Cyber Survivability for Future and Legacy DoD Weapon Systems

using the JCIDS System Survivability KPP and the Cyber Survivability Endorsement (CSE) framework to provide a shared understanding of the "cybersecurity" and "cyber operational resilience" levels required throughout a system's lifecycle, regardless of the acquisition pathway, for prioritizing mitigations with the greatest Combatant Commander OPLAN and Mission Risk

Mr. Steve Pitcher, GS-15, CISSP, CEH
Mr. Tom Andress, CISM, DAWIA PM
Joint Staff J-6 Cyber Survivability
Updated: 10 June 2021

Why Cyber Survivability "Endorsement"?

- **DepSecDef (DSD) directed Joint Staff to develop a Cybersecurity KPP in 2015**
  - DSD had been briefed by the Director of Operational Test & Evaluation (OT&E) on their annual report, that highlighted multiple weapon systems with:
    - ❑ Known high risk vulnerabilities that should have been fixed prior to OT&E
    - ❑ Same "dirty dozen" vulnerabilities found every year in almost every system
    - ❑ Fixes that would now be hard and costly, since not identified and mitigated early
- **Probable Cause:** Legacy systems' only CDD (and RFP) threshold requirement for cyber (*cybersecurity and cyber resilience*) was to obtain an Authorization To Operate (ATO) (or its predecessor, a Platform IT Risk Acceptance (PRA) from the designated risk acceptance official
- **Question:** Is a system with an ATO of 90% RMF compliance more operationally cyber-survivable than one with 70% compliance?
- **Answer:** It depends – on which aspects of that RMF compliance best mitigates the vulnerabilities with the greatest system risk, Service mission risk, and/or Combatant Commander (CCMD) OPLAN/mission risk, enabling the system to prevent, mitigate, recover and adapt to cyber events.

Instead of a Cybersecurity KPP, a Cyber Survivability Endorsement (CSE) was added to the Joint Staff's System Survivability Key Performance Parameter (SS KPP), which kept it within a PM's operational risk trade-space for functionality (cost, schedule and performance)

Why Transition to Cyber "Survivability"?

Congress has passed several NDAAs focused on improving the cyber~~security~~ **survivability** (including "cybersecurity" and "cyber operational resilience" requirements) of weapon systems (WS) and the critical infrastructure (CI) supporting them. The Department is pursuing the initiation of the Strategic Cybersecurity Program (SCP), and continuing to assess and mitigate cyber vulnerabilities of existing weapons systems, however …

- DoD guidance is:
  - Fragmented, with ~ 20 DoDIs updated in 2020 getting no meaningful coordination
  - Not building on 2018 JCIDS guidance, or orchestrating other DoD best practices
  - Not keeping pace with Services' efforts to apply cyber survivability to all acquisitions
  - Uses definitions of cybersecurity and resilience that are obsolete or counter-productive
- Legacy systems' only cyber threshold requirement was/is to get an ATO under RMF
  - No threshold requirements for cybersecurity or cyber operational resilience in CDD or RFP
  - No resourced requirement to actively manage system configuration to achieve and maintain operationally relevant Cyber Survivability Risk Posture (CSRP) by adapting to adversary changes
  - DoD mission assurance requires **both** cybersecurity and cyber operational resilience
- Cyber threat intel is disjointed and insufficient to justify PM plans to mitigate cyber mission risks
  - No overlay of classified intel including zero-days, supply chain risk, and adversary threat advances on top of publicly available info for the HW/SW/FW integrated into DoD WS and CI

Recommend a CFT from OUSD(A&S), OUSD(R&E), OUSD(I), NSA, CAPE and DoD CIO to align OSD and JS guidance on requirements, acquisition, resourcing, testing and sustainment for orchestrating cyber survivability of existing/future weapon systems and supporting critical infrastructure to support (cyber survivable) mission assurance

BLUF: Notional SCP Purpose for Orchestrating DoD Efforts

- DoD governance needs to orchestrate a two-pronged approach for achieving a cyber risk posture greater than the sum of individual organization efforts
  - **Rapid response:** Promulgate and review emergent intelligence identifying potentially unacceptable mission risks, driving assessment and mitigation of cyber risks to missions across the DoD
  - **Steady state:** CCMDs, Services and Agencies (CC/S/A) coordinating to actively manage systems' configurations to mitigate cyber vulnerabilities with the greatest CCMD mission risks (with JS/OSD assistance with gaps and redundancies)

Cyber survivability includes attributes for cyber security, safety, and operational resilience

BLUF: Notional SCP Purpose for Orchestrating DoD Efforts

- This will require adjustments to the authorities of DoD working groups and boards, with greater synchronization of existing roles/responsibilities for CC/S/As, JS and OSD:
  - **Intelligence Community deliverables:** Overlay classified adversary cyber threat intel on publicly available information on the cyber vulnerabilities of, and adversary threat against, the GOTS/COTS HW/SW/FW integrated in DoD systems; a key component of the OUSD (A&S) Cyber Risk Mitigation Tool (CRMT), enabling PMs to develop timely POA&Ms to mitigate acquisition and operations risks
  - **Service/Agency deliverables:** Capability owners perform cyber survivability risk posture (CSRP) assessments to manage HW/SW/FW configuration baselines, develop POA&Ms to mitigate vulnerabilities, and report results to CCMDs, OSD and JS, enabling prioritizing mitigations with greatest mission risks
  - **CCMD deliverables:** Assess Service/Agency CSRP reports on WS and CI for the success of their OPLANs/missions, by integrating vulnerability and threat intel from the CRMT database into Exercises, Wargames, Deep Cyber Resiliency Assessments or Table Top Exercises. CCMDs must prioritize cyber vulnerabilities and report if Service/Agency mitigation POA&Ms pose an unacceptable mission risk, enabling integration within existing Integrated Priority List/Issue processes
  - **OSD/JS deliverables:** Arbitrate and prioritize programmatic disconnects between Service/ Agency mitigation POA&Ms and CCMD OPLAN/mission requirements

Cyber survivability includes attributes for cyber security, safety, and operational resilience

CSE Threshold Requirements Throughout the Lifecycle

CSE's measurable and testable requirements provide a foundation for scalable DoD-wide guidance, and consistent understanding of the level of cyber survivability (cybersecurity and cyber operational resilience) **required throughout a weapon system's lifecycle**

- **Analysis of Alternatives:** Use ICD's Cyber Survivability Risk Category (CSRC) and Cyber Survivability Attributes (CSAs) to understand the resource/mission risk implications of each capability alternative, preventing pursuit of flawed capabilities
- **Request For Proposal:** Use CDD's CSRC and those CSAs most critical to system survivability as Source Selection Criteria, preventing development of capabilities so flawed it would be inconceivable to cost-effectively mitigate cyber risks to an operationally acceptable level
- **System Engineering & Testing:** Decompose CDD's CSAs into specific cyber survivability requirements, engineering and validating the effective implementation of cyber mitigations
- **Resource Sponsor and Program Manager Operational Risk Trade-Space Decisions:** Balancing functional and cyber threshold requirements, and building to attain threshold performance capabilities, including the capability's cyber survivability, and iteratively update to maintain an operationally relevant Cyber Survivability Risk Posture (CSRP) despite adversary advances
- **Acquisition and Authorizing Official Risk Decisions:** Validate that CSRC and CSA threshold requirements are identified/updated at each decision point; validate POA&M implementation effectiveness; and inform risk acceptance decisions
- **Combatant Commander Risk Acceptance:** Understand OPLAN/mission risk implications by reviewing the CSRP of the systems, system-of-systems, and associated critical infrastructure to drive mitigation priorities, and finite resources to do so
- **SCP Mitigation Priorities:** Based on CSRP, mitigation POA&Ms, and CCMD priority disconnects.

Provide contractually-binding cyber threshold requirements tailored to all acquisition pathways, so authorities can consider effectiveness at each decision point

How Can CSE Reduce Cost and Improve Mission Assurance?

Examples of cost-drivers:

- Buying "bleeding edge" technology: personal computer and new car phone integration
  - ~30% greater cost than previous generations, with latest and greatest functions
  - Rushing to market, before bugs understood sufficiently for reasoned risk decision
- Acquiring Collision Detection/Reporting (threshold req.) vs Avoidance (objective req.)
  - Same sensors/hardware -- only paying for threshold SW/FW requirements
  - Enables path to field future SW/FW at reduced cost and risk … similar to Tesla rollout

Pursuing Threshold SW capabilities, with sufficient HW for future SW

- Initial limit in program scope fields threshold capabilities sooner, enables resourcing for:
  - Sustained adapting to "actively manage the system configuration to maintain an operationally relevant CSRP" throughout lifecycle
  - Technology refreshes to support intent of objective capabilities, when mature, reliable and cost effective
  - Avoids paying up-front for capability that may never materialize!

