New DoD Approaches on the Cyber Survivability of Weapon Systems

Mr. Steve Pitcher, GS-15, CISSP
JS Senior Cyber Survivability Analyst
Cyberspace Division, Joint Staff/J-6

Updated: 25 Mar 2019

CSE is the critical foundation for ensuring Cyber Survivability Attributes (CSAs) considered as part of the Operational Risk Trade-Space … CSE does NOT define any new CS requirements … it helps requirement sponsors understand the risk and articulate their CS requirements, with CSAs driving Source Selection Criteria and justifying specific RMF CS Technical Controls

x

Background: Cyber Vulnerability Assessments

- **DepSecDef (DSD) initially directed Joint Staff develop Cybersecurity KPP**
  - Initiated when DSD briefed on DOT&E Cybersecurity Report w/ OUSD(AT&L), OUSD(P), DOD-CIO and VCJCS … *Highlighted multiple weapon systems with vulnerabilities that should have been known and fixed prior to DT&E…continue to find...fixes hard/costly…*
  - **Problem:** System survivability requirements not sufficiently articulated for cyber-attack prevention, mitigation and recovery, within requirements documents … Threshold = ATO

Three Pronged Approach

- **Improving Cyber Survivability of New Weapon Systems**
  - **JCIDS Manual Dec 2015:** Added Cyber Survivability Endorsement SS - KPP
  - **JROCM (Jan 2017):** Cyber Survivability Endorsement Implementation Guide
  - **JCIDS Manual Aug 2018:** Now includes ICDs and more specifics on CSRC and CSAs
- **Improving Cyber Survivability of Legacy Weapon Systems –> Dec 2019+**
  - **FY16 NDAA 1647:** Evaluation of Cyber Vulnerabilities of DoD Major Weapon Systems
  - **JROCM 39-16 (May 2016):** prioritized 136 critical weapon system assessments, binned by Mission, CCMD mission based assessments and risk mitigation prioritization
- **Improving Cyber Surv. of DoD Installation Critical Infrastructure –> Dec 2020**
  - **FY17 NDAA 1650:** Eval of Cyber Vulnerabilities of DoD Installation Critical Infrastructure
  - **JROCM 137-17 (Dec 2017):** prioritized 474 installation assessments

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

x

CSE Momentum

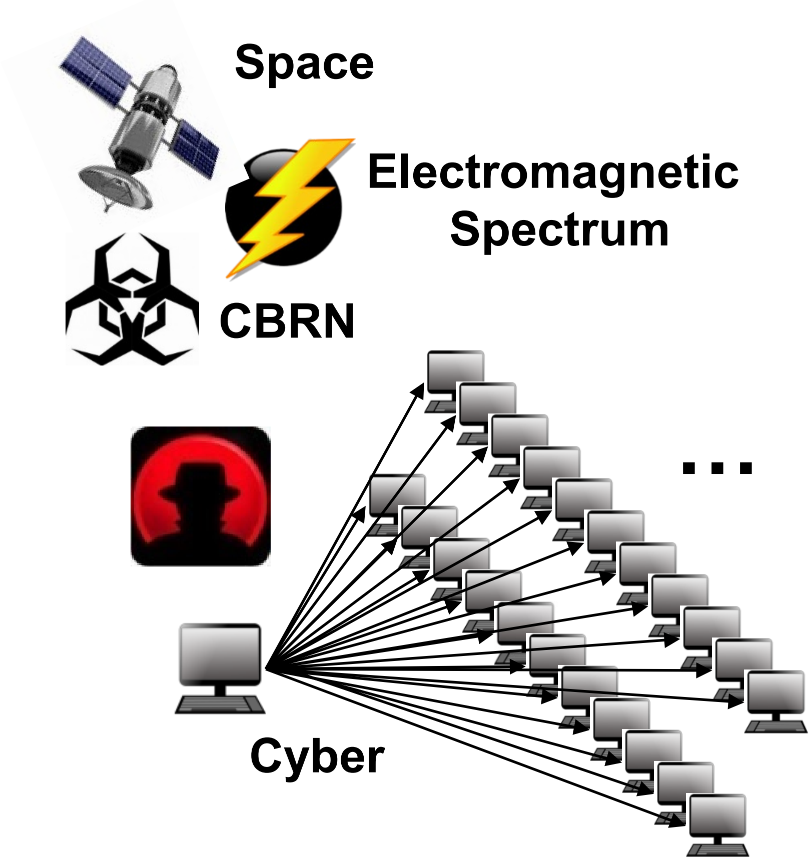
- **Improving Cyber Survivability of New Weapon Systems**
  - **Dec 2015:** JCIDS Manual added Cyber Survivability Endorsement (CSE) to SS - KPP
  - **Jan 2017:** JS formally approved CSE Implementation Guide (IG)
  - **Feb 2017:** DoD-CIO published CSE-IG companion document
  - **Feb 2018:** DAU RQM-310, Adv Requirements Mgmt curriculum includes CSE
  - **Apr 2018:** OUSD(R&E) and DOT&E DoD Cybersecurity Test and Evaluation Guidebook includes CSE
  - **Apr 2018:** DOT&E DoD Operational Test guidance includes CSE
  - **Apr 2018:** Air Force System Security Engineering guidance includes CSE
  - **Jul 2018:** OUSD(R&E) published DoD Cyber Table Top Guidebook includes CSE
  - **Aug 2018:** JCIDS update includes ICD reviews and more specifics on CSRC and CSAs
  - **2019:** AFRL working with NSA, CIO and JS to develop CSA Tool to support requirement definition, acquisition, technical control engineering, testing, authorizing official and maintaining cybersecurity posture during O&M…management support tool.
  - **2019:** Working on Standardizing Assessment Levels, Mission Based - Deep Cyber Resiliency Assessment (DCRA) process, and prioritizing mitigations across the DoD.

