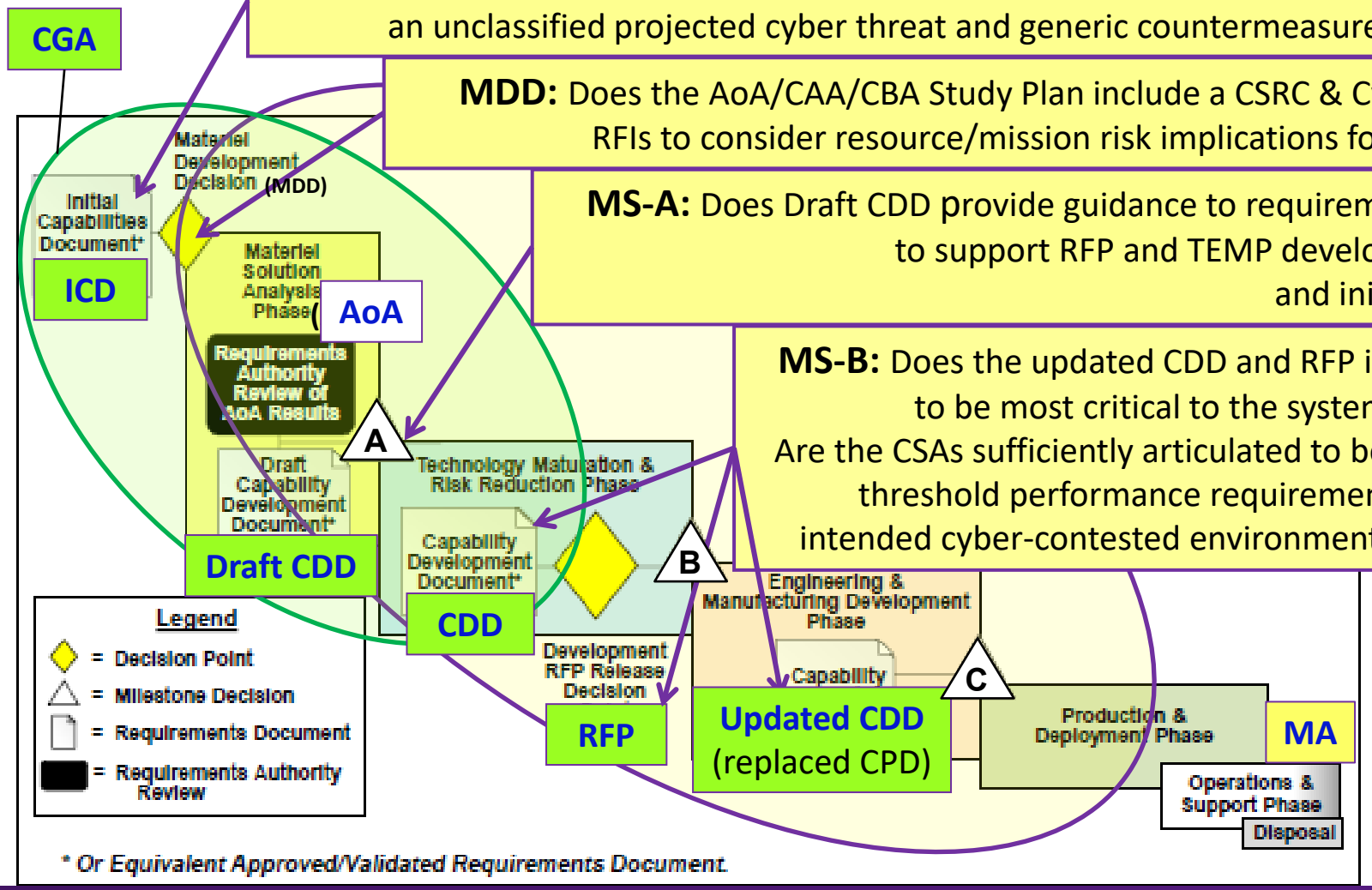
Reducing Resource/Mission Risk … Lifecycle

Resource Sponsor: Does the ICD Cyber Survivability Risk Category (CSRC) summary statement incorporates an unclassified projected cyber threat and generic countermeasures before formal threat assessment?

MDD: Does the AoA/CAA/CBA Study Plan include a CSRC & Cyber Survivability Attributes (CSA) with RFIs to consider resource/mission risk implications for a Rough Order of Magnitude (ROM)?

MS-A: Does Draft CDD provide guidance to requirements writers on tailoring a subset of CSAs to support RFP and TEMP development consistent with the updated CSRC and initial intelligence cyber threat assessment?

MS-B: Does the updated CDD and RFP include a tailored subset of CSAs determined to be most critical to the systems move, shoot and communicate functions. Are the CSAs sufficiently articulated to be decomposed into measurable and testable threshold performance requirements that could support mission completion in intended cyber-contested environment; forming basis for source selection criteria?



AoA: *Analysis of Alternatives*

CAA: *Course of Action Analysis*

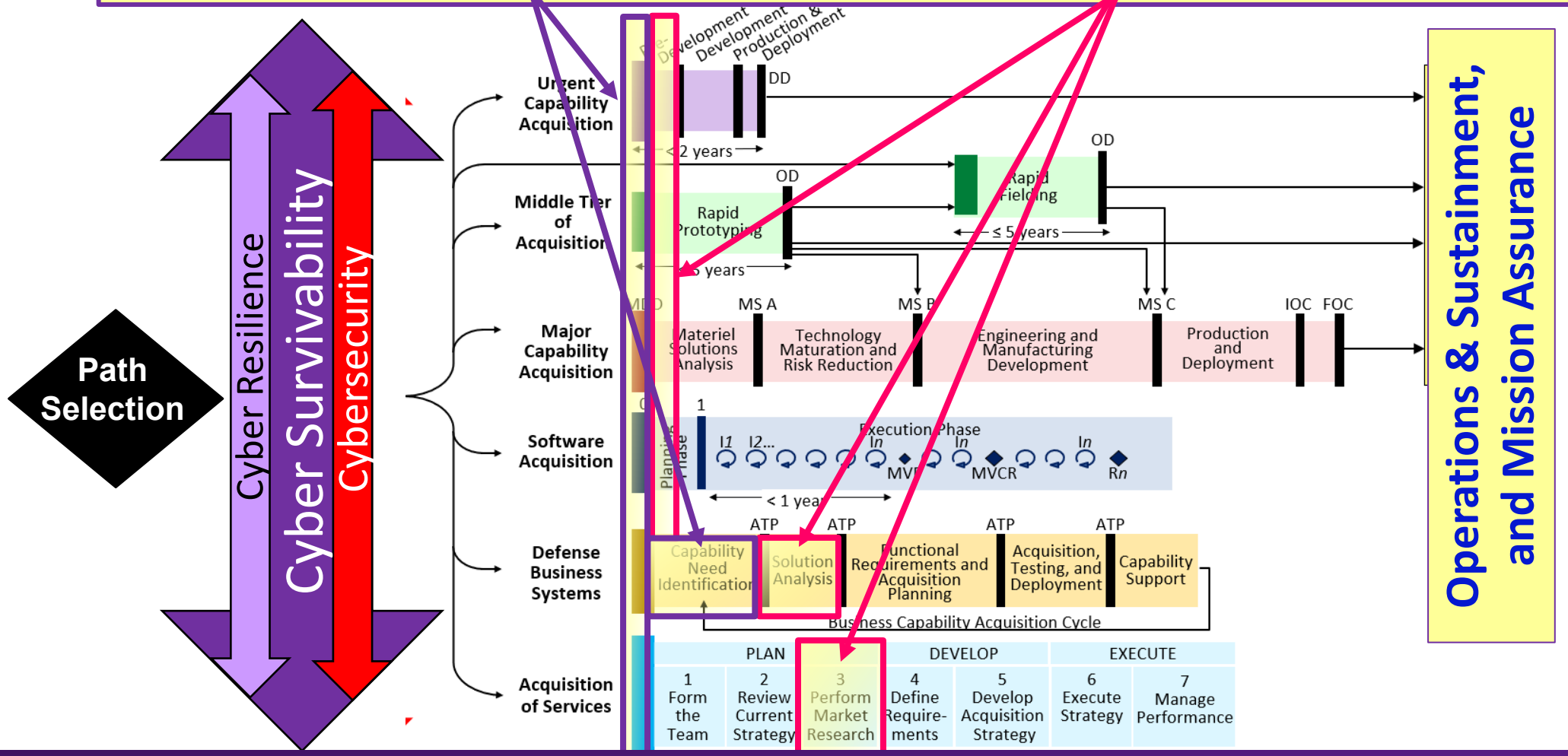
CBA: *Capability Based Assessment*

CGA: *Capability Gap Assessment*

If cyber survivability considered at each knowledge point, the risk of pursuing flawed capabilities can be reduced, along with the cost to mitigate vulnerabilities to achieve and sustain an operationally-acceptable risk posture

Reducing Resource/Mission Risk … All Acquisition Pathways

All acquisition paths define requirements and assess alternatives to reduce resource and mission risk



Cybersecurity and Cyber Resilience Functional Requirements should drive Requests for Information (RFIs) to be considered during any analysis of alternatives and source selection!