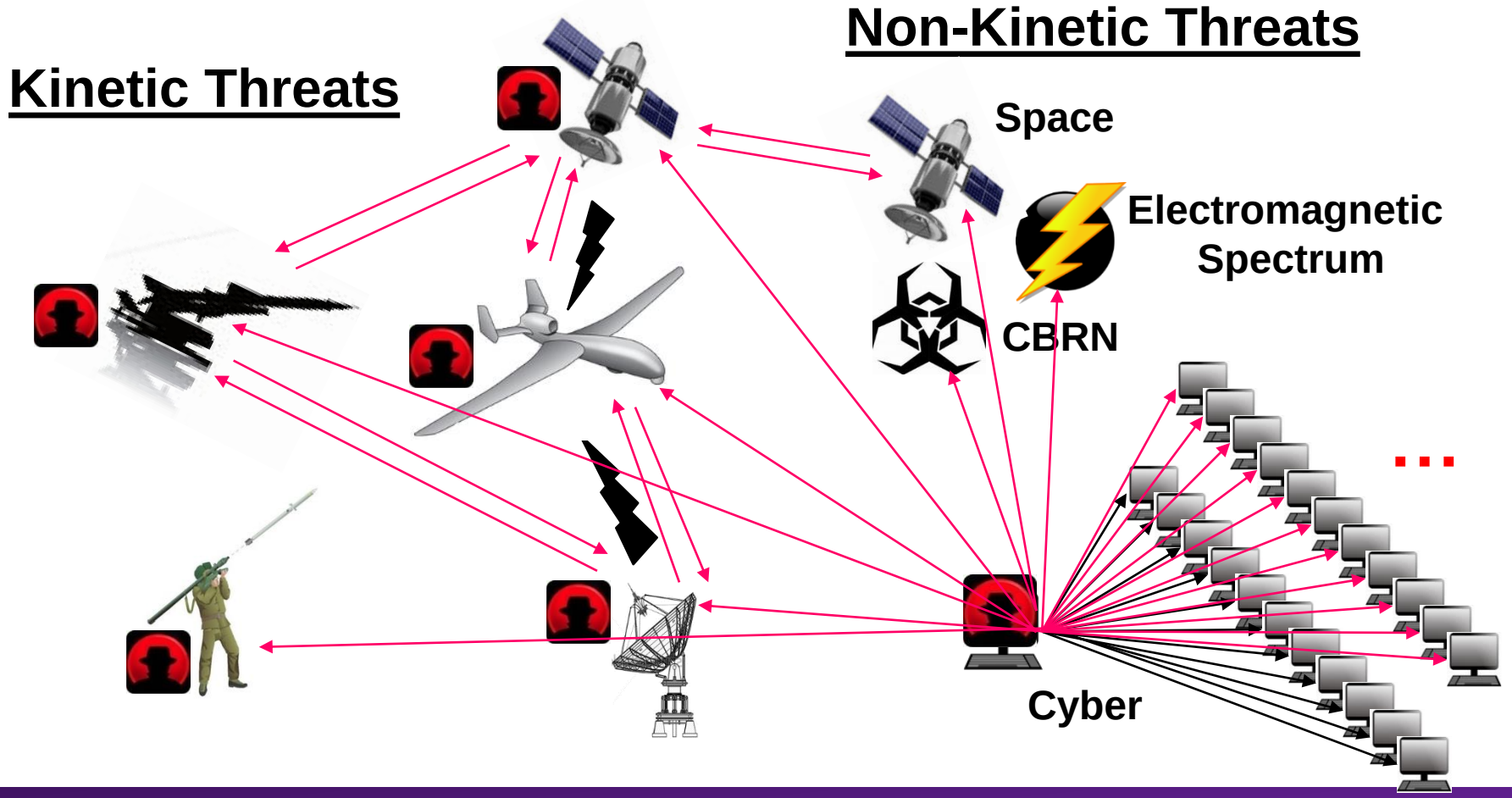
Aligns with Services' best practices and rapid acquisition/RMF efforts

- Drives consideration of cyber "performance" most critical to system survivability and mission accomplishment in the expected cyber threat environment
- Enables early understanding of the potential resource and mission risk implications of a capability's ability or inability to meet the intent of the CSAs

Less operator cost, risk, and frustration, with greater mission assurance!

Why add the Cyber Survivability Endorsement to SS KPP?

Today's stressing interconnected, cyber-contested environment

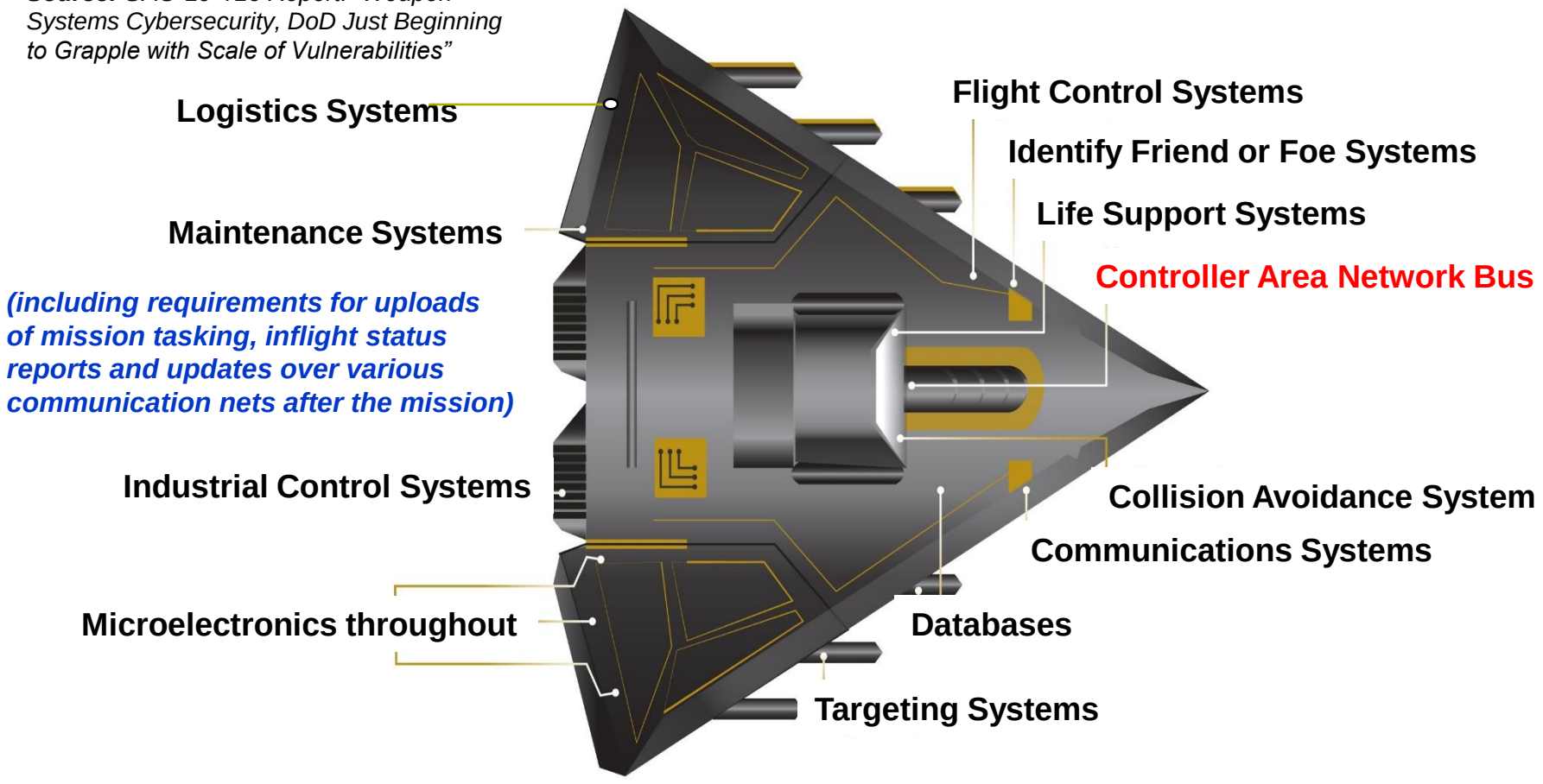


One cyber "bullet" can achieve multiple mission kills against ALL similarly connected/configured systems, so buying more systems won't provide increased mission assurance; cyber bullets are being fired, and hitting targets, TODAY

Degree of Integration and Connectivity: Good News & Bad News

(Pervasiveness represented via a fictitious weapon system for classification reasons)

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



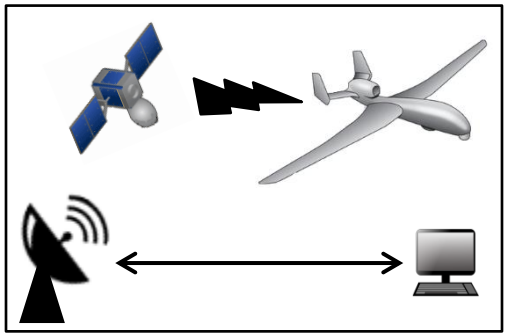
Source: GAO analysis of Department of Defense information. | GAO-19-128

Functionality designed for good can be used for evil --
critical mission functionality (move, shoot, communicate)
must be segregated from all others to complete mission, or return to base

CSE's Cyber Dependence Level (CDL)