CSE is only mandatory for requirements going through JCIDS process, but JROCM recommended requirement sponsors use CSE-IG or develop their own guidance

SS-KPP & Cyber Survivability Endorsement

Kinetic Threats

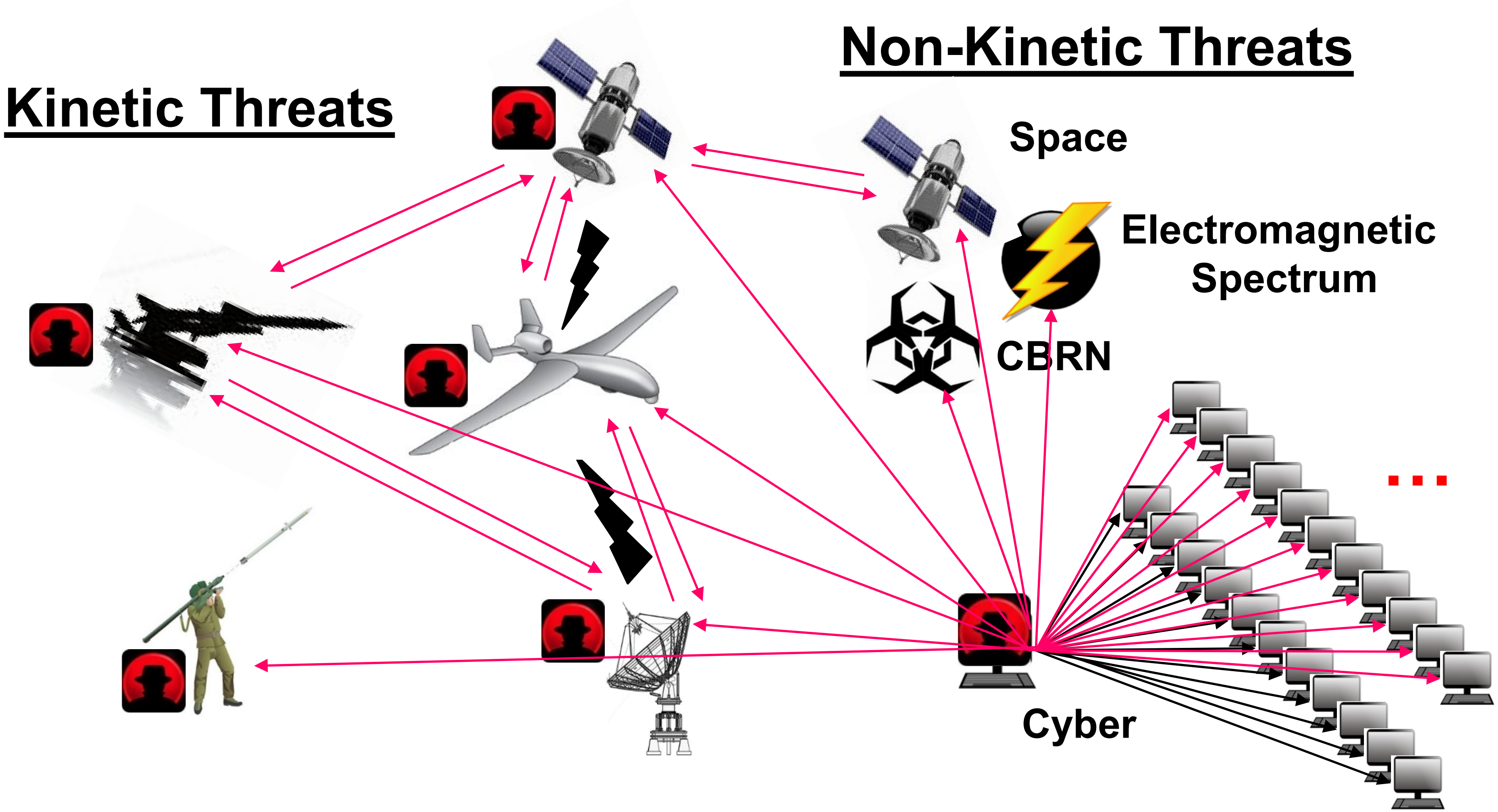
Non-Kinetic Threats



Paradigm Shift

1+ kinetic bullet → 1 kinetic kill … 1 cyber bullet → 1+++ kinetic kills, multi-path