Determining CSRC

STEP ONE

Select system's **Mission Type (MT)**

STEP TWO

Select system's expected **Adversary Threat Tier (ATT)**

MT and ATT are the minimum known at **ICD**.

CDL not known until after AoA, ***unless*** an AI/ML or unmanned systems will be required in the ICD

STEP THREE

Select system's **Cyber Dependence Level (CDL)**

AoA should provide sufficient technical detail to identify CDL and refine the CSRC for the selected capability in the **CDD** and **RFP**

STEP FOUR

Select system's **Impact Level (IL)** of compromise or loss

An overall mission impact level is best defined by CCMD mission and OPLAN assessments during Exercises, DCRAs, and Wargames

STEP FIVE

Determine system's **Cyber Survivability Risk Category (CSRC)**

Drives tailoring of a subset of the 10 CSAs determined to be critical to system survivability and its move, shoot and communicate functions, and identifies countermeasures for the expected ATT level.

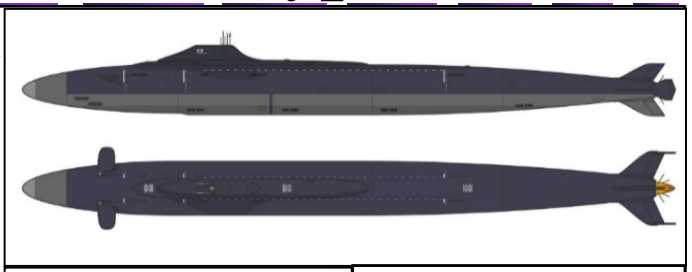
Although CSE leverages RMF categorization, it is not RMF… but it does support the RMF aspects applicable to WSs.

The resulting Risk Category frames the risk tolerance for consistent levels of cyber survivability threshold performance requirements for acquisition, development, testing and operations

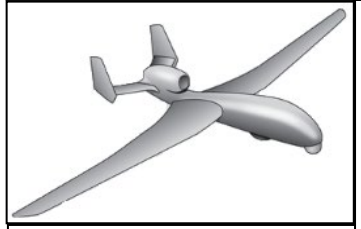
Step 1: Mission Type (MT)

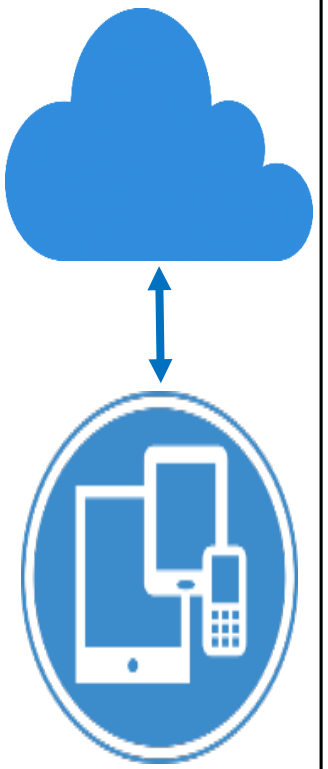
Contested Environment

MT 5 – Strategic / National – Deterrence ***[2+ CCMDs]***
Degradation results in the highest risks to achieving national objectives. (e.g. nuclear weapon platform systems, nuclear munitions and subsystems, ballistic missile radars, nuclear command and control systems/networks, space systems, and capabilities required to maintain nuclear deterrence)



MT 4 – Operational – Before/during 1st 72 hrs [1 CCMD]
Degradation results in high risk to mission completion. (e.g. primary mission systems used in contested environments, munitions, command and control capabilities, mission planning systems, and their supporting comm networks required to ensure mission assurance)





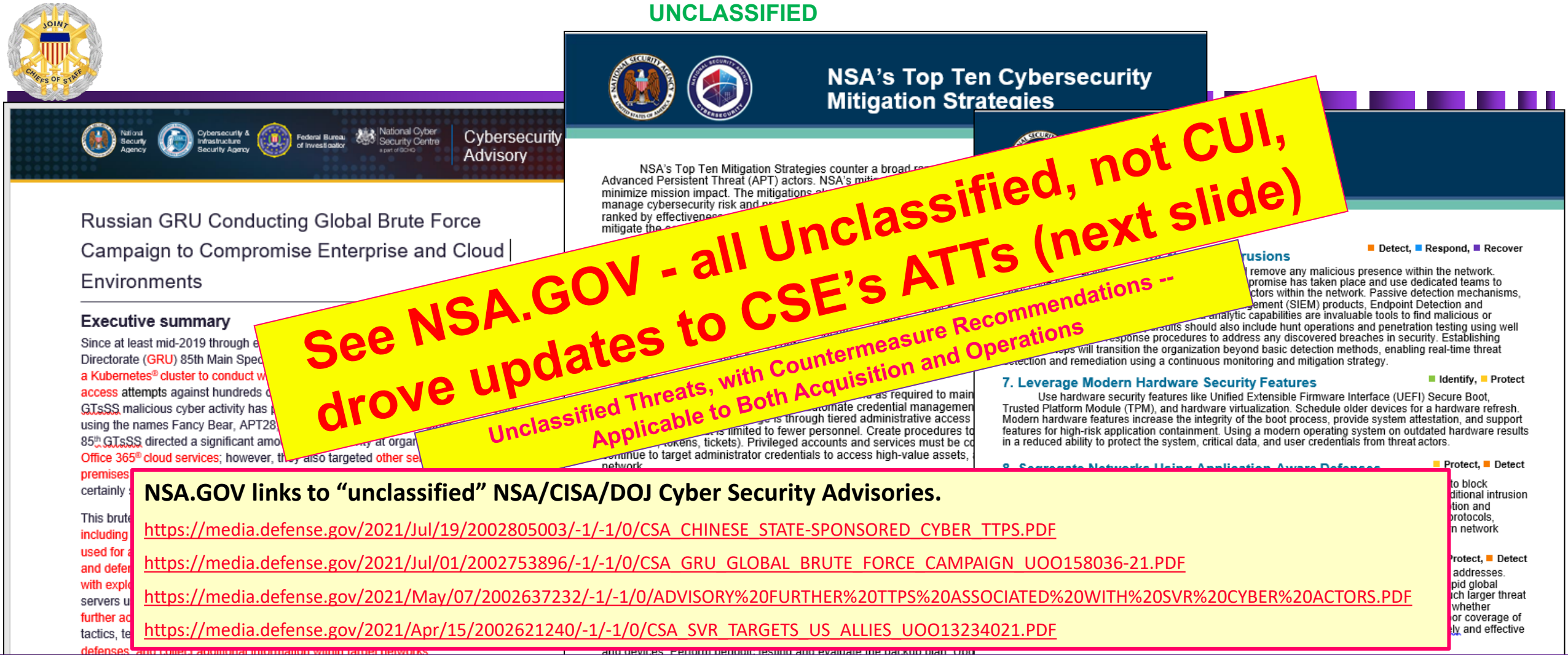
MT 3 – Tactical – Before/during 1st 72 hrs
Degradation results in moderate to high risk to mission completion. (e.g. tactical weapon systems/munitions for contested environments, and their supporting communications networks to ensure mission assurance)

Permissive Environment

MT 2 – Mission Support – After 1st 72 hrs
Degradation results in moderate risk to mission completion. (e.g. mission systems used in permissive environments, logistics systems, and their supporting communication networks to sustain operations)

MT 1 – Organizational Programs & Services
Degradation results in low risk to mission completion (e.g. MWR, finance and accounting systems, and defense health systems)

Determining the system's Mission Type helps understand the system's risk tolerance and define the required level of cyber survivability protections for the capability



NSA.GOV links to "unclassified" NSA/CISA/DOJ Cyber Security Advisories.

https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/0/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF

https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/0/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

https://media.defense.gov/2021/May/07/2002637232/-1/-1/0/ADVISORY%20FURTHER%20TTPS%20ASSOCIATED%20WITH%20SVR%20CYBER%20ACTORS.PDF

https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

Adversary cyber threat has not been sufficient, timely or actionable ... Until now

But need annual unclassified updates … along with classified intel "overlay" of zero-days, supply chain, intent, attribution, changes in adversary threat to link with publicly available information on vulnerabilities, threat, and countermeasure options.