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

Determine the mission-critical functions of the system



Move: Sustain Flight and/or Maneuverability

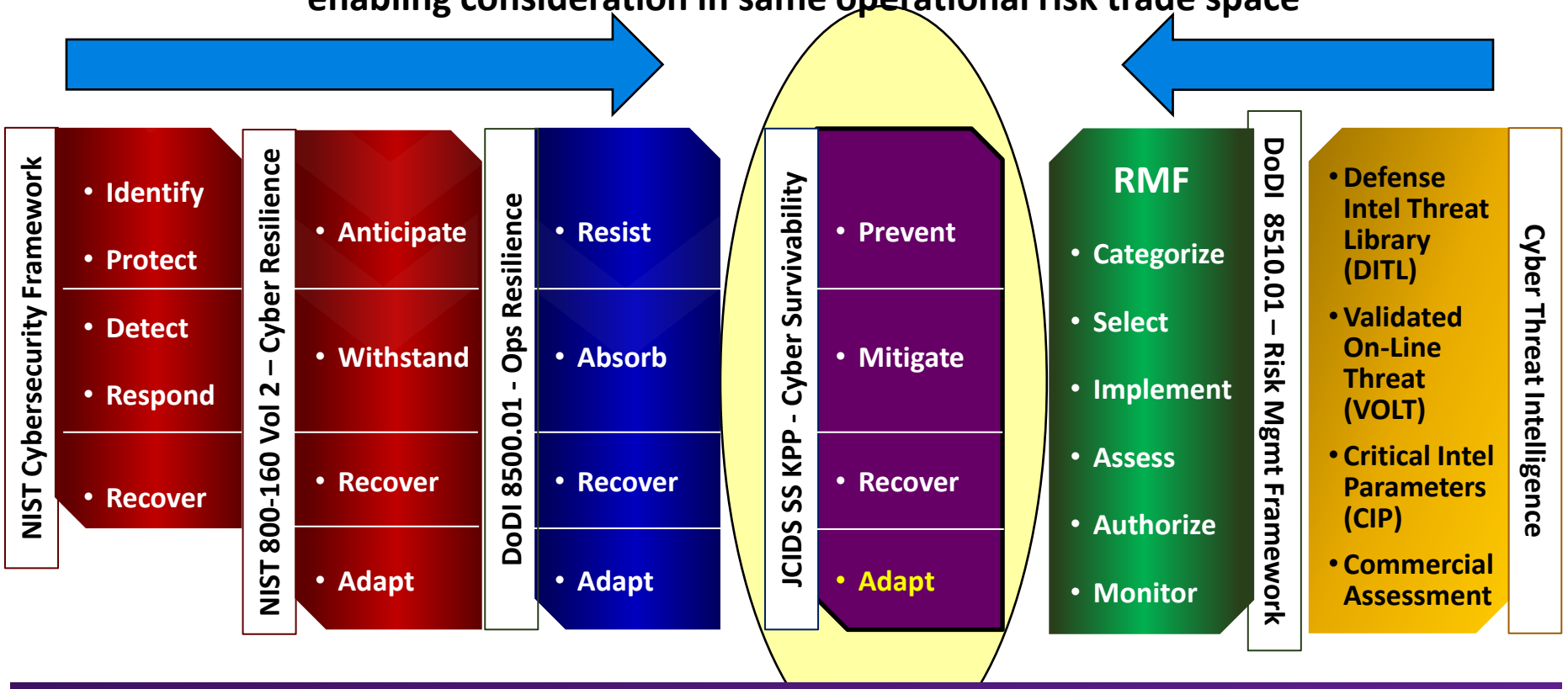
Shoot: Perform Mission (offensive and defensive actions)

Communicate: Maintain Internal and External Communications

"Cyber Dependence" is based upon the intrinsic cyber survivability risks associated with performing mission-critical functions (Move, Shoot and Communicate)

Cyber Survivability Framework Integration

SS KPP terminology connects cyber to kinetic functionality – enabling consideration in same operational risk trade space



Risk-focused, measurable, testable, implementable Cybersecurity and Cyber Operational Resilience requirements can drive AoA guidance, RFP source selection criteria, and selection of RMF technical controls

***** Need DoDIs updated to direct contractually-binding threshold requirements *****

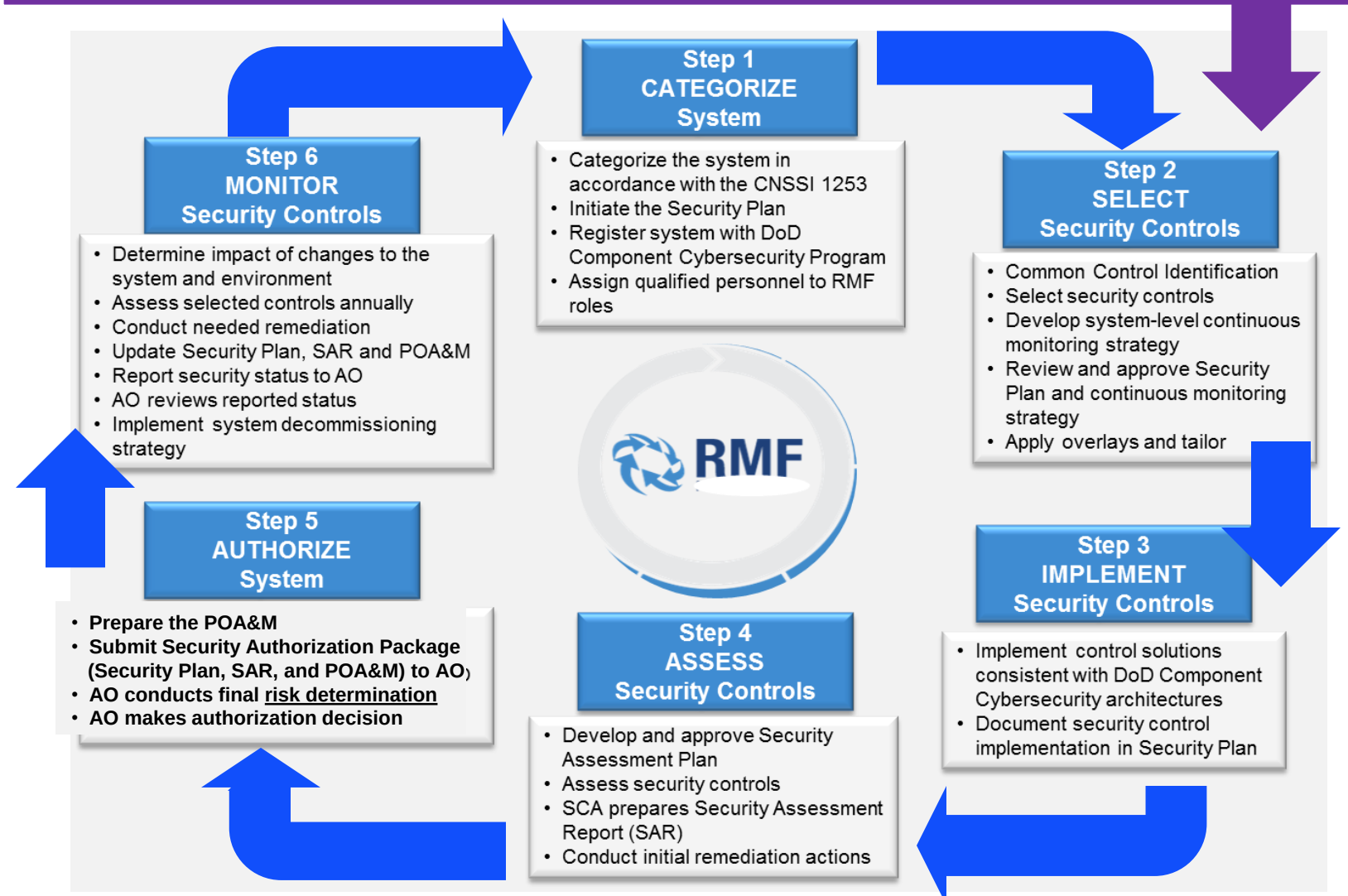
JCIDS SS KPP and CSE Align with NIST SP 800-160 Vol 2 and DoDI 8500.01

- **NIST SP 800-160 vol. 2:** **Cyber resilience** is "the ability to anticipate, withstand, recover from, and **adapt** to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."
- **DoDI 8500.01:** **Operational resilience** is "the ability of systems to resist, absorb, and recover from or **adapt** to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions."
- **CSEIG v3 definition (draft):** **Cyber Survivability** is "the ability of warfighter systems to prevent, mitigate, recover from and adapt to adverse cyber-events that could impact mission related functions, by applying a risk-managed approach to achieve and maintain an operationally-relevant risk posture, throughout its lifecycle."
- **System Survivability KPP Pillars for Cyber Survivability** (principles and attributes)**:**
  - **Prevent CSA-01 to CSA-06:** ability to anticipate/resist cyber-event
  - **Mitigate CSA-07 and CSA-08:** ability to withstand/absorb cyber-event, by adapting responses during adverse conditions, stresses, attacks or compromises *to complete the current mission*
  - **Recover CSA-09:** ability to recover after a cyber-event *to fight another day*
  - **Adapt CSA-10:** enables adapt capability to achieve and maintain an operationally-relevant CSRP, countering risk changes due to adversary's capabilities

All "mission-critical" systems should have sufficient resourcing of CSA-10 to ensure capabilities can adapt to emergent risks to sustain operationally-relevant mission assurance throughout its lifecycle

RMF, DAS and JCIDS Cyber Survivability Attributes

CSAs provide outcome-defined cyber threshold requirements that should drive development of source selection criteria, support system engineering decomposition of requirements, and a resource sponsor/PM's operational risk trade-space decisions for resourcing Security Controls