SS-KPP & Cyber Survivability Endorsement

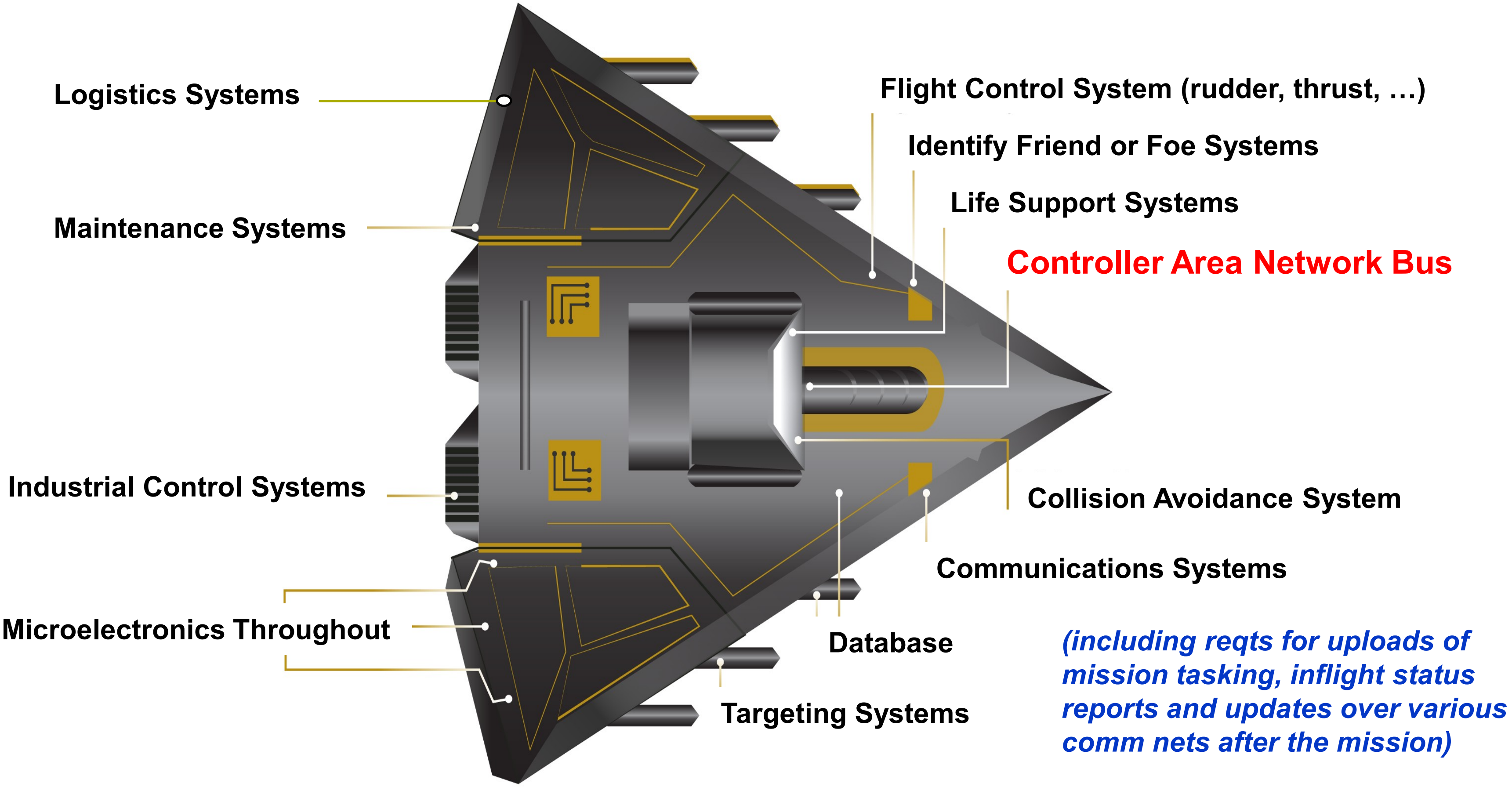


Paradigm Shift

1+ kinetic bullet → 1 kinetic kill … 1 cyber bullet → 1+++ kinetic kills, multi-path

Degree of Connectivity and Operational Requirements

(Pervasiveness Represented via Fictitious Weapon System for Classification Reasons)


Logistics Systems
Maintenance Systems
Industrial Control Systems
Microelectronics Throughout
Flight Control System (rudder, thrust, …)
Identify Friend or Foe Systems
Life Support Systems
Controller Area Network Bus
Collision Avoidance System
Communications Systems
Database
Targeting Systems

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

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

Functionality designed for good … can also be used for evil…

SS-KPP Pillars and Cyber Survivability Attributes

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

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

Fundamental to CSE construct is sponsor to selecting/articulating CSA choices to achieve each SS KKP Pillar … Min of 1 per Pillar, but historically → CSRC-4 (9-10), CSRC-3 (6-8), CSRC-2 (4-6)