Step 2: CSE Adversary Threat Tiers (ATT)

Adversary Threat Tier → Most Likely & Greatest Risk

ATT 5 – Extreme: (e.g., **Russia SVR, APT-29**). Uses a range of initial exploitation techniques that vary in sophistication, coupled with 'stealthy' intrusion tradecraft to cause denial, degradation, deception, disruption, and destruction of mission capabilities. Uses custom tools, compromised accounts, and system misconfiguration to blend in with normal/unmonitored traffic to move undetected in victim networks. Demonstrated capability to target cloud resources and supply chain (e.g., SolarWinds).

ATT 4 – Advanced: (e.g., **Russia GRU, APT-28; China APT-41**). Conducts complex, long-term cyber attack operations combining multiple intelligence sources to obtain access to high-value networks. After gaining access, combines well known TTPs to move laterally, evade defenses and collect additional info. Uses tools to conduct widespread, distributed and anonymized 'brute force' access to cloud services. Develops detailed target technical knowledge for more damaging attacks.

ATT 3 – Moderate: Sophisticated, persistent, and well-resourced adversaries at nation-state level. Capable of advanced cyber tradecraft to use publicly available tools, develop/use customized malware, and acquire access to some ATT-4/ATT-5 tools to stealthily implant malware/vulnerabilities, conduct wide-ranging intelligence collection operations, gain access to more isolated networks, and in some cases, create limited effects against defense critical infrastructure networks.

ATT 2 – Limited: Capable of limited advanced cyber tradecraft using publicly available and customized tools to exploit known and unknown vulnerabilities. Able to identify -- and target-for espionage or attack -- easily accessible unencrypted networks running common operating systems using publicly available tools. Possesses some limited strategic planning.

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

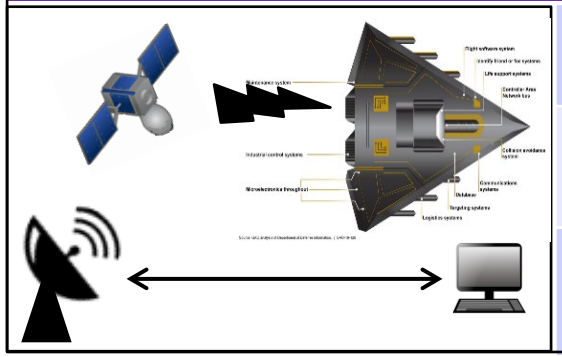
Unclassified & Actionable for ICD and 1st Draft of CDD (prior to VOLT availability)

Sources: GAO analysis of DoD information, GAO-19-128; NSA/Cybersecurity and Infrastructure Security Agency (CISA)/U.S. Department of Justice (DOJ) Cybersecurity Advisories - April and July 2021 for SVR/GRU and APT-41.

Step 3: Cyber Dependence Level (CDL)

Criticality analysis provides basis for intrinsic cyber survivability assessment of critical functions, components and information exchanges -- beyond C-I-A

- **Cyber is digital – 0 or 1** … it does not degrade on a continuous analog scale.
- **Unrealistic to expect to maintain/restore 100%** of a system functions … What can we afford to lose?
- **What system functionality must not be lost** (segregated to complete mission or safely return to base for restoral to a known good condition), and what are its cyber dependencies and the adversary cyber threats driving cyber threshold 'performance' requirements?

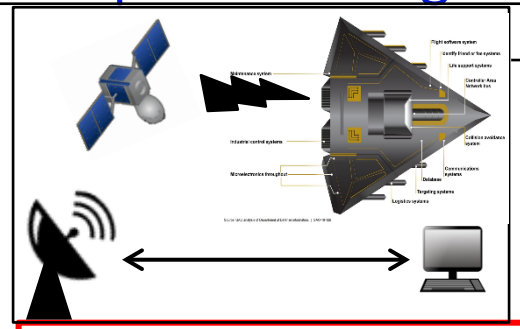
Determine the Mission Critical functions of the system	
	**Move**: Sustain Flight and/or Maneuverability
	Shoot: Perform Mission, including Offensive and Defensive Actions
	Communicate: Maintain Internal and External Communications

Technical Exposure (origin, export, sys architecture), combined with Degree of Connectivity (internal/external operational requirements) → this intrinsic cyber risk defines the CDL

Step 4: Impact Level (IL)

Critical Functions: What are the resource, system and mission risk implications of compromised flight or maneuverability due to a cyber event?

Example



Mission Critical Functions

- **I Move: Sustained Flight / Maneuverability**
- **II Shoot: Offensive / Defensive Capabilities**
- **III Communicate: Internal / External**

CNSSI No. 1253 *NOTIONAL SCORING

Confidentiality	Integrity	Availability
H – Severe	H – Disruptive	H – Minutes
M – Serious	M – Degraded	M – Hours
L – Limited	L – Nuisance	L – Days

- **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

CSE's 5 Impact Level exemplars aligned with NIST 800-30: Focused on CCMD Mission Risk
The weighting of C-I-A for each critical function will vary depending on the weapon system

Determining CSRC

Most JCIDS SS KPP requirements will fall within the top 3 tiers/levels

STEP ONE: Select Mission Type (MT)	STEP TWO: Select Adversary Threat Tier (ATT)	STEP THREE: Select Cyber Dependency Level (CDL)	STEP FOUR: Select Impact Level/System Compromise (IL)
MT 5: Strategic/National-Deterrence	ATT 5: Extreme	CDL 5: Extreme	IL 5: **Catastrophic** Impact
MT 4: Operational – 1st 72 hrs	ATT4: Advanced	**CDL 4: High**	IL 4: Severe Impact
MT 3: Tactical – 1st 72hrs	**ATT 3: Moderate**	CDL 3: Moderate	**IL 3: Moderate Impact**
MT 2: Mission Support – After 72hrs	ATT 2: Limited	CDL 2: Low	IL 2: Limited Impact
MT 1: Organizational Progs/Srvces	ATT 1: Nascent	CDL 1: Very Low	IL 1: Negligible Impact
		CDL 0: No Cyber Dependence	

STEP FIVE: Determine Cyber Survivability Risk Category (CSRC) of 0 to 5

CSRC can be determined using scoring methods such as High Water Mark (HWM), and SME criticality analyses for critical Move, Shoot, and Communicate functionality. Scrutinize, but don't agonize!

Example Above:
High Water Mark (HWM) scoring → CSRC-4
Subject matter experts scoring → CSRC-3 or CSRC-4

The <u>process</u> is more important than exactness: Understanding the risk, assessing the resource/system risk implications, and defining cyber threshold performance requirements for operational risk trade-space decisions … are critical.