Cyber Survivability Attributes Support RMF

- **CSE leverages the ~800 NIST SP 800-53 cybersecurity technical controls**
  - CSE is the onramp to, and supports, the Risk Management Framework (RMF)
  - The CSAs have been traced directly to the 17 RMF control families
  - The CSAs articulate the measurable and testable cyber survivability requirements, supported by the NIST cybersecurity technical controls
  - CSE SMEs identified 239 technical controls potentially applicable to weapon systems
    - ❖ 98 highly applicable, 86 somewhat applicable, and 55 requiring interpretation
- **CSE Implementation Guide (CSEIG) Ver. 2.0:** Mar 2020 (Ver. 3.0 in 2021)
- **Air Force Research Lab's (AFRL) CSA Tool:**
  - Integrates DoD CIO's CSEIG Vol. 2 and NSA's CSEIG Vol. 3 guidance to support decomposing CSAs into measurable/testable requirements
  - Maps NIST SP 800-53 Rev 5 controls to CSAs
    - ❖ DoD starting review of MITRE and AFRL's proposed Rev 5 to CSA mappings.
    - ❖ Need CNSSI 1253 and DISA CCI updates, but more critical for RMF than CSE
    - ❖ Need to find funding for "strength-of-implementation" updates (CSEIG vol. 3)
  - Will map MITRE ATT&CK TTPs and future national vulnerability DB
  - CSA Tool's relational DB is foundation for A&S's Cyber Risk Mitigation Tool (CRMT)

Leveraging and linking CSAs to NIST 800-53 cybersecurity technical controls enables an easier understanding and implementation by cybersecurity professionals, and informs mission-focused requirements to support operational risk trade-space decisions

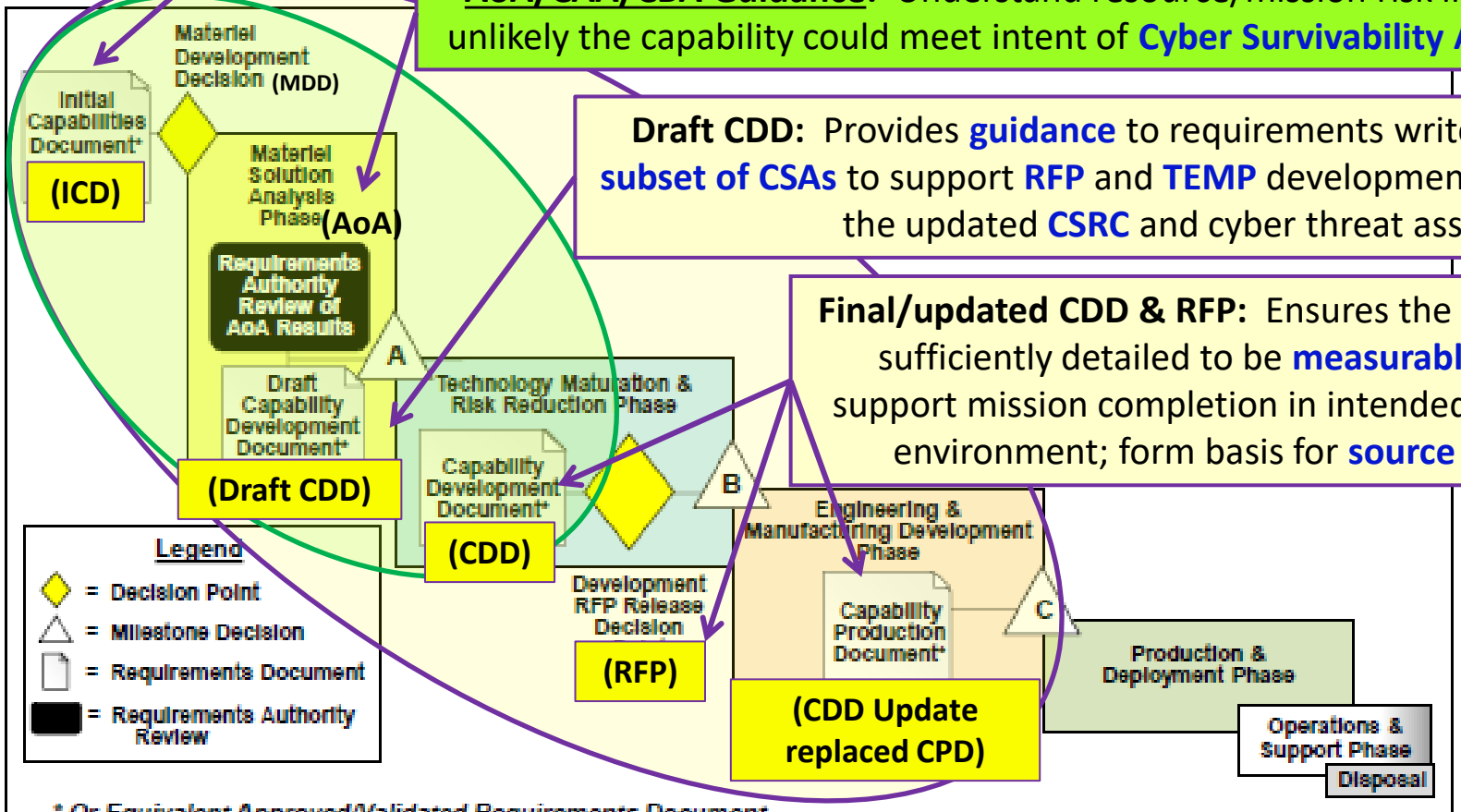
CSE's Greatest Impact: Start Early!

ICD: Cyber Survivability Risk Category (CSRC) summary statement incorporates an unclassified **projected cyber threat** and **mitigations** before formal threat assessment

AoA/CAA/CBA Guidance: Understand resource/mission risk implications if it is unlikely the capability could meet intent of **Cyber Survivability Attributes (CSAs)**

Draft CDD: Provides **guidance** to requirements writers on **tailoring a subset of CSAs** to support **RFP** and **TEMP** development consistent with the updated **CSRC** and cyber threat assessment at MS A

Final/updated CDD & RFP: Ensures the **tailored CSAs** are sufficiently detailed to be **measurable and testable** to support mission completion in intended cyber-contested environment; form basis for **source selection criteria**



* *Or Equivalent Approved/Validated Requirements Document.*

AoA: *Analysis of Alternatives*

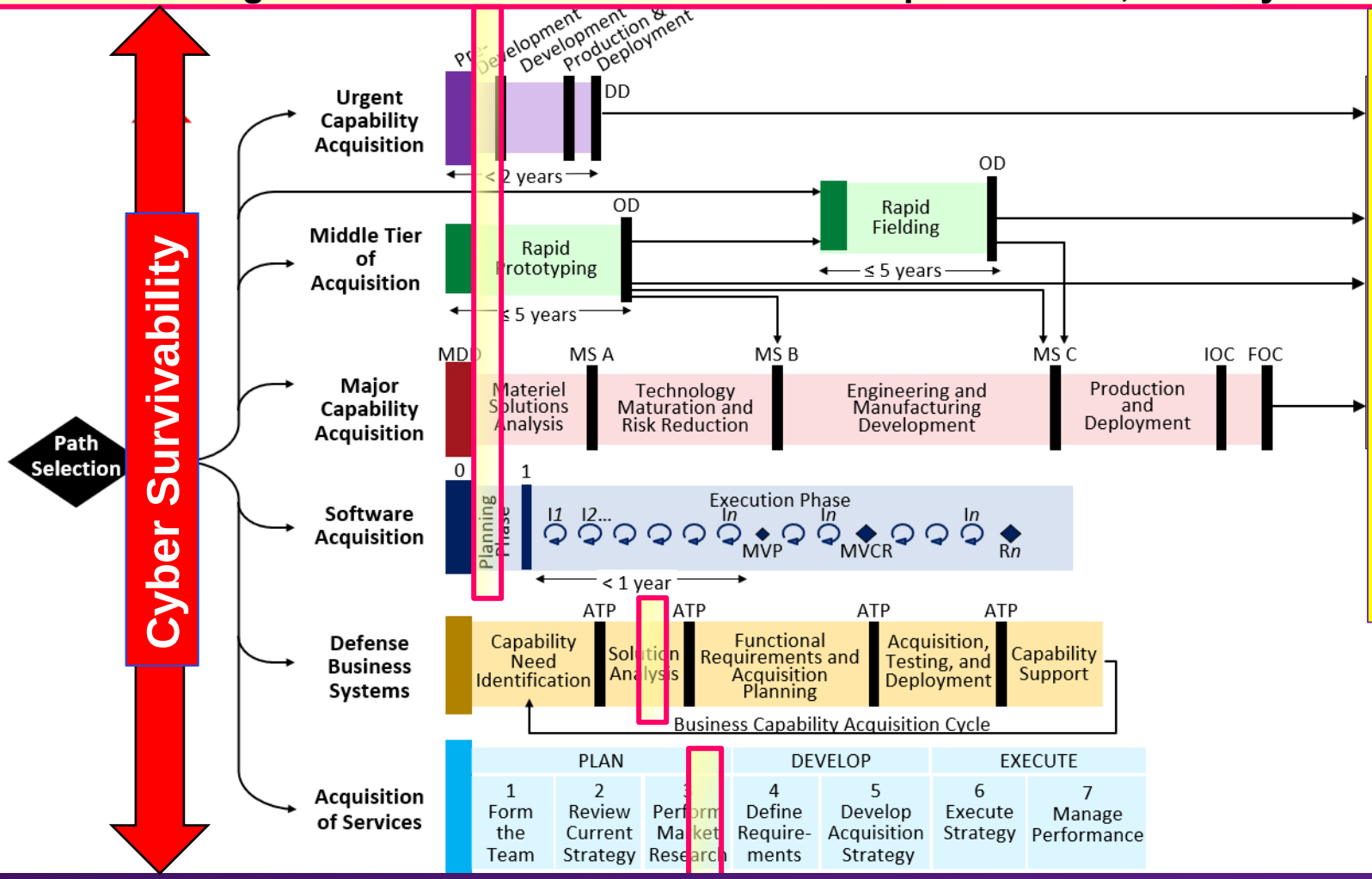
CAA: *Course of Action Analysis*

CBA: *Capability Based Assessment*

Contrary to popular belief: If the ICD, AoA, CDD and RFP consider cyber survivability, it reduces risk of acquiring capabilities so flawed it is inconceivable the cyber vulnerabilities could be cost effectively mitigated to an operationally acceptable level

Cyber Requirements – Early, AND Throughout O&S

Considering risk of "alternatives" can reduce acquisition risk; an early fail is also a win!