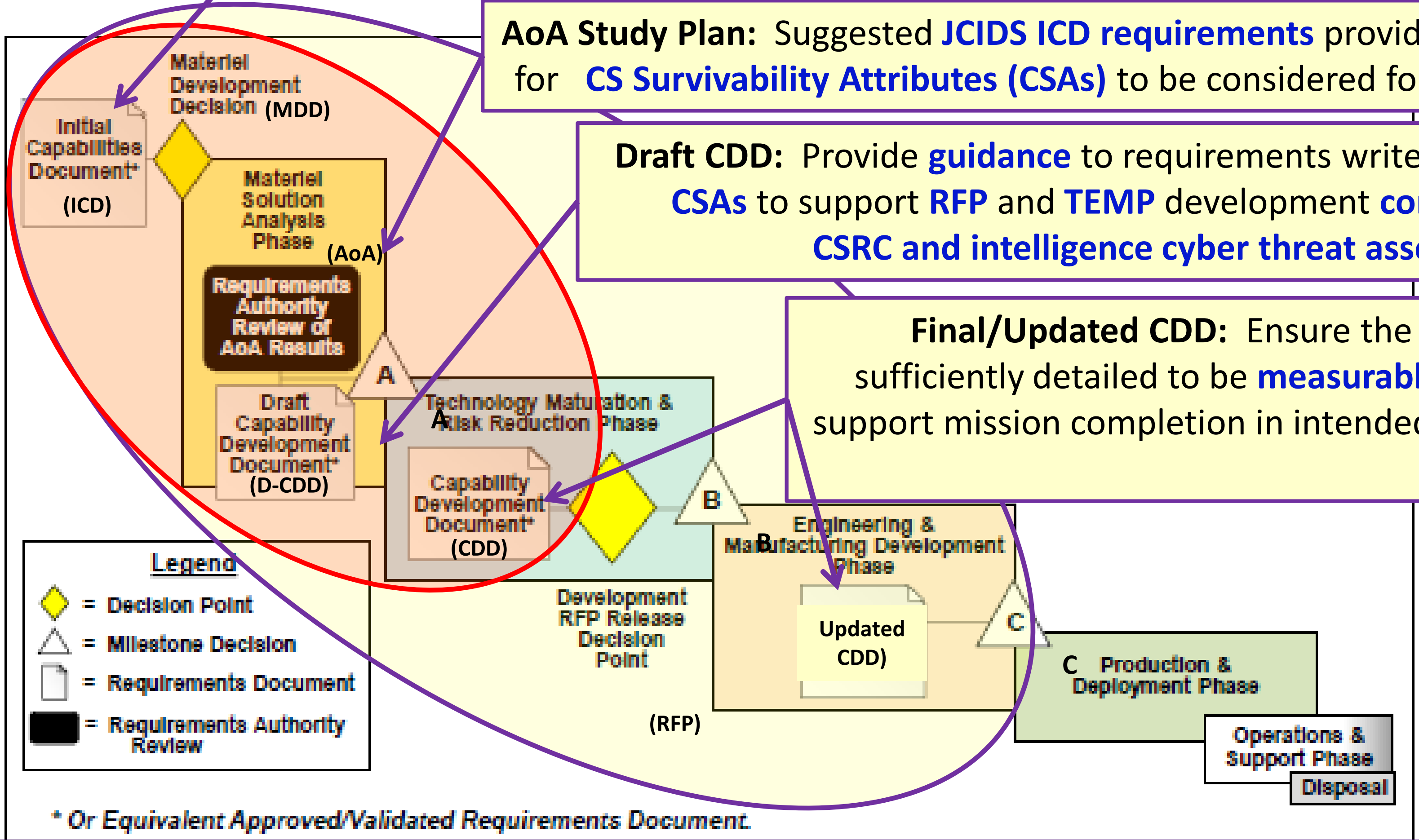
CSE's Greatest Impact Opportunity

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

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

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

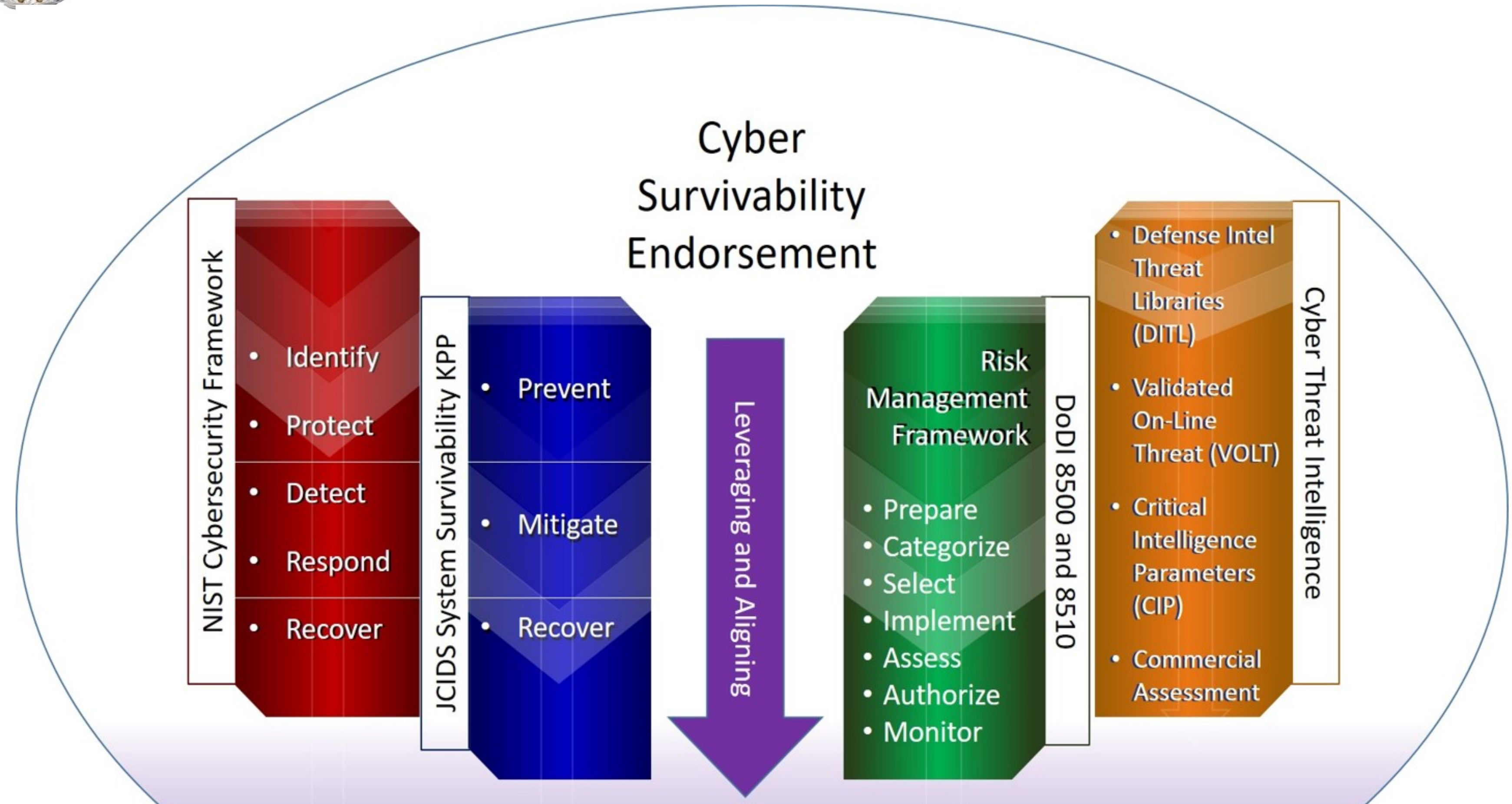
Final/Updated CDD: Ensure the **tailored CSAs** are sufficiently detailed to be **measurable and testable** to support mission completion in intended cyber contested environment


Materiel Development Decision (MDD)
Initial Capabilities Document* (ICD)
Materiel Solution Analysis Phase (AoA)
Requirements Authority Review of AoA Results
A
Draft Capability Development Document* (D-CDD)
Technology Maturation & Risk Reduction Phase
A
Capability Development Document* (CDD)
B
Development RFP Release Decision Point
(RFP)
Engineering & Manufacturing Development Phase
B
Updated CDD)
C
C Production & Deployment Phase
Operations & Support Phase
Disposal
Legend
= Decision Point
= Milestone Decision
= Requirements Document
= Requirements Authority Review

** Or Equivalent Approved/Validated Requirements Document.*

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

Cyber Survivability Framework Integration



Cyber Survivability Endorsement

NIST Cybersecurity Framework

- Identify
- Protect
- Detect
- Respond
- Recover

JCIDS System Survivability KPP

- Prevent
- Mitigate
- Recover

Leveraging and Aligning

Risk Management Framework

- Prepare
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

DoDI 8500 and 8510

Cyber Threat Intelligence

- Defense Intel Threat Libraries (DITL)
- Validated On-Line Threat (VOLT)
- Critical Intelligence Parameters (CIP)
- Commercial Assessment

Risk Managed, Measurable, Testable and Implementable Cybersecurity Requirements …