CSRC → Requirements

Vulnerability + Threat Capability = Survivability Risk Requirements

CSRC-5: Extreme. Same as CSRC-4, except periodically request specific ATT-5 threat and mitigation recommendations.
CSRC-4: Very High. System must implement best available mitigations to prevent/mitigate effects of cyberevents to maintain a minimum functionality to complete the mission or recover/adapt to fight another day. Implement NSA's Top 10 Cybersecurity Mitigations to ensure C-I-A for trusted internal and external information flows; defense in-depth architecture, with no single points of failure; DoD-developed cyberprotections (including protections inherited from the operational environment); and as-required specific custom protections to actively manage the systems' configuration to achieve and maintain an operationally relevant CSRP. Periodically (e.g., annually/quarterly) request classified adversary cyberthreat updates for the system and its HW/FW/SW (including open-source module), in each capability release, to develop plans of action and milestones (POA&Ms) for mitigating the greatest system risks and achieving/maintaining an operationally relevant risk posture. See NSA.GOV for cybersecurity advisories with latest **ATT-4** threat and recommended mitigations.
CSRC-3: High. System must implement mitigations to prevent/mitigate effects of cyberevents to maintain a minimum functionality to complete the mission or recover/adapt to fight another day. Implement NSA's Top 10 Cybersecurity Mitigations to ensure C-I-A for trusted internal and external information flows; defense in-depth architecture, with no single points of failure; DoD-developed cyberprotections (including protections inherited from the operational environment); and as-required specific custom protections to actively manage the system's configuration to achieve and maintain an operationally relevant CSRP. Periodically (e.g., annually/quarterly) request classified adversary cyberthreat updates for the system and its HW/FW/SW(including open-source module), in each capability release, to develop POA&Ms for mitigating the greatest system risks and achieving/maintaining an operationally relevant risk posture. See NSA.GOV for cybersecurity advisories with latest **ATT-3** threat and recommended mitigations .
CSRC-2: Moderate. Mitigations include both commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) best practices, including DoD-specific threat signatures, layered defenses, TTPs, and selective DoD technologies. Implement NSA's Top 10 Cybersecurity Mitigations.
CSRC-1: Low. Mitigations include COTS with best practices (if commercially hosted) or strong DoD-layered defenses and possible use of DoD technology (if DoD hosted). As appropriate, implement NSA's Top 10 Cybersecurity Mitigations.
CSRC-0: None. No information exchange, no HW/SW/FW processing/sensors, and no wired/wireless network connections.

CSRC provides consistent level of requirements during design, testing, and operations

CSRC 5 – Exemplar Statement for ICD

THREAT

The capability's mission criticality and impact of system compromise requires the capability must survive and operate in an extreme cyber-contested environment (e.g., threatened by Russian SVR, APT-29). This level of adversaries uses a range of initial exploitation techniques that vary in sophistication, coupled with 'stealthy' intrusion tradecraft of custom tools, compromised accounts, and system misconfigurations to blend in with normal/unmonitored traffic and move undetected in victim networks for denial, degradation, deception, disruption, and destruction of mission capabilities. They have demonstrated capabilities to target cloud resources and supply chain (e.g., SolarWinds). Recognizing these cyber threats will increase, the system must implement best available defensive capabilities and mitigations to prevent/mitigate effects of cyber-related events to maintain a minimum functionality to complete the mission and recover/adapt to fight another day, including: implement NSA's Top 10 Cybersecurity Mitigations to ensure Confidentiality, Integrity, & Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; a defined hierarchy of assigned human defenders, equipped with specialized tools as needed; DoD developed cyber protections, including protections inherited from the operational environment; and as required specific custom protections; to actively manage the system's configuration to achieve and maintain an operationally-relevant cyber risk posture.

COUNTER MEASURES

CSAs

The following 10 CSAs must be assessed for each AoA/CBA alternative to understand the resource and mission risk implications, if the capability itself, hosting system or enterprise services are unable to provide each CSA's intent:"
[list all 10 CSAs by pillar]

Puts Cyber Survivability requirement in context, incorporating top-level projected cyber threat <u>before</u> AoA/CBA results can drive initial cyber threat assessment and risk determination, setting the AoA/CBA up for success (i.e. avoiding unfixable cyber vulnerabilities)

CSRC 5 – Exemplar Statement for CDD

THREAT

The capability's mission criticality and impact of system compromise requires the capability must survive and operate in an extreme cyber-contested environment (e.g., threatened by Russian SVR, APT-29). This level of adversaries uses a range of initial exploitation techniques that vary in sophistication, coupled with 'stealthy' intrusion tradecraft of custom tools, compromised accounts, and system misconfigurations to blend in with normal/unmonitored traffic and move undetected in victim networks for denial, degradation, deception, disruption, and destruction of mission capabilities. They have demonstrated capabilities to target cloud resources and supply chain (e.g., SolarWinds).

COUNTER MEASURES

Recognizing these cyber threats will increase, the system must implement best available defensive capabilities and mitigations to prevent/mitigate effects of cyber-related events to maintain a minimum functionality to complete the mission and recover/adapt to fight another day, including: implement NSA's Top 10 Cybersecurity Mitigations to ensure Confidentiality, Integrity, & Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; a defined hierarchy of assigned human defenders, equipped with specialized tools as needed; DoD developed cyber protections, including protections inherited from the operational environment; and as required specific custom protections; to actively manage the system's configuration to achieve and maintain an operationally-relevant cyber risk posture.

CSAs

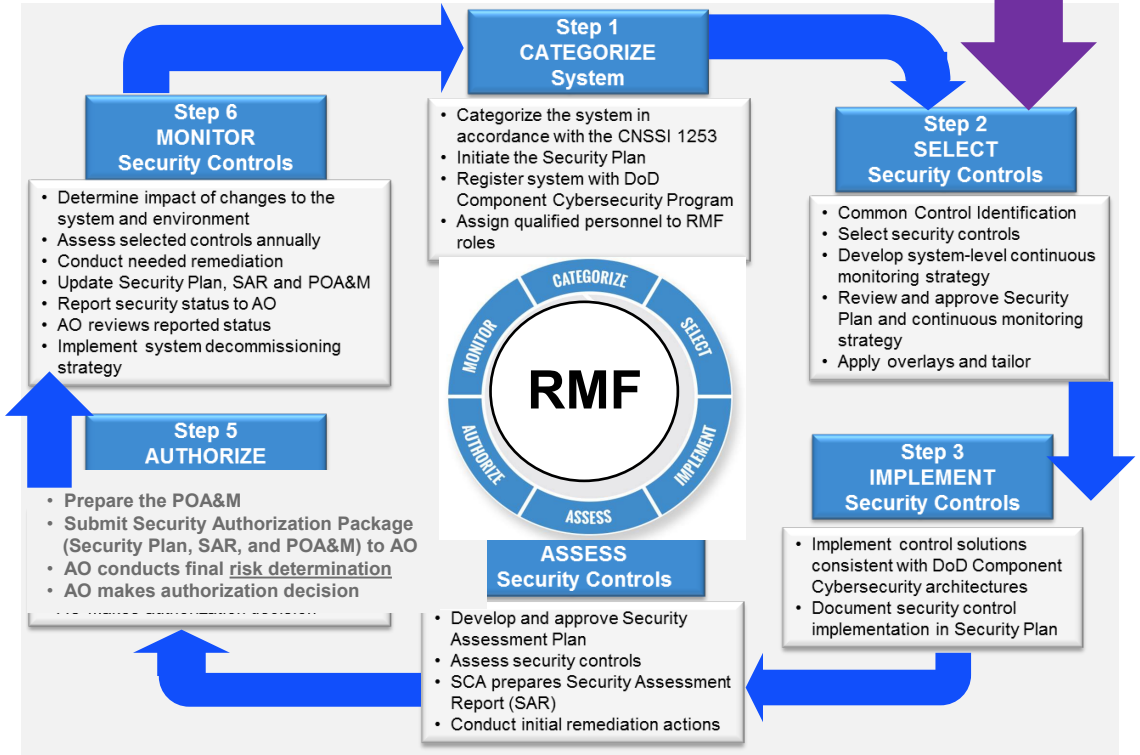
The following subset of the 10 CSAs in the table below have been determined to be most critical for (capability's name) cyber survivability, and should drive development of the RFP and source selection criteria. These CSAs have been tailored to define the capability's threshold requirements, with CSA-10 enabling adaptive, incremental improvements for countering advances in adversary capabilities, and newly identified vulnerabilities, to maintain an operationally- relevant cyber risk posture:" ***[CSA Threshold/ Objective table follows]***

Contractually-binding cyber threshold requirements will keep the government/industry team working together to win the cyber battle

Cybersecurity Compliance Necessary, but Not Sufficient

RMF: focuses on providing cybersecurity controls/standards for a generic system (not threat informed), and then documenting compliance of a system that has already been designed/built.