Operations And Sustainment

*** Actively managing the system's configuration to maintain an operationally-relevant Cyber Survivability Risk Posture (CSRP) throughout its lifecycle**

Understanding resource/mission risk implications, if alternatives are not able to meet intent of Cyber Survivability Attributes (CSAs), reduces resource, system and mission risk throughout the system's lifecycle, if adapting continues during Ops & Sustainment

Analysis of Alternatives – Assessing Cyber Survivability

Purpose: AoAs are meant to investigate, assess, and ultimately, recommend the best way(s) to proceed with meeting a validated capability requirement. It is an analytical comparison of the operational effectiveness, suitability, and lifecycle cost of alternatives that satisfy the capability's needs.

- Analyzing cost, schedule, and performance trade-space ("both the capability of the options examined and the effect each option has on mission accomplishment.")
- Initial methods of system employment, as well as tactics, techniques, and procedures for the system, are established (these may change with new information).
- The requirements for the alternatives are prioritized; the analysis is to balance precision, simplicity, and economy, adding complexity only to provide needed explanatory power, applying the appropriate level of fidelity that best informs (timely) decisions.
- The team/study are designed to quantify options' likely performance, and the effect on mission accomplishment; and conduct sensitivity analysis to identify the dependence of results on key parameters of the analysis, enabling decision makers to understand whether the solutions examined (and recommended) are robust.

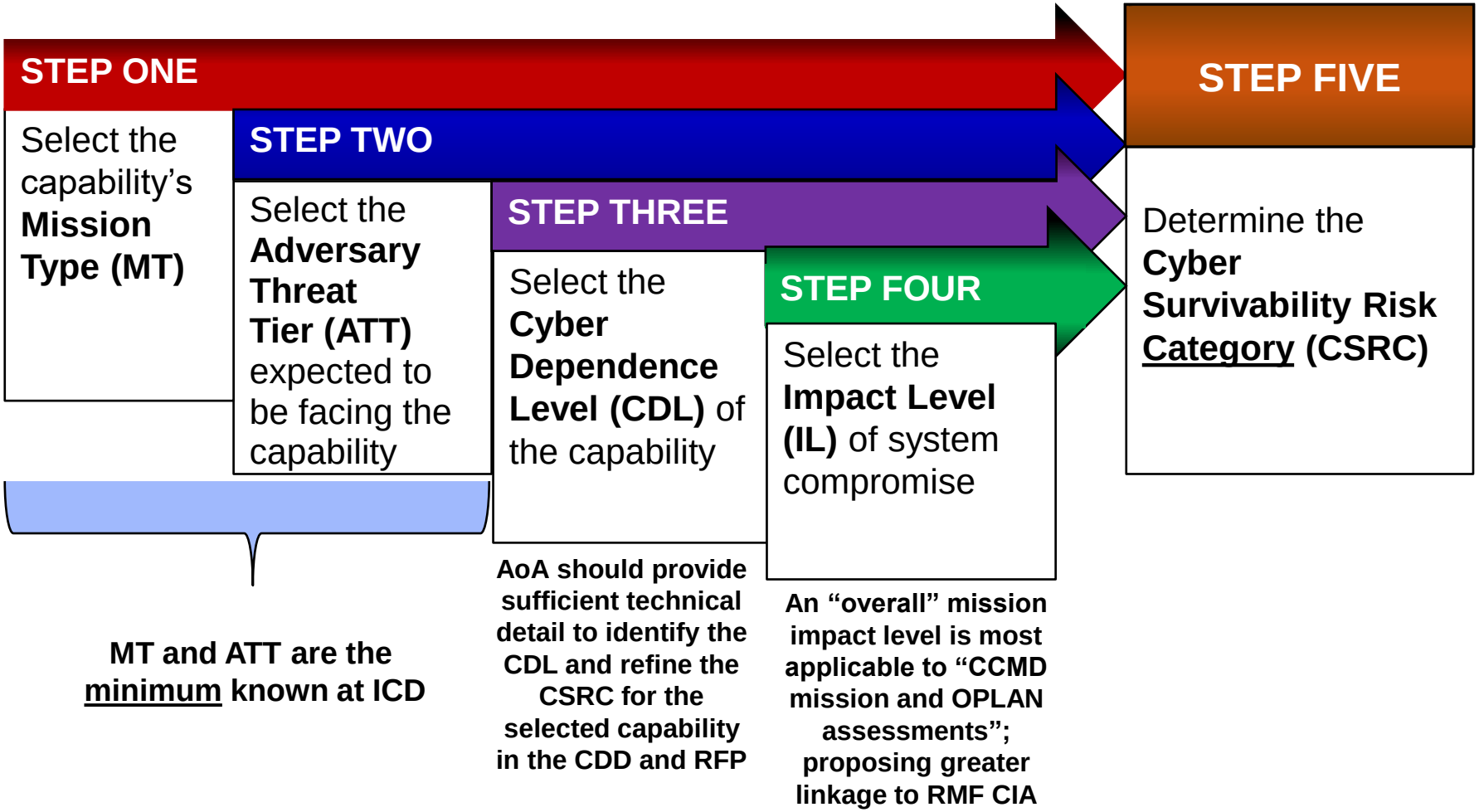
AoAs which don't consider system (cyber) survivability 'performance' requirements run the risk of recommending pursuit of a foundationally flawed capability, and incurring unaffordable cost growth in attempting to 'backfit' it later

Supports Rapid Acquisition/RMF and Abbreviated CDD

- **Requirement sponsors are able to use the CSE (cybersecurity and cyber operational resilience) process to:**
  - Understand the likely threat posed to their capability without a detailed threat assessment informed by technologies identified during the AoA/CBA
  - Assess the resource and system/mission risk implications of the as-is capability's ability/inability to meet the holistic set of CSAs
  - Select and tailor a subset of the 10 CSAs determined to be most critical to their capability's system survivability as threshold performance attributes
  - Use CSA threshold performance requirements as source selection criteria to ensure capabilities are not acquired that are so flawed that it is inconceivable that the cyber vulnerability risks could be cost-effectively mitigated to an acceptable level
- **System security engineers can decompose the subset of critical CSAs into cybersecurity and cyber operational resilience technical controls to:**
  - Enable operational risk trade-space decisions, included with all of other functional performance requirements, as long as it is possible that cyber vulnerability "risks" can be mitigated to achieve an operationally acceptable cyber risk posture
- **Milestone Decisions can be based on plans/effectiveness of implementing CSAs**
- **Authorizing Officials can determine if the RMF compliance issues place an unacceptable risk to the CSAs identified as critical to the system's survivability**

CSE's framework and set of measurable and testable attributes provide a foundation for a consistent understanding of cyber survivability requirements throughout a system's lifecycle

The Risk-Managed Approach to Determining CSRC



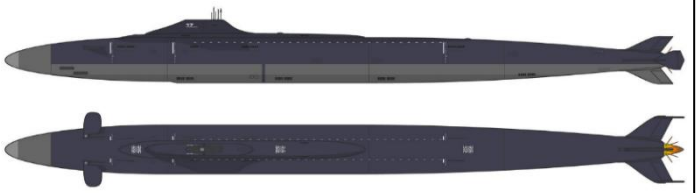
The 5 step approach takes appropriate variables into account; the resulting CSRC provides consistency between levels of CS requirements during development, testing and O&S

Step 1: Mission Type (MT)

Contested Environment

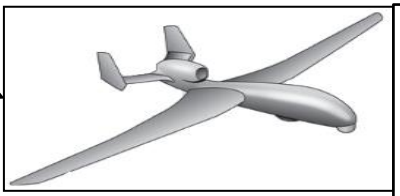
MT 5 – Strategic / National Deterrence

Degradation results in the highest risks to achieving national objectives. Requires the very best DoD Unique and cybersecurity practices for the highest levels of C, I, & A. (Ex. Nuclear deterrence, NC3, Space systems, national logistical systems, international communications network)



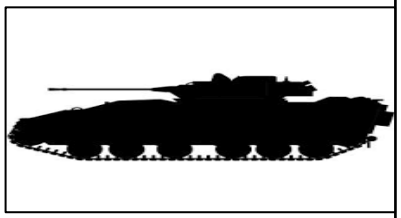
MT 4 – Operational – before and during first 72 hrs

Degradation results in high risk to mission completion. Requires DoD-unique cybersecurity practices for high levels of C, I, & A. (Ex. Primary C2, logistics, combat enablers, and integrated weapon systems/munitions for contested environments)



MT 3 – Tactical – before and during first 72 hrs

Degradation results in high to medium risk to mission completion. Requires DoD-unique cybersecurity practices for high levels of C, I, & A. (Ex. Tactical weapon systems/munitions for contested environments)



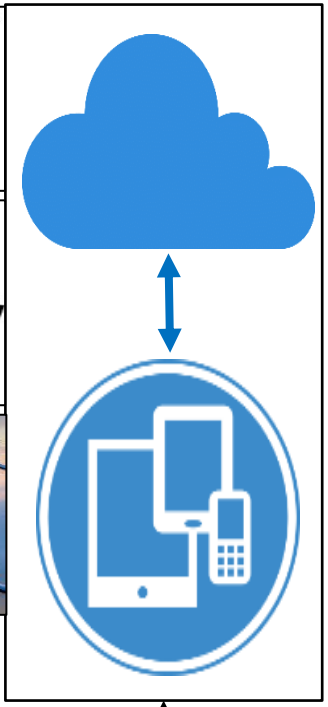
Permissive Env.