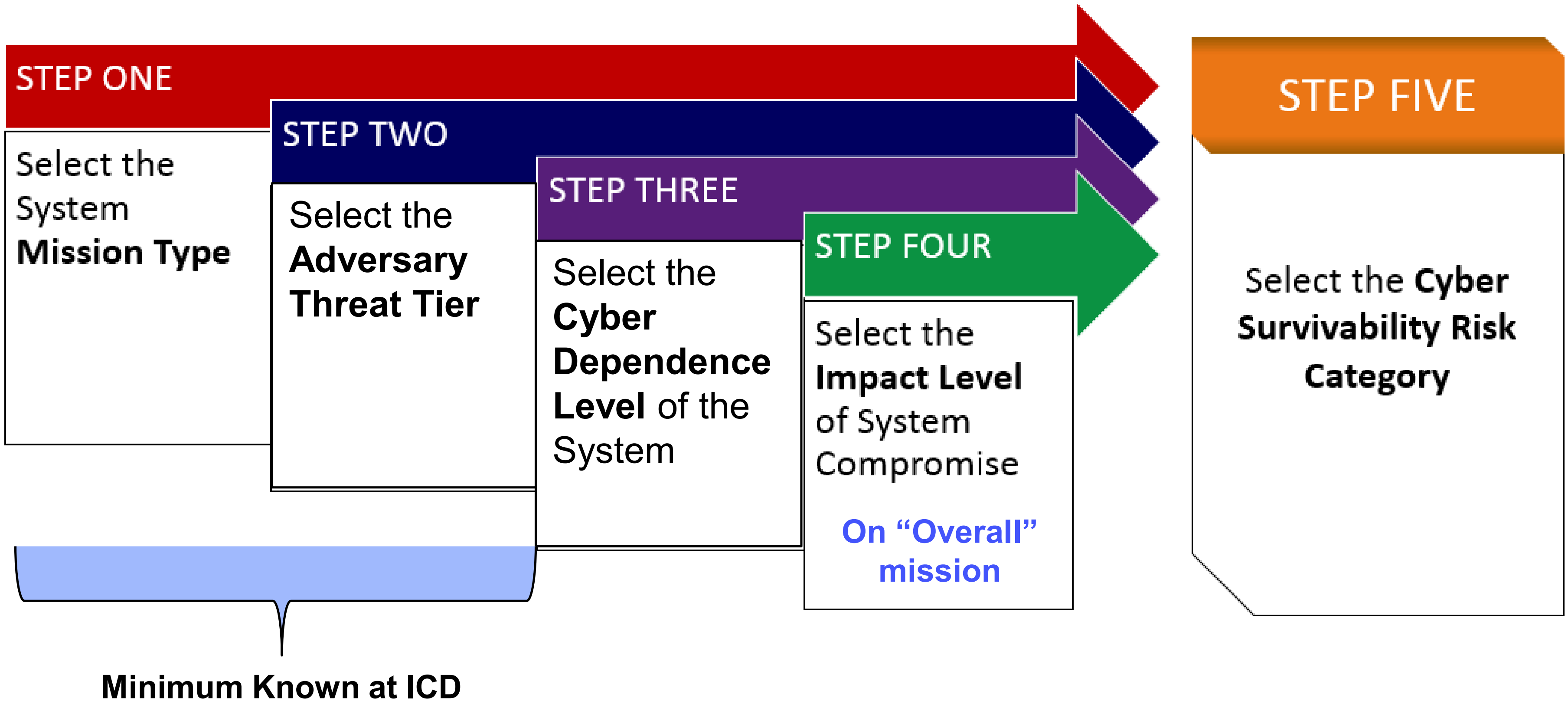
Driving Source Selection Criteria and Supporting RMF Technical Controls

Cyber Survivability Attributes (CSAs) and the RMF

- **CSE Leverages the ~800 NIST 800-53 Cybersecurity Technical Controls**
  - CSE is the onramp to and supports the Risk Management Framework (RMF)
  - CSE's 10 CSAs can be traced directly to the 17 Control Families
  - CSE's 10 CSAs articulate the measurable and testable cyber survivability requirements and are supported by the NIST Cybersecurity Technical Controls
- **Identified 239 NIST Controls Potentially Applicable to Weapon Systems**
  - 98 Highly Applicable
  - 86 Somewhat Applicable
  - 55 Require Interpretation
- **CSE Implementation Guide - Volumes 2 and 3:** OSD-CIO's Vol 2 and NSA-IAD Vol 3 will provide additional detail the Acquisition and Test communities can use to tailor and test recommended cybersecurity technical controls associated with applicable CSAs.
- **Cyber Survivability Risk Category (CSRC):** The level of cyber hardening acquired, tested and implemented is directly related to and consistent with the system's CSRC.

Leveraging and linking the CSAs to the NIST 800-53 cybersecurity technical controls, enables an easier understanding and implementation by cybersecurity professionals, but also articulates a mission focused requirement to support operational risk tradespace decisions.

5 STEP: *Risk Managed Approach*



STEP ONE

Select the System **Mission Type**

STEP TWO

Select the **Adversary Threat Tier**

STEP THREE

Select the **Cyber Dependence Level** of the System

STEP FOUR

Select the **Impact Level** of System Compromise

On "Overall" mission

STEP FIVE

Select the **Cyber Survivability Risk Category**

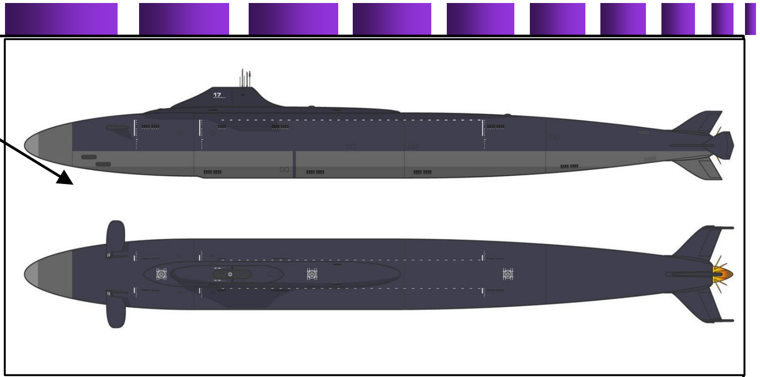
Minimum Known at ICD

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

STEP 1: *System Mission Types*

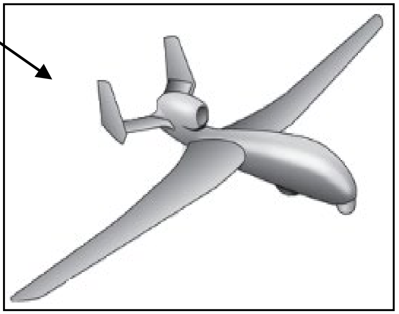
MT 4 – Strategic / National – Deterrence