Cyber Survivability Endorsement: focuses on providing contractually binding cybersecurity and cyber resilience threshold performance requirements for a specific system in the expected operating environment … to justify, resource and design-in prioritized cyber controls/standards.



Transformational:

- Win-Win – RMF and CSE are complementary
- Bridges gap between requirement sponsors and the system security engineers designing in cyber
- Enables PMs and AOs to prioritize and take less risk in the cyber performance areas most critical to the system's move, shoot and communicate functions
- Places cyber in the same operational risk trade space with other system functional requirements

CSE Alignment with DoD Cybersecurity Program Requirements

- **CSE leverages the ~800 NIST SP 800-53 Rev 5 cybersecurity technical controls**
  - Originally identified 239 of ~800 NIST 800-53 rev4 controls applicable to Weapon Systems
    - ❖ 98 highly applicable, 86 somewhat applicable, and 55 require interpretation
  - CSE framework aligned with DoDI 8500.01 and DoDI 8510.01 18 RMF control families
  - CSE's 10 holistic CSA threshold performance requirements intended to flow down to system specs that are measurable and testable, supported by NIST 800-53 and CNSS 1253 controls
- **Air Force Research Lab's (AFRL) CSA Tool – automating DoD guidance**
  - AFRL, CIO, NSA and JS automated mapping of 10 CSAs to NIST 800-53 rev 5 and CNSS 1253
  - AFRL, JS and NIST aligned CSE framework with NIST 800-160 vol 2
  - AFRL Mapping MITRE ATT&CK TTPs and National Vulnerability DB
- **CSE Implementation Guide Ver. 3.0, approved for public release, Jul 2022.**
  - JS leveraged Army's use of NIST 800-30 to update CSE's Impact Level.

A similar approach is needed to meet "intent" of Zero Trust (ZT) reqts for weapon systems.

…

All ZT reqts will NOT be applicable to weapon systems. Most will need interpretation.

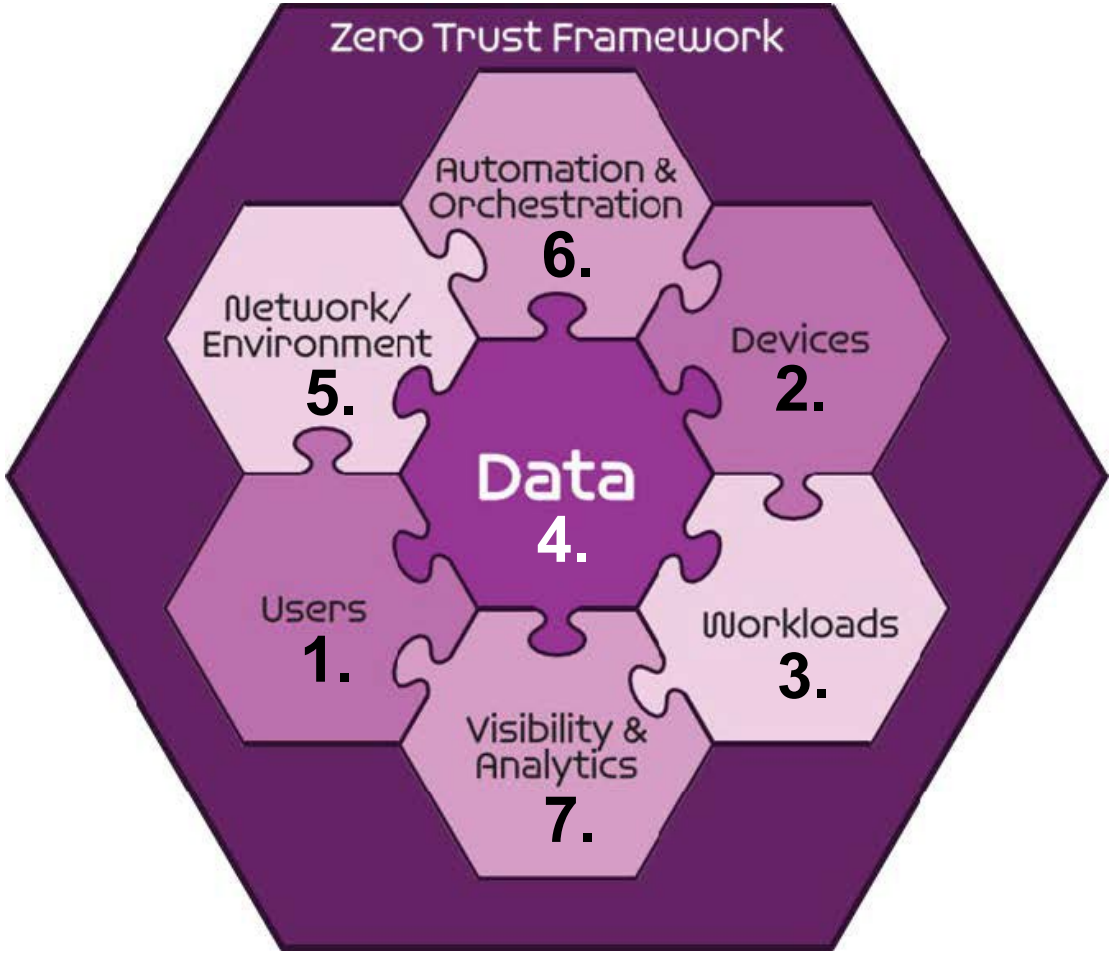
Leveraging and linking CSAs to NIST 800-53 rev 5 cybersecurity controls enables an easier understanding and implementation by system security engineers, with mission-focused performance requirements to support operational risk trade-space decisions

SS KPP Pillars and Cyber Survivability Attributes

- **Prevent** – Design requirements **identify, protect** and harden weapon system's functions from adversary **cybersecurity threats** **(to anticipate most likely and greatest risk)**
- **Mitigate** – Design requirements **detect and respond** to cyber-events making it through defenses; enabling **cyber safety and operational resilience** **(to complete the mission)**
- **Recover** – Design requirements to **recover** to a known good condition after a cyber event; at a minimum, **restore partial-to-full mission capability** **(to fight another day)**
- **Adapt** – Enables DevOps to **adapt** to changes in adversary threat and vulnerabilities **(to win this war and next war)**