MT 2 – Mission Support – after first 72 hrs

Degradation results in moderate risk to mission completion. Requires DoD-unique cybersecurity practices for moderate levels of C, I, & A. (Ex. Logistics, mission and weapon systems for permissive environments)

MT 1 – Organizational Programs & Services

Degradation results in low risk to mission completion. Requires best business cybersecurity practices levels of C, I, & A. (Ex. Finance, MWR, and health systems)



Determining the capability's Mission Type helps define the required level of cyber survivability protections

Proposed ATT Tiers for CSEIG v3 – still working with J-2 and DIA

Step 2: Adversary Threat Tier (ATT)

Adversary Threat Tier → Most Likely & Greatest Risk

ATT 5 – Extreme: Reserved for the most formidable nation states' 'best of their best' APT capability using multiple attack vectors that cause denial, degradation, deception, disruption or destruction of mission capabilities. May develop detailed technical and system knowledge of the target system to deploy more damaging cyber attacks.

ATT 4 – Advanced: May conduct complex, long-term cyber attack operations that combine multiple intelligence sources to obtain access to high-value networks. May develop detailed technical and system knowledge of the target system to deploy more damaging cyber attacks.

ATT 3 – Moderate: Able to develop and use customized malware to 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: 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 or industry beyond publicly connected open-source information.

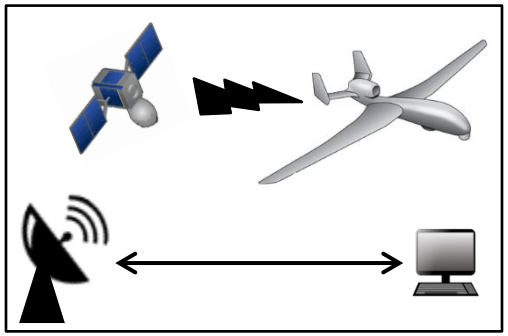
Source: GAO analysis of Department of Defense (DOD) information, GAO-19-128

Updated intelligence assessments need to include relevant adversary capabilities and potential approaches for the cyber kill-chain vs. fielded HW/SW/FW

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

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

Cyber Dependence is based upon the intrinsic cyber survivability risks associated with performing its mission critical functions of Move, Shoot and Communicate

Step 3: Cyber Dependence Level (CDL)

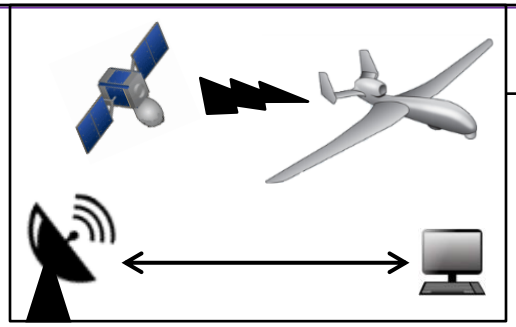
Technical Exposure	Degree of Connectivity & Dependence (Operational requirements for internal & external information exchange)	CDL Level
Broad	**Extreme** - Systems are entirely dependent on cyber connectivity and functionality, reliant on other systems, and will likely not function at all without full, high-bandwidth network support (wired and wireless). Ex. AI/ML (automated response), continuous comms over networks or complex SW/HW, with no human to take control in unmanned and robotic/autonomous system	CDL 5
Limited	**High** - Systems are dependent on cyber connectivity and functionality, but are able to function to a limited extent with intermittent or low-bandwidth network support (wired and wireless) Ex. AI/ML (non-automated response)	CDL 4
Restricted	**Moderate** - Systems are somewhat dependent on cyber connectivity and functionality, but can operate effectively with intermittent or low-bandwidth network support (wired and wireless)	CDL 3
Narrow	**Low** - Systems have little dependence on cyber connectivity and functionality, and can operate effectively for long periods without network support (wireless)	CDL 2
Narrow to None	**Very Low** - Systems have no external communication requirements during operations, and can operate effectively with no network support	CDL 1
None	**No Cyber Dependence** - No electronic sensors, no electronic processing/storage, and no internal/external information exchange requirements	CDL 0

Technical exposure (origin, export, sys architecture) combines with Degree of connectivity (based on operational requirements) → to define a system's Cyber Dependency Level

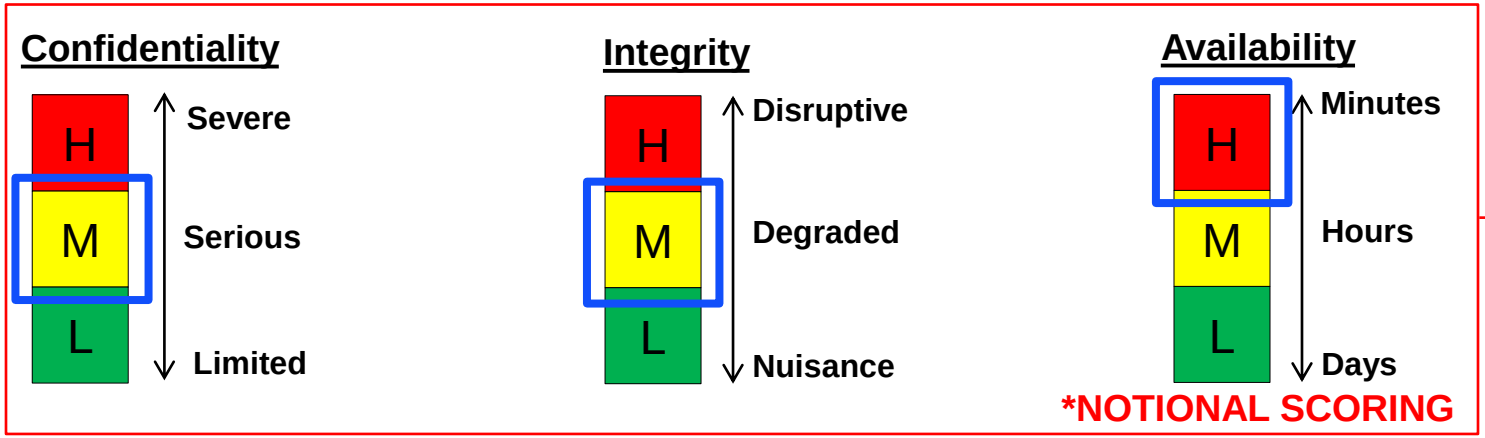
Step 4: Impact Level (IL)

Example

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



Mission Critical Functions
I Move: Sustained Flight / Maneuverability
II Shoot: Offensive / Defensive Capabilities
III Communicate: Internal / External



- **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

The weighting of C-I-A for each critical function will vary, depending on weapon system

Step 4: Impact Level (IL)

Overall mission Impact Level (IL) of system loss or compromise. Aligns with RMF Security Impact Levels

IL 5: Catastrophic Adverse Effect (RMF IL High) – A compromise of system confidentiality, integrity, and availability would lead to complete mission failure with few, if any, mission objectives accomplished and likely friendly force losses.
IL 4: Serious Adverse Effect (RMF IL High) – A compromise of system confidentiality, integrity, and availability would seriously degrade mission performance leaving some mission objectives unaccomplished and endangering friendly forces.
IL 3: Moderate Impact (RMF IL Moderate) – A compromise of system confidentiality, integrity, and availability would partially degrade mission performance, requiring more time or other resources to accomplish mission objectives and possibly endangering friendly forces.
IL 2: Limited Impact (RMF IL Low) – A compromise of system confidentiality, integrity, and availability would have little effect on mission accomplishment and would not likely endanger friendly forces.
IL 1: No Impact (RMF IL Low) – A compromise of system confidentiality, integrity, and availability would have little effect on mission accomplishment and would not likely endanger friendly forces.

What is the CCMD's mission / OPLAN impact if a weapon system's critical functions (move, shoot, communicate) are cyber-compromised?