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



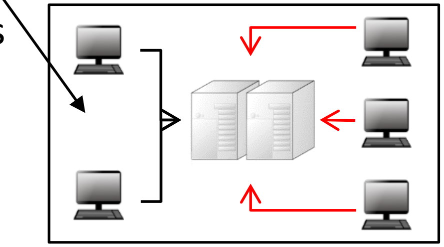
MT 3 – Operational / Tactical – 1st 72 hrs

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



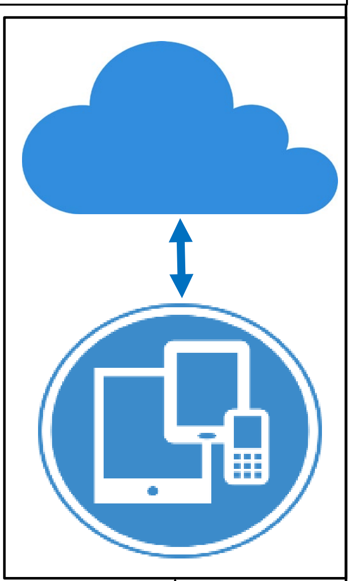
MT 2 – Mission Support – After 1st 72 hrs

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 environment.



MT 1 – Organizational Support

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



Determining the System Mission Type helps define the required level of cyber survivability protections for the capability

STEP 2: *Adversary Threat*

Adversary Threat Tier – Most Likely Greatest Risk

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 use customized malware to conduct wide-ranging intelligence collection operations, gain access to more isolated networks, and in some cases creates 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.

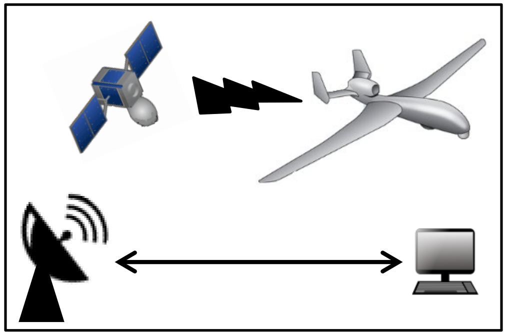
Source: GAO analysis of Department of Defense (DOD) information. | GAO-19-128

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

STEP 3: *Cyber Dependence*

Criticality analysis provides basis for "intrinsic" cyber survivability assessment of critical functions, components and information exchanges

Determine the Mission Critical Functions of the System



Move: Sustain Flight / Maneuverability

Shoot: Perform Offensive / Defensive Activities

Communicate: Maintain Internal/External Comm

Degree of connectivity (based on operational requirements), and Technical exposure (origin, export, open sys arch) combine to define the system's cyber dependency

STEP 3: *Cyber Dependency*

Level	**Degree of Connectivity** (Operational Requirements for Internal and External Information Exchange)	Technical Exposure
CDL 4	**Extreme** - Systems are entirely dependent on cyber connectivity and functionality, and may not function at all without full high bandwidth network support (both wired and wireless). Ex. Continuous comm over minimally protected networks or complex SW/HW, with no human to take control in Unmanned and Robotic/Autonomous Systems.	**Broad**
CDL 3	**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 (both wired and wireless).	**Limited**
CDL 2	**Moderate** - Systems are somewhat dependent on cyber connectivity and functionality, and can operate effectively with intermittent or low bandwidth network support (both wired and wireless).	**Restricted**
CDL 1	**Low** - Systems have little dependence on cyber connectivity and functionality, and can operate effectively with little or no network support.	**Narrow**

Cyber Dependence, based upon the "Intrinsic" Cyber Survivability Risks Associated with Performing its Mission Critical Functions of Move, Shoot and Communicate

STEP 4: "Overall" *Mission Impact*

Impact Level (IL) of System Loss/Compromise

<u>IL 4: Catastrophic Adverse Effect</u> – 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.

<u>IL 3: Serious Adverse Effect</u> – A compromise of system confidentiality, integrity, and availability would seriously degrade mission performance leaving some mission objectives unaccomplished and endangering friendly forces.

<u>IL 2: Limited Adverse Effect</u> – 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.

<u>IL 1: Risks Acceptable for Meeting Military and Organization Needs</u> – 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 system's mission impact of compromised "move, shoot, communicate" due to a cyber event … on all its critical functions? <u>AND</u> then what is the "Overall" Mission Impact …

STEP 5: *System Survivability Risk*

Vulnerability in the face of Threat Capability → Survivability Risk

Cyber Survivability Risk Categories (CSRC)

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

Cyber Survivability Risk Category (CSRC) provides consistent understanding of requirements
OPTIONS: High-Water Mark, Balanced Scorecard Adaptation or Delphi Scoring

JCIDS Requirements Document Reviews

- **JS J6 cyberspace Division has reviewed as of 27 December 2018:**
  - **164 JCIDS requirements document reviews in the last 18 months**
    - **50 ICDs**
    - **73 CDDs**
    - **41 CPDs**

Requirements Sponsors						
USAF	USA	USN	USMC	Joint Staff	COCOMs	Other
48	32	21	8	19	26	10

  - **Reviews represent 106 different systems from information systems to aircraft to biological agent detection systems**
  - **No instances of CSE non-applicable systems**
  - **Staff has regular direct coordination with PEOs, PMs, Command sponsors and program cybersecurity personnel to support CSE language development**

CSE-IG being updated in Nov 2018 – lesson learned updates and clarification. Test community has stated proposed exemplars are now measurable and testable

JCIDS Requirements Document Reviews

- **What level of cyber actor must the system be capable of withstanding if it is to fulfill its warfighting purposes?**
  - ATT 4 – Advanced
  - **ATT 3 – Moderate**
  - ATT 2 – Limited
  - ATT 1 – Nascent

- **Most system requirements reviewed under JCIDS are CSRC-3 meaning:**
  - The mission criticality and impact of system compromise requires that the capability must survive and operate in a cyber contested environment
  - Threat actors in this risk category range are persistent and well-resourced adversaries at a nation state level.
  - For this CSRC level, the Cyberspace Division recommends requirements' sponsors consider specific CSAs. The CSAs are associated with mandatory SS KPP Pillars: Prevent, Mitigate and Recover.