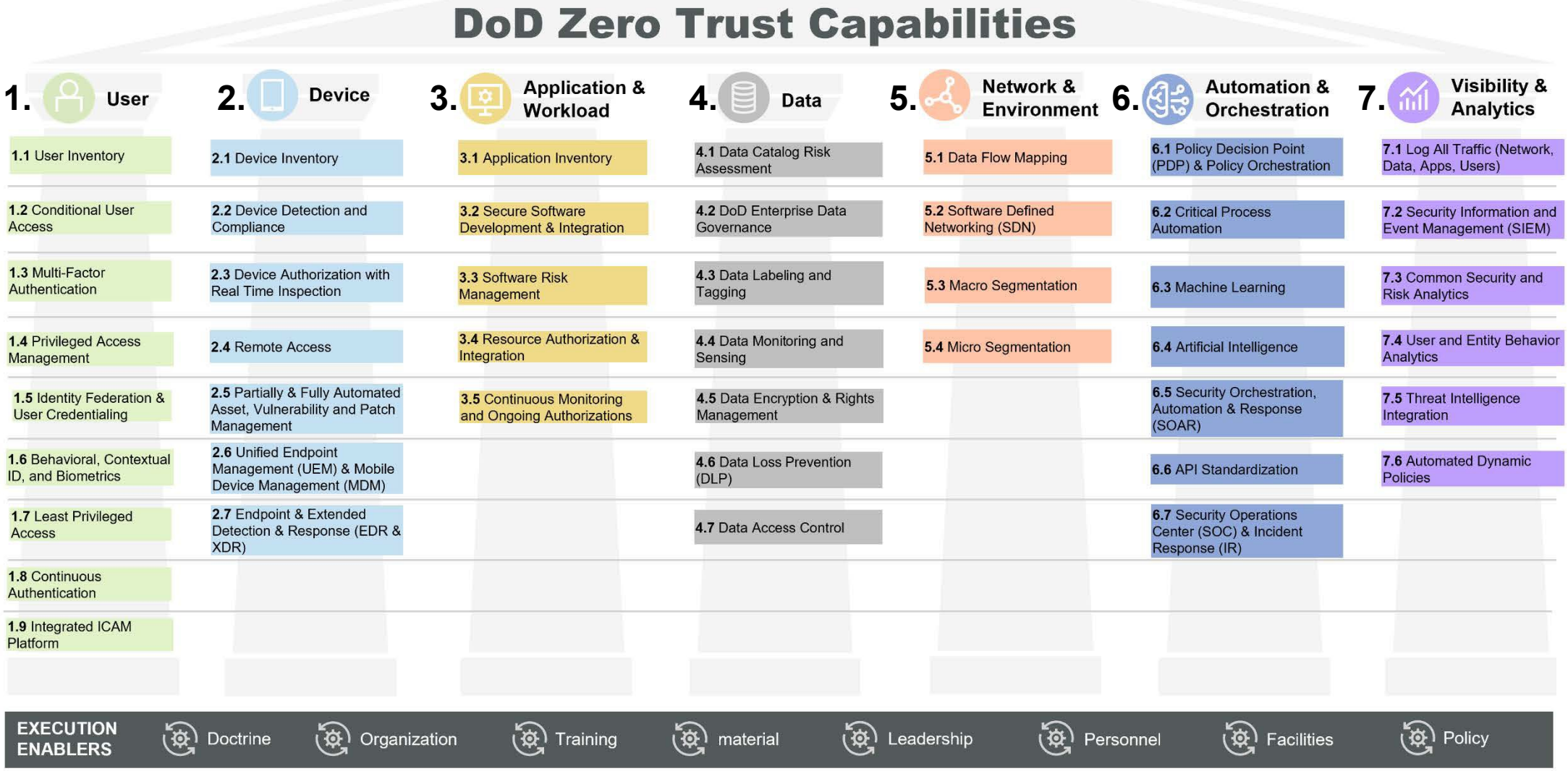
SS KPP Pillars (Mandatory)	Cyber Survivability Attributes (CSAs) (All are to be considered; select those that are applicable)
Prevent	CSA 01 - Control Access (not RMF Access Control)
	CSA 02 - Reduce Cyber Detectability
	CSA 03 - Secure Transmissions and Communications
	CSA 04 - Protect Information from 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 and Enable Cyberspace Defense
Recover	CSA 09 - Recover System Capabilities
Adapt	CSA 10 - Actively Manage System's Configurations to Achieve and Maintain an Operationally Relevant Cyber Risk Posture … also applicable to legacy systems that did not consider CSAs during development …

Zero Trust Pillars



All Resources Bound into Zero Trust Framework

DoD Zero Trust Pillar Capabilities



Mapping ZT Pillar Capabilities to CSAs

Zero Trust Capability Alignment with the Cyber Survivability (Cybersecurity and Cyber Resilience) Framework

(Draft, and not yet coordinated with CIO)

Highlighted Cells -- Indicate Direct System-level CSA Alignment with the DoD ZT Objectives from DoD ZT Strategy (Nov 22) (Requires tailoring)

	ZT 1 - USER	ZT 2 - DEVICE	ZT 3 - APPLICATION and WORKLOAD	ZT 4 - DATA	ZT 5 - NETWORK and INFRASTRUCTURE	ZT 6 - AUTOMATION and ORCHESTRATION	ZT 7 - VISIBILITY and ANALYTICS
Zero Trust Pillars (Right) ========== **Cyber Survivability Attributes** (Below)	Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.	Understanding the health and status of devices informs risk decisions. Real-time inspection, assessment and patching informs every access request	Secure everything from applications to hypervisors, to include the protection of containers and virtual machines.	Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.	Segment, isolate, and control (physically and logically) the network environments with granular policy and access controls.	Automated security response based on defined process and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.	Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.
CSA-01: Control Access (for WS, the intent of 2FA can be met with controls like guards, access logs, IDs, visual recognition)	1.3 Multi-Factor Authentication	2.3 Device Authorization with Real Time Inspection	3.4 Resource Authorization & Integration	4.7 Data Access Control			
	1.5 Identity Federation & User Credentialing (ABAC)	2.4 Remote Access					
CSA-02: Reduce System's Cyber Detectability (most costly and least likely)							
CSA-03: Secure Transmissions and Communications (Data in transit)				4.6 Data Loss Prevention			
CSA-04: Protect System Information from Exploitation (Data at rest)				4.6 Data Loss Prevention			
				4.3 Data Labelling & Tagging (Fully- automated via AI/ML)			
				4.5 Data Encryption & Rights Management			
CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels	1.9 Integrated ICAM Platform				5.3 Macro Segmentation		
					5.2 Software Defined Networking (SDN)		
					5.4 Micro Segmentation		
CSA-06: Minimize and Harden Attack Surfaces						6.6 API Standardization	
CSA-07: Baseline and Monitor Systems and Detect Anomalies	1.1 User Inventory	2.1 Device Inventory	3.1 Application Inventory	4.1 Data Catalog Risk Assessment (Classification)	5.1 Data Flow Mapping	6.2 Critical Process Automation	7.1 Log all Traffic (Network, Data, Applications, Users)
	1.6 Behavioral, Contextual ID & Biometrics (Transparent Auth)	2.2 Device Detection and Compliance	3.5 Cont Monitoring and Ongoing Authorizations	4.4 Data Monitoring and Sensing			7.4 User and Entity Behavior Analytics
	1.8 Continuous Authentication	2.7 Endpoint & Extended Detection & Response (EDR & XDR)					
CSA-08: Manage System Performance and Enable Cyberspace Defense (to complete mission)	1.4 Privilege Access Mgmt.	2.7 Endpoint & Extended Detection & Response (EDR & XDR)				6.5 Security Orchestration, Auto & Response (SOAR)	7.2 Security Information and Event Management (SIEM)
						6.7 Security Ops Center (SOC) Incident Response (IR)	7.5 Threat Intelligence Advanced Threat Protection
CSA-09: Recover System Capabilities (Continuity of ops, to fight another day)							
CSA-10: Actively Manage System's Configuration to Sustain Operationally Relevant Cyber Risk Posture (Could support continuous ATO/DevOps)	1.2 Conditional User Access	2.5 Partially & Fully Automated Asset, Vulnerability & Patch Mgmt	3.2 Secure Software Development & Integration (Dev~~Sec~~Ops)	4.2 DoD Enterprise Data Governance		6.1 Policy Decision Point (PDP) & Policy Orchestestration	7.3 Common Security and Risk Analytics
	1.7 Least Privileged Access	2.6 Unified Endpoint Mgmt (UEM) Mobile Device Mgmt (MDM)	3.3 Software Risk Management			6.3 Machine Learning	7.6 Automated Dynamic Policies
						6.4 Artificial Intelligence	

ZT – most equities
ZT – some equities

CSA Exemplars to be Tailored in a CDD (1 of 2)

Primarily … Cyber Security Attributes

Prevent - CSAs	Exemplar Language – Threshold, Contractually-Binding Requirements
ZT **CSA-01: Control Access**	(U) "System shall only allow identified, authenticated, and authorized persons and non-person entities (including all assigned cyber defenders and their tools) access or interconnection to system or sub-system elements. The capability shall enforce a validation mechanism to protect the C, I, A of system resources (e.g., memory, files, interfaces, logical networks). The system shall employ anti-tamper measures that include features for protection of critical system components, information technologies, and maintenance of technology/program protection. Physical access to the system shall also be controlled." **Incl. Cyber Resilience Attributes, cred mgmt**
CSA-02: Reduce System's Cyber Detectability	(U) "System survivability requires signaling and communications (both wired and wireless) implemented by the system (or state "supported by system/capability") shall minimize the ability of an adversary to monitor and/or target system and/or supported DoD weapon systems through its emanations, which may include deception." **Incl. Cyber Resilience Attributes**
ZT **CSA-03: Secure Transmissions and Communications**	(U) "System shall ensure all transmissions and communications of data 'in transit' are protected commensurate with its confidentiality and integrity requirements. System shall only use NSA-certified cryptographic capabilities." [NOTE: if a National Security System, add: "System shall develop, coordinate and maintain a System TRANSEC Plan (STP) throughout the system's lifecycle."]
ZT **CSA-04: Protect System Information from Exploitation**	(U) "System shall ensure all data at rest is protected commensurate with its confidentiality and integrity requirements. System shall prevent unauthorized access, use, modification, and transfer/removal of data, including attempted exfiltration, from the system to unauthorized person and non-person entities throughout the system's lifecycle (including development)."
ZT **CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels**	(U) "System partitioning shall implement technical/logical mitigations including logical and physical segmentation. The system shall be able to maintain mission critical functions at minimum performance thresholds identified within the system's CONOPS. Compromise of non-critical functions shall not significantly impact system mission capability." **Incl. Cyber Resilience Attributes, micro-segmentation, zero trust**
ZT **CSA-06: Minimize and Harden Attack Surfaces**	(U) "System shall automatically disable all unauthorized ports, protocols, and services (PPS), including access points, by default. Any deviations from PPS baselines shall be approved and documented by a configuration management board. System shall support automated monitoring and logging of system attack surface and associated cyber events. Any removable media use must be approved, documented and strictly monitored." [UPDATE FOR NEXT CSEIG: CSRC 3, 4 and 5 systems should consider including "Component operating systems must be currently supported, have a reasonable expectation of future supportability, and have an appropriate trust level. New development must include programming languages that reduce cyber survivability risks, can easily integrate with other languages, and has sufficiently low memory/processor requirements to run on embedded devices (e.g., RUST)."]