The Five Step Approach to determine CSRC

STEP 1: Select Mission Type	STEP 2: Adversary Threat Tier	STEP 3: Select Cyber Dependency Level (CDL)	STEP 4: 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: Serious 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 Programs/Services	ATT 1: Nascent	CDL 1: Very Low	IL 1: No Impact
		CDL 0: No Cyber Dependence	

STEP FIVE: Determine Cyber Survivability Risk Category
CSRC 5 – Extreme: Mitigations rely on state-of-the-art technologies and countermeasures, to include offensive protections to preclude the likelihood of threat. (draft, not fully coordinated)
CSRC 4 – Very High: Mitigations rely on best available countermeasures, to include custom DoD protections, commensurate against assumed threat capabilities.
CSRC 3 – High: Mitigations include Enhanced Assurance – redundancy, and TTPs, strong COTS/GOTS securely configured in layered architectures – with DoD added technology, as needed.
CSRC 2 – Moderate: Mitigations include COTS/GOTS cybersecurity products and technologies, with potential DoD technology additions, with best practices, strong DoD layered defenses, and selective use of DoD technology.
CSRC 1 – Low: Mitigations include COTS with best practices if commercially hosted, or strong DoD layered defenses, possible use of DoD technology if DoD hosted
CSRC 0 – None: No requirement for information exchange, HW/SW/FW processor/storage, or network connection (wired or wireless).

Modern weapon systems with Joint Interest are likely to be CSRC-3, with an ATT of 3

Step 5: Cyber Survivability Risk Category (CSRC)

Vulnerability + Threat Capability = Survivability Risk

CSRC 5: Extreme – Mitigations rely on state-of-the-art technologies and countermeasures, to include offensive protections to preclude likelihood of threat. (not fully coordinated)

CSRC 4: Very High – Mitigations rely on best available COTS/GOTS countermeasures, to include custom DoD protections, commensurate against assumed threat capabilities.

CSRC 3: High – Mitigations include enhanced assurance (redundancy, TTPs, strong COTS/GOTS securely configured within layered architectures) with DoD technology additions as needed [most DoD Weapon Systems]. NOTE: GOTS "services" can be used to meet CSA requirements (ingest classified signatures; compliment or integrate with COTS capabilities to identify / respond to anomalies)

CSRC 2: Moderate – Mitigations include both COTS and GOTS cybersecurity technologies, with addition of specific threat signatures and TTP best practices.

CSRC 1: Low – Mitigations include COTS with best practices if commercially hosted, or strong DoD layered defenses, possible use of DoD technology if DoD-hosted.

CSRC 0: None – No information exchange, no processor HW/SW/FW, no network, wired, or wireless connections.

CSRC provides consistent understanding of the level of requirements during design, testing, and operations; determined using High-Water Mark, Balanced Scorecard Adaptation, or Delphi scoring

ICD - CSRC 3 Exemplar (for AoA/CBA)

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

The system's mission criticality and impact of system compromise requires the capability must survive and operate in a high risk cyber-contested environment against the span of anticipated adversaries ranging from amateurs to very sophisticated, persistent, and well-resourced adversaries at a nation state level. Adversaries are capable of advanced cyber trade craft using publicly available and customized tools to exploit known and unknown vulnerabilities, as well as the ability to develop and stealthily implant malware/vulnerabilities to conduct wide-ranging intelligence collection operations for identifying/targeting espionage/attack on both unencrypted and isolated networks, and in some cases create limited effects against defense critical infrastructure networks. Recognizing the adversaries' current/projected cyber threat capabilities, the system must prevent or mitigate the effects of cyber events to maintain minimum functionality to complete the mission or return to base for recovery of sufficient capability to fight another day. Mitigations must ensure Confidentiality, Integrity, & Availability for trusted availability of internal and external information flows; must implement a defense in depth architecture, with no single points of failure; must leverage available DoD-developed cyber protection technologies (including consideration of protections inherited from the intended operational environment); and as required build specific custom protections, countermeasures and technologies to actively manage the system's configuration to achieve and maintain an operationally relevant CSRP. The following 10 CSAs *must be assessed for each AoA/CBA alternative to* ***understand the resource and mission risk implications***, if the capability itself, the hosting system or enterprise services are unable to provide the CSA's intent: *(list CSAs by pillar)*

INTENT: reduce risk of acquiring capabilities so flawed it is inconceivable the **known** cyber vulnerabilities could be cost-effectively mitigated to an operationally acceptable level.

Puts Cyber Survivability requirement in context by incorporating a high level "projected cyber threat" -- before AoA/CBA results can drive a cyber threat assessment and risk determination

CDD - CSRC 3 & CSA Exemplars (for RFP)

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

NOTE: Text in red is the only difference between an ICD and CDD.

The system's mission criticality and impact of system compromise requires the capability must survive and operate in a high risk cyber-contested environment against the span of anticipated adversaries ranging from amateurs to very sophisticated, persistent, and well-resourced adversaries at a nation state level. Adversaries are capable of advanced cyber trade craft using publicly available and customized tools to exploit known and unknown vulnerabilities, as well as the ability to develop and stealthily implant malware/vulnerabilities to conduct wide-ranging intelligence collection operations for identifying/targeting espionage/attack on both unencrypted and isolated networks, and in some cases create limited effects against defense critical infrastructure networks. Recognizing the adversaries' current/projected cyber threat capabilities, the system must prevent or mitigate the effects of cyber events to maintain minimum functionality to complete the mission or return to base for recovery of sufficient capability to fight another day. Mitigations must ensure Confidentiality, Integrity, & Availability for trusted availability of internal and external information flows; must implement a defense in depth architecture, with no single points of failure; must leverage available DoD-developed cyber protection technologies (including consideration of protections inherited from the intended operational environment); and as required build specific custom protections, countermeasures and technologies to actively manage the system's configuration to achieve and maintain an operationally relevant CSRP.

The following "subset" of the 10 CSAs in the table below have been determined to be most critical for **(system's name)** cyber survivability, and should drive development of RFP Resource 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 achieve and maintain an operationally relevant CSRP:

CSAs drive RFP and source selection criteria to prevent acquisition of capabilities so flawed that they could not be cost-effectively mitigated to an operationally-relevant level

SS KPP Pillars and CSAs

- **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; restoring minimum sufficient functionality (to fight another day)
- **Adapt** – enables **adapting** to changes in adversary threat and our vulnerabilities (to maintain an operationally-relevant CSRP) -- beyond initial requirements, and RDT&E

SS KPP Pillars	Cyber Survivability Attributes (CSAs)
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**
Adapt for Prevent, Mitigate & Recover	**CSA-10 - Actively Manage System's Configurations to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture (CSRP) -- supports DevOps, and is applicable to legacy systems that did not consider CSAs during development**

Select a sufficient number of the capability's most mission-critical CSAs to support each SS KPP Pillar

CSRC and Expected CSA Requirements

- **CSRC 5: 9 to 10 CSAs**
  - Probably 5-6 Prevents, 2 Mitigates, Recover and Adapt CSA
- **CSRC 4: 6 to 9 CSAs**
  - Probably 3-5 Prevents, 1-2 Mitigates, Recover and Adapt
- **CSRC 3: 5 to 7 CSAs**
  - Probably 2-4 Prevents; may implement 1 Mitigate, Recover and Adapt; probably no replacement strategy
- **CSRC 2: 2 to 5 CSAs**
  - Probably 1-3 Prevents; may implement 1 Mitigate and Recover, or a replacement strategy, but probably no Adapt
- **CSRC 1: 1 to 3 CSAs**
  - Probably 1-3 Prevents; probably implement a replacement strategy, and probably no Mitigate, Recover or Adapt CSAs
- **CSRC 0: no CSAs** (capability has no internal or external information exchange, no electronic components, and no data storage)

A system's CSRC relates to risk tolerance, driving the subset of CSAs that need to be considered, tailored, and implemented in its design to support that CSRC level

Exemplars for a CDD's CSA Table (1 of 2)

Prevent CSAs	Prevent Exemplar Language (threshold, contractually-binding rqmts)
CSA-01: Control Access	(U) "System shall only allow identified, authenticated, and authorized persons and non-person entities 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."
CSA-02: Reduce System's Cyber Detectability	(U) "System survivability requires that signaling and communications (both wired and wireless) implemented by the system (or state "supported by system/capability") shall not enable an adversary to monitor and/or target system and/or supported DoD weapon systems through its emanations."
CSA-03: Secure Transmission 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 it is a National Security System (NSS), add "System shall develop, coordinate and maintain a System TRANSEC Plan (STP) throughout the system's lifecycle."]
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)."
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 Concept of Operations. Compromise of non-critical functions shall not significantly impact system mission capability."
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."