Weapon Systems with Joint Interest are likely to be CSRC-3 with an ATT-3

Proposed update, based on GAO Report

"CSRC 3" Exemplar:

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

The systems' mission criticality and impact of system compromise requires the capability must survive and operate in a 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 counter vulnerabilities at tactically relevant speeds. Cyber Survivability Attributes, which must be assessed for each AoA alternative and tailored for system-specific architectures are:

Puts Cyber Survivability requirement in context by *incorporating a high level "projected cyber threat"* … before an Analysis of Alternatives can drive detailed cyber threat assessment

Proposed update, based on GAO Report

UNCLASSIFIED

"CSRC 4" Exemplar:

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

The systems' mission criticality and impact of system compromise requires the capability must survive and operate in the highest cyber-contested environment against the span of anticipated adversaries ranging from amateurs to the most sophisticated, persistent, and extremely well-resourced adversaries at an advanced nation state level. Adversaries are capable of the highest level of cyber tradecraft using publicly available and customized tools to exploit known and unknown vulnerabilities, as well as the ability to develop and deploy sophisticated/stealthy malware/vulnerabilities to conduct complex/long-term cyber operations that combine multiple intelligence sources to obtain access for identifying/targeting espionage/attack on both unencrypted and isolated high-value networks, and may develop detailed technical and system knowledge of the target system to deploy more damaging cyber attacks. Recognizing the adversaries' current/projected cyber threat capabilities, the system must implement the best available countermeasures to prevent/mitigate the effects of cyber events for maintaining a 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 internal and external information flows; must implement a defense in depth architecture, with no single points of failure; must leverage available DoD developed cyber protections (including protections inherited from the operational environment); and as required build specific custom protections to actively manage the system's configuration to counter vulnerabilities at tactically relevant speeds. Cyber Survivability Attributes, which must be assessed for each AoA alternative and tailored for system-specific architectures are:

Puts Cyber Survivability requirement in context by *incorporating a high level "projected cyber threat"* … before an Analysis of Alternatives can drive detailed cyber threat assessment

Cyber Survivability Attribute (CSA) Exemplars

Prevent - CSAs	Prevent Exemplar Language (threshold & objective statements)
SS KPP Pillar: Prevent **CSA-01: Control Access**	"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) and must withstand cyber-attack Tactics, Techniques and Procedures (TTPs) of an ATT-xx (specified by sponsor). 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."
SS KPP Pillar: Prevent **CSA-02: Reduce System's Cyber Detectability**	"System survivability requires that signaling and communications (both wired and wireless) do not enable an adversary to monitor and/or target system and/or supported DoD weapon systems through its emanations."
SS KPP Pillar: Prevent **CSA-03: Secure Transmissions and Communications**	"System shall protect all transmissions and communications of data 'in transit' commensurate with its confidentiality requirements. System shall only use NSA certified cryptographic devices. System shall prevent unauthorized transmissions/communications, including attempted data exfiltration, from the system to unauthorized person and non-person entities."
SS KPP Pillar: Prevent **CSA-04: Protect System Information from Exploitation**	"System shall protect all data 'at rest' commensurate with its confidentiality 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)."
SS KPP Pillar: Prevent **CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels**	"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."
SS KPP Pillar: Prevent **CSA-06: Minimize and Harden Attack Surfaces**	"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 → Source Selection Criteria & RMF CS Tech Controls

Cyber Survivability Attribute (CSA) Exemplars

Mitigate - CSAs	Mitigate Exemplar Language (threshold & objective statements)
SS KPP Pillar: Mitigate **CSA-07: Baseline and Monitor Systems and Detect Anomalies**	"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 = (# of seconds/minutes [specified by sponsor]) and O = (# of seconds/minutes [specified by sponsor])."
SS KPP Pillar: Mitigate **CSA-08: Manage System Performance if Degraded by Cyber Events**	"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 - CSAs	Recover Exemplar Language (threshold & objective statements)
SS KPP Pillar: Recover **CSA-09: Recover System Capabilities**	"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 (timeline specified by sponsor and consistent with mission needs), in order to fight another day. System recovery shall prioritize critical functions (specified by sponsor)."
SS KPP Pillar: Recover ★ **CSA-10: Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds**	"Throughout the system's lifecycle and within one standard mission cycle of xx hours of notification for operational systems and xx days for systems in development (specified by sponsor), the system shall have a configuration management process supported by automated capabilities to maintain a defined cybersecurity baseline, by authenticating, approving, deploying and verifying the success of cybersecurity configuration changes (including patches and software updates) to mitigate high priority threats on local and remote components, as well as validate that cybersecurity baselines have not been altered."

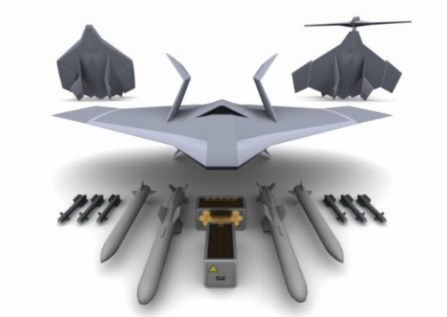
Fundamental CSE construct: sponsor selects subset of CSAs most critical to achieve each SS KKP Pillar … Min of 1 per Pillar, but historically → CSRC-4 (9-10), CSRC-3 (6-8), CSRC-2 (4-6)

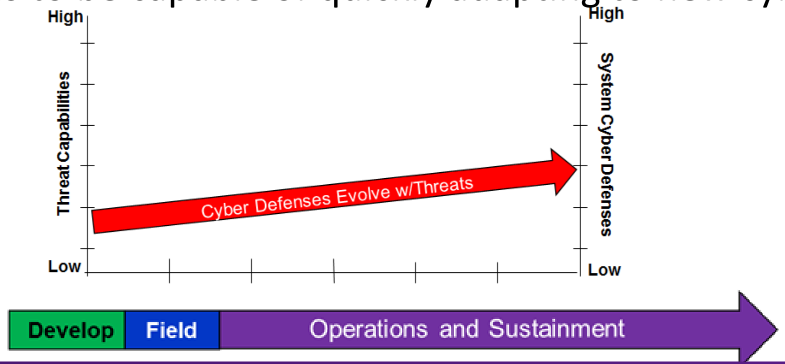
CSA-10's Cultural Shift - Adapt to Cyber Risks

CSA-10 Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds

"Throughout the system's lifecycle and within one standard mission cycle of xx hours of notification for operational systems and xx days for systems in development (specified by sponsor), the system will have a configuration management process supported by automated capabilities to maintain a defined cyber secure baseline, by authenticating, approving, deploying and verifying the success of cybersecurity configuration changes (including patches and software updates) to mitigate high priority threats on local and remote components, as well as validate that cybersecurity baselines have not been altered."