Tailored subset of CSAs drive RFP source selection criteria, RMF controls, and DT/OT assessments

ZT – most equities
ZT – some equities

CSA Exemplars to be Tailored in a CDD (2 of 2)

Primarily … Cyber Resilience Attributes

Mitigate - CSAs	Exemplar Language – Threshold, Contractually-Binding Requirements
CSA-07: Baseline and Monitor Systems, and Detect Anomalies ZT	(U) "System shall implement and maintain a cyber survivability configuration baseline for its GOTS/COTS HW, SW, FW and open source modules, by version # to ensure an operationally acceptable cyber risk posture 24/7. System shall monitor, detect and report system health status and anomalies indicative of cyber events, based on its current adversary threat intelligence, CONOPS and MRT-C. Applicable report detail shall be provided to users, system operators and assigned cyber defenders (e.g., config changes, cyber-event indicators, slowed processing, or loss of functionality within T = (# of seconds/minutes) [specified by sponsor])." (drives CDRLs)
CSA-08: Manage System Performance and Enable Cyberspace Defense ZT	(U) "If anomalies are detected and/or cyber-events degrade system capability, the system shall be sufficiently resilient to mitigate cyber-related event effects through orderly, structured and prioritized system responses, in order to ensure minimum mission functionality requirements [system functionality threshold specified by sponsor] to complete the current mission or return for recovery. The system shall enable assigned cyber defenders to impose effects on adversaries to counter their operations and objectives. Alternatively, the mission commander shall be able to selectively disconnect/disable subsystems that are not critical as well as isolate the system from integrated platform systems and/or Department of Defense Information Network (DoDIN)."
Recover - CSA	**Exemplar Language – Threshold, Contractually-Binding Requirements**
CSA-09: Recover System Capabilities	(U) "After a cyber-event, the system shall be capable of being restored to a known good configuration from a trusted source; at a minimum, restored to partial mission capability, between mission cycles or within xx hours [specified by sponsor, to fight another day. System recovery shall prioritize cyber operational resiliency functions."
Adapt – CSA	**Exemplar Language – Threshold, Contractually-Binding Requirements**
★ CSA-10: Actively Manage System's Configurations to Achieve and Sustain an Operationally-Relevant Cyber Risk Posture ZT	(U) "Throughout a system's lifecycle and within one standard mission cycle of xx hours [specified by sponsor] of identification of a drop in cyber risk posture below its commensurate CSRC level, the system shall have a configuration management process, supported by automated capabilities and technology refresh options, to achieve and continuously maintain an objectively assessed and operationally-relevant risk posture. The process shall include inputs from operators, defenders and intel analysts to continuously assess changes in adversary threat, and include a machine readable Bill of Materials of the system's GOTS/COTS HW, SW (including open source), and FW for a supply chain risk assessment prior to each milestone decision and supported release. The process shall determine the sufficiency of the system's cyber survivability and support a DevOps framework to prioritize vulnerability mitigation and remediation in the system and connected infrastructure with greatest mission risks." (drives CDRLs)

If capability relies on another system/service to meet CSA requirement, state which and how

How does CSE Support ZT in DevOps? Answer: CSA-10!

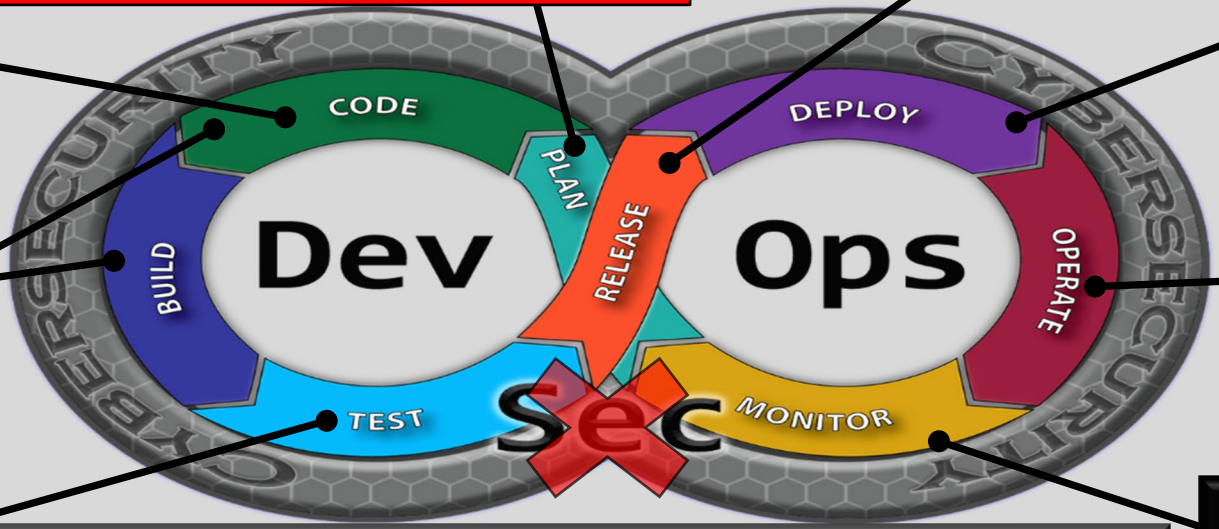
Secure Coding Standards/CWEs
- Secure Design Principles
- Design/Code Inspection
- Automated Code Scanning
- Manual Code Review
- Secure Container Framework

Security and Resilience Requirements *
- Understand Threats/Risks
- Criticality Analysis
- Security /Resilience Architecture

Artifact Scanning
- STIG Conformance
- Assurance Case Update

Secure Deployment
- Cryptographic Integrity Check
- Configuration Checker
- Host Based Vulnerability Scans
- Network Based Vulnerability Scan

Static Code Analysis
- Origin Analysis/CVEs
- Binary Code Analysis
- Architecture Conformance Checks



Secure Operation
- Two man rules
- Respond to Incidents/Defects
- Threat Awareness
- Contingency Plans
- Cyber Offensive Capability

Dynamic Analysis
- Test Coverage Metrics
- Fuzz Testing
- Penetration Testing

Secure Development & Operational Environments
- Controlled/Monitored Access
- Encryption at rest & in-flight
- Monitor/Maintain Integrity of all Tools, Libraries, Scripts

Monitor Threats/Attacks
- Operational Metrics
- Logging & Auditing
- Threat Detection & Intelligence

CSA 10 – Actively Manage System's Configuration to Achieve and Sustain an Operationally Relevant Cyber Risk Posture – "*Minimum Viable Capability*"

Defining ZT Threshold Performance Requirements … puts ZT in DevOps Risk Trade Space