Measurable, testable CSAs usable as Source Selection Criteria & RMF Tech Controls, DT/OT Assessments throughout lifecycle… *all CSA are intended to be tailored!*

Exemplars for a CDD's CSA Table (2 of 2)

Mitigate CSAs	Mitigate Exemplar Language (threshold, contractually-binding rqmts)
CSA-07: Baseline and Monitor Systems and Detect Anomalies	(U) "System shall implement and maintain a cybersecurity configuration baseline, to detect and report system anomalies indicative of a cyber-event. System shall monitor the cybersecurity configuration baseline of system functions, and report health status and anomalies to system operators based on system CONOPS (e.g., System shall notify system users of anomalies such as configuration changes, cyber-event indicators, slowed processing or loss of functionality within T = (#) and O = (# of seconds/minutes) [specified by sponsor]."
CSA-08: Manage System Performance if Degraded by Cyber Events	(U) "If anomalies are detected and/or cyber-events degrade system capability, the system shall be sufficiently resilient to mitigate cyber-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. 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 the Department of Defense Information Network (DoDIN)."
Recover CSA	**Recover Exemplar Language (threshold, contractually-binding rqmts)**
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 between mission cycles or within xx hours, in order to fight another day. System recovery shall prioritize critical functions." [time and functionality metrics consistent with mission needs]
Adapt (P/M/R) CSA	**Adapt Exemplar Language (threshold, contractually-binding rqmts)**
★ **CSA-10: Actively Manage System's Configurations to Achieve and Maintain an Operationally-Relevant Cyber Survivability Risk Posture (CSRP)**	(U) "Throughout a system's lifecycle and within one standard mission cycle of xx hours of identification of a drop in CSRP below its CSRC for operational systems, and xx days for systems in development ["xx" timelines specified by sponsor], the system shall have a configuration management process supported by automated capabilities to achieve and continuously maintain an objectively assessed, operationally-relevant CSRP commensurate with its CSRC level. The process shall continuously assess the adversary threat to prioritize and mitigate vulnerabilities in the system's hardware, software, firmware, connected infrastructure and supply chain with the greatest mission risks." NOTE: Objective statements are not necessary if CSA-10 is effectively resourced to address unforeseen risks due to changes in vulnerabilities/ threat capabilities)

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

CSA-10's Focus: Monitor, and Adapt to, Cyber Risks throughout Lifecycle

All future and legacy "mission-critical" systems should have a funding line for:

CSA-10: Actively manage system's configurations to achieve and maintain an operationally relevant Cyber Survivability Risk Posture (CSRP)

"Throughout the system's lifecycle and within one standard mission cycle of xx hours of notification of a drop in CSRP below its CSRC for operational systems, and xx days for systems in development [timelines specified by sponsor], the system shall have a configuration management process supported by automated capabilities to achieve and maintain an objectively assessed, operationally-relevant CSRP commensurate with its CSRC level. The process must continuously assess the adversary threat to prioritize and mitigate vulnerabilities in the system's hardware, software, firmware, connected infrastructure and supply chain with the greatest mission risk."

Most critical CSA, and applicable to both future and legacy systems: No matter how much risk was accepted on day 1, if properly resourced/supported, and if AoA did not select a foundationally-flawed capability, CSA-10 supports execution of a POA&M to maintain an operationally-relevant CSRP.

This is DevOps~~/DevSecOps~~: Keeping survivability requirements in operational risk trade-space, where operators own the responsibility for mitigating mission risks discovered during operations, is what enables use of CSA-10 by all mission-critical legacy systems. We believe that industry is seeing greater security when DevOps teams realize there will be no "DevSecOps Security Cavalry" to fix their errors

This is not a "management reserve". On the first day a system is fielded, there is a known list of vulnerabilities being accepted, which should initiate requirement to actively assess, identify, prioritize and buy-down those with highest "mission risks"

WS/CI Example: Quarterly Service CSRP w/CSA Remediation POA&M

Cyber Survivability Attribute (CSA)	FY21 Assessed "As-Is" of CSA Threshold Requirements	FY22 Residual Risk (If planned/funded are implemented/tested)	FY23 Residual Risk (If planned/funded are implemented/tested)	FY24 Residual Risk (If planned/funded are implemented/tested)
CSA-01: Control Access (for WS, the *"intent"* of 2FA can be met with physical controls like guards w/guns, access logs, ids, visual recognition)	Incomplete user/admin 2FA, RBAC and PKI, or identified physical security access risks	User 2FA, RBAC & PKI. Minimize remote physical access risk. Resource C2C	Admin 2FA, RBAC & PKI. Minimize local physical access risk	Test implementation of User/Admin 2FA/RBAC/PKI, physical security, and C2C
CSA-02: Reduce System's Cyber Detectability (most costly and least likely)	**No CSA-02 requirement identified**	**N/A**	**N/A**	**N/A**
CSA-03: Secure Transmissions and Communications (**SCP CRYPTO**, Data transit)	Crypto uncertified/obsolete, no System TRANSEC Plan 0-49% funded, 12+mo delay	Fund/develop crypto server, publish STP	Implement certified crypto server	Test implementation of crypto, assess STP and if upgrades funded/on-sched
CSA-04: Protect System Information from Exploitation (Data at rest)	Lacks data integrity checks and encryption at rest	Resource C2C	Implement C2C w/policies to mitigate risk integrity and mobile device data	Test C2C policies to mitigate risk to data integrity, and mobile device data at rest
CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels	Lacks certified partitioning of critical functions, with no physical/logical diversity	Resource C2C	Implement C2C w/policies to mitigate risk to move, shoot and comm functions	Test C2C policies to mitigate risk to move, shoot and comm functions
CSA-06: Minimize and Harden Attack Surfaces (**SCP KNOWN VULNERABILITIES**)	Publicly known external and internal interface vulns. No autopatch or C2C	Prioritize/mitigate system vulns w/greatest risk. Resource autopatch & C2C	Implement autopatch, C2C w/ policy mitigations to reduce int/ext interface risk	Test autopatch & C2C policy mitigations, to reduce int/ext interface risk
CSA-07: Baseline and Monitor (**SCP**) Systems and Detect Anomalies	No baseline, uncertified CSSPs, w/o tools to mon/reprt	Define baseline. Certify T3 CSSP w/tools to monitor/rpt	Certify Tier 2 CSSP, w/tools monitor/report	Exercise T3/T2 CSSPs w/ tools, C2C mon/rpt risk
CSA-08: Manage Sys Perf if Degraded by Cyber Events (To Complete Mission)	No failover, uncertified CSSPs w/o tools to mitigate events	Certify T3 CSSP w/tools to mitigate events, ID failover	Certify T2 CSSP w/TS clearance to coord, failover	Exercise T3/T2 CSSPs w/ tools/C2C to coord response
CSA-09: Recover System Capabilities (To Fight Another Day)	No automated processes, recovery > 72 hours	Automate some processes recovery < 24 hours	Automate most processes recovery < 8 hours	Exercise C2C policies for trusted recovery < 4hrs
CSA-10: Actively Manage System's Configuration to Achieve and Maintain Operationally Relevant CSRP (Adapt – **SCP HYGIENE+**, Support continuous RMF/DevOps)	CSA-10 not funded, unable to actively assess and pri/mit HW/SW/FW vulns w/greatest risk, CSRP 2+ levels < CSRC Must do mits > 28 days	Resource CSA-10, CSRP 2+ levels < CSRC Must do mits > 28 days	Funded. CRSP stagnant CSRP 1 level < CSRC Must do mits 15 - 28 days	Funded. CRSP rising, but CSRP 1 level < CSRC Must do mits 3 - 14 days
Cyber Survivability Attribute (CSA) Cyber Survivability Risk Posture	**1 – Low Protect High Risk**	**1 – Low Protect High Risk**	**2 – Moderate Protect Medium Risk**	**3 – High Protect Low Risk**

SCP "CSA" Risk Posture | **SCP Risk ScoreCard** | **SCP "CSA" Remediation ScoreCard … by FY**

Way Ahead

- Identify SS KPP lessons learned to improve DoD and Joint Staff guidance to implement and maintain CSE's threshold cyber requirements throughout lifecycle
- Update DoDIs and CJCSIs to apply CSE framework to Accelerated Acquisition and Rapid RMF, orchestrating alignment of DoD best practices, even if recently updated
  - E.G., **DoDI 5000.02, 5000.cs, 5000.ul, 8580.01**, 8500.01, 8510.01, 8115.01
  - Include process for identifying legacy systems critical to CCMD OPLANs/missions and adding a CSA-10 like capability to achieve and maintain an operationally relevant CSRP, and reporting to MACB or other Boards for programmatic decisions
- Rationalize DoD assessment methodologies to determine system, system-of-systems and CCMD OPLAN/Mission Cyber Survivability Risk Postures
- Work with A&S to identify vulnerabilities and mitigation options associated with the GOTS/COTS HW/SW/FW by version # integrated within DoD capabilities
- Work with Intelligence Community to provide quarterly adversary cyber threat updates associated with the HW/SW/FW integrated within DoD capabilities
- Use CSE's holistic framework to define a CCMD OPLAN/Mission-focused and scalable governance process that preserves CC/S/A and OSD/JS responsibilities for prioritizing cyber vulnerabilities with the greatest mission risk

Leverage CSE's holistic framework to orchestrate DoD's cyber survivability efforts to achieve an ROI greater than the sum of our individual efforts

Questions?

J-6 Cyber Survivability

Mr. Steve 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

Mr. Tom Andress, CISM, DAWIA PM
JS Cyber Survivability Analyst
703-692-0905
NIPR: Thomas.R.Andress.ctr@mail.mil
SIPR: Thomas.R.Andress.ctr@mail.smil.mil

Mr. Evan Lundh
Advanced Cyber Threat Analyst
703-614-7393
NIPR: Evan.F.Lundh.ctr@mail.mil
SIPR: Evan.F.Lundh.ctr@mail.smil.mil

Mr. James Brown, CISSP
Cyber Survivability Analyst
703-697-8276
NIPR: James.L.Brown2.ctr@mail.mil
SIPR: James.L.Brown2.ctr@mail.smil.mil