Voluntary CSE Adoption Progress

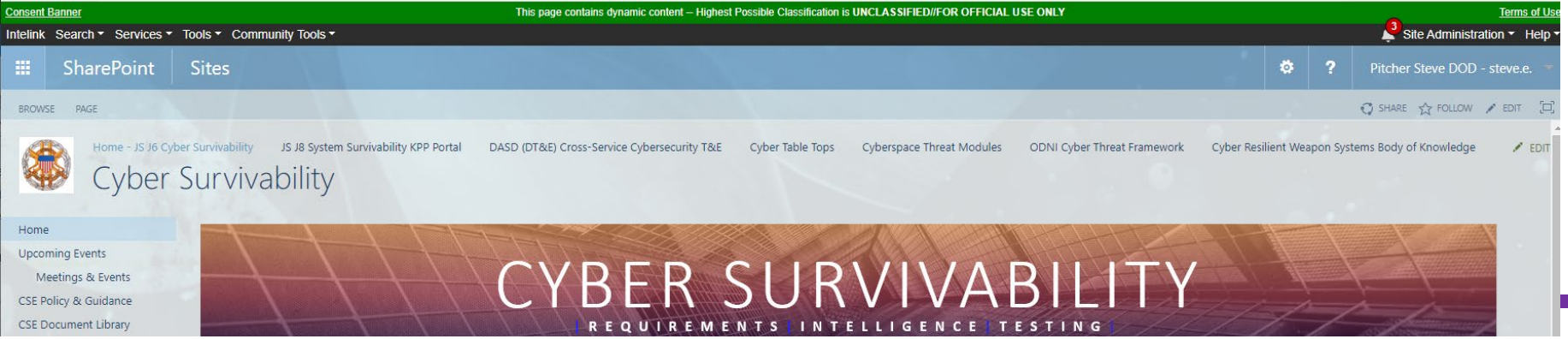
CSE Aligned Guidance: (**Purple:** OSD/JS/Allies, **Blue:** Air Force, **Green:** Army, **Black:** Navy/Marine Corps)

- **Dec 2015:** JCIDS Manual... added CSE to SS KPP
- **Jan 2017:** CSEIG v1.0 … published
- **Feb 2018:** DAU RQM-310 ... J6 began briefing CSE
- **Apr 2018:** DoD Cybersecurity T&E Guidebook
- **May 2018:** AF System Security Engineering (SSE) Cyber Guide
- **Jul 2018:** OUSD(R&E) Cyber Table Top Guidebook
- **Oct 2018:** JCIDS updated ICD reviews, CSRC and CSA
- **Oct 2019:** DISA/JITC Test Criteria… using SSKPP CSRP
- **Nov 2019:** AFI 99-103 Capabilities-Based Test & Eval
- **2019 – 2021:** ~40 DoDIs with cyber equities not fully coordinated below GO/FO… many include reference to CSE
- **Feb 2020:** DoD Cybersecurity T&E Guidebook v2
- **Mar 2020:** CSEIG v2.0… focusing on CSA-10 [DevOps]
- **2020:** AFRL CSA Tool… support throughout lifecycle
- **2020:** NAVAIR PPP and SSE Work Breakdown Structure
- **2020:** Army Cyber Acq Discipline Policy applies to 'All Army Acquisition Programs that Research/Develop/Acquire IT'
- **2020:** Army Memo for Cyber resiliency in all WS
- **2021:** MITRE and AFRL aligned CSA Tool to NIST 800-53 rev 5 controls, prior to being implemented in DoD
- **2021:** NIST SP 800-160 v2 r1 [draft] cites CSE for cyber resilience
- **2021:** DoD Cyber Table Top Guide v2
- **2021:** AFSOC C-146A CSRA success story (SIPR email)
- **2021:** SERC DTE&A and Cyberattack Resilient Systems
- **2022:** CSEIG v3 … Declassified ATTs and publicly releasable
- **2022**: Navy Integrated PP, Cybersecurity & Engineering (IPPCE)
- **2022:** AF Measures of Performance Report (MOPR), includes CSF-like tiers linked to CSE's CSAs
- **2022:** Army Cyber Acquisition Discipline (ACAD) updated
- **2022:** MDA CSE Implementation Instruction
- **2023:** AF SSE Cyber Guide v.5 published (also adopted by NAVAIR)

In process

- **FY23:** OSD R&E Measuring Resilience Pilot
- **CY23:** CCEB Adoption of CSE to Influence National Development

CSE is only mandatory for requirements going through JCIDS, but Services seeing Resource/Mission Risk Benefits for considering Cyber Survivability for All Acquisition Pathways



How to Apply Cyber Survivability

- **Use latest JCIDS Manual (Oct 21) and CSE Implementation Guide (CSEIG) v 3.0 (Jul 22)**
  - **NIPR CSE:** https://intelshare.intelink.gov/sites/cybersurvivability/
  - **SIPR CSE:** https://intelshare.intelink.sgov.gov/sites/cybersurvivability/
  - **SIPR Joint Staff KM/DS:** "JROC Admin Tools" tab - https://jrockmdsbpm.osd.smil.mil/bizflow/bizindex.jsp

  Above links include System Security Engineering references to instructions and exemplar statements for drafting contract clauses, system specifications, and developmental test thresholds.

- **CSEIG provides detailed guidance for an ICD/CDD, IS-ICD/IS-CDD and CDD updates**
  - Includes exemplar text for Cyber Survivability Risk Categories (CSRCs), Cyber Survivability Attributes (CSAs).
  - Includes recommendations on how the CSRC and CSAs can support AoA Requests for Information.
  - Includes exemplar text for Program Protection Plans, Cybersecurity Strategies, and Requests for Proposals.

CSE is a bridge between non-cyber professionals and the System Security Engineers who have to sufficiently decompose CSA performance requirements into system specifications

Way Ahead -- CSE Alignment with other DoD Processes

- **CSA Updates –** Coordinate within DoD and with FVEY/CCEB on CSEIG threshold performance requirement exemplars for ZT, AI/ML, and trusted/supported OS, programming languages and open source SW.
- **Cyber Adversary Threat –** Coordinate a CSEIG annual cyber ATT update process, that includes risk to the HW, FW and SW (incl. open source) integrated in DoD systems and meets CIP intent.
- **Cyber Survivability Metrics** – Coordinate on cyber survivability metrics for status reports at each acquisition milestone, knowledge point, approval to operate, operations and version release risk decision.
- **DB framework –** Coordinate on efforts to rationalize a DB framework that leverages CSE's holistic attribute requirements for the HW, FW and SW (incl. open source) integrated in DoD systems.
- **Orchestrate a CCMD focused/scalable DoD assessment process –** Coordinate on efforts that leverage CSE to determine legacy system, system-of-systems and CCMD OPLAN/Mission cyber risk postures, and minimize gaps/overlaps between assessments to prioritize/mitigate vulnerabilities with greatest CCMD risks.
- **CSE Alignment with DoD/JS Cyber Guidance for All Acquisition Pathways and Throughout Lifecycle –**
  - Coordinate on updating the 40+ DoDDs/DODIs with cyber equities, to orchestrate DoD best practices that leverage CSE's holistic cyber threshold performance requirements for all acquisition pathways.
  - Recommend starting with high order DoDDs/DoDIs, and flow down to supporting guidance.

Realize the benefits of extending the CSE Framework to all acquisition pathways and Legacy Systems with "critical risk to mission" will help sponsors identify and justify resourcing to prevent, mitigate, recover from, and adapt to cyber events

J6 Cybersurvivability Team (Pentagon Room 1E1045)

Mr. Steve E. Pitcher, GS-15, CISSP, CEH
JS Senior Cyber Survivability Analyst
703-614-7813
NIPR: Steve.E.Pitcher.civ@mail.mil
SIPR: Steve.E.Pitcher.civ@mail.smil.mil
JWICS: Steve.E.Pitcher@coe.ic.gov

Tom Andress, CISM, Security+
Cyber Survivability Analyst
703-692-0905
thomas.r.andress.ctr@mail.mil
thomas.r.andress.ctr@mail.smil.mil
thomas.r.andress@coe.ic.gov

James Brown, CISSP
Cyber Survivability Analyst
703-697-8276
james.l.brown2.ctr@mail.mil
james.l.brown2.ctr@mail.smil.mil
james.l.brown3@coe.ic.gov

Steve Brady, CISSP
Cyber Survivability Analyst
703-614-7393
steven.j.brady10.ctr@mail.mil
steven.j.brady10.ctr@mail.smil.mil
steven.j.brady@coe.ic.gov