- Weapon systems are becoming more cyber dependent … while adversary threats are increasing
- The current 6-18+ month process to identify new vulnerabilities, prioritize risk mitigation options, acquire funding and implement risk reductions increases operational risk
- Resources must be allocated for systems to be capable of quickly adapting to new cyber threats





On the 1st day a system is fielded, there is a known level of risk being accepted … which starts requirement to actively prioritize/buy-down the highest "mission" risks

What we think we need from Testing

- **Shared Calendar:**
  - https://intelshare.intelink.gov/sites/atlcoi/cyberTableTops/SitePages/Home.aspx
- **Standard Assessment Levels**
  - Assessment Level 4 - Cyber Survivability Risk Category 4: Builds upon the Level 3 assessment to add non-public and mission specific vulnerabilities generally considered only available to the most sophisticated Adversary Threat Tier (ATT) 4 level actors.
    - Compliance: Security Controls Assessment for RMF, which could include a Cyber Tabletop to validate cybersecurity and interoperability standards.
    - System Cyber Survivability: JCIDS SS KPP with CSE, and Developmental Testing, source selection criteria, decompose to technical controls.
    - System and System of Systems Operational Resilience:
    - Mission Based Cyber Risk Assessment:
      - Includes a mission assurance assessment depending upon criticality of the supported infrastructure.
      - Includes a Red Team MDV A, augmented by weapon systems engineers to determine how an "evil genius" could exploit a cyber threat vector to subvert the weapon system or its subsystems through a sequence of compromises. It requires more time, effort and resources than a Level 3 assessment. It is a holistic assessment of the specific system, system of systems and operational infrastructure to determine if an adversary's indirect exploit could cause mission degradation or failure

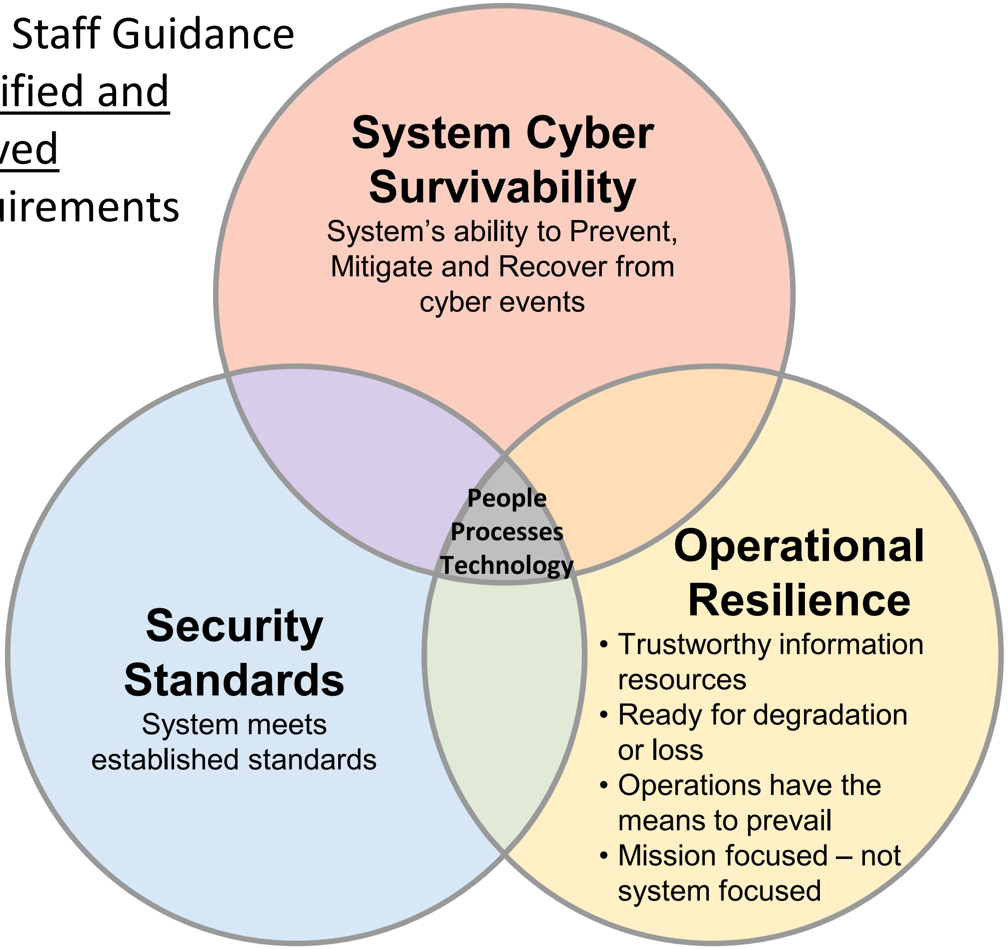
There are a lot of things we should be doing. Need to map path using CSA-7, CSA-8 maintain a CSRP and CSA-10 to prioritize/buy-down the highest “mission” risks

Three Types of Requirements to Test!

Joint Staff Guidance Specified and Derived Requirements

DoDI 8510.01 Specified Requirements

DoDI 8500.01 Implied Requirements



System Cyber Survivability

System's ability to Prevent, Mitigate and Recover from cyber events

Security Standards

System meets established standards

Operational Resilience

- Trustworthy information resources
- Ready for degradation or loss
- Operations have the means to prevent
- Mission focused – not system focused

Cybersecurity T&E Crosses All Aspects Of T&E From The Perspective Of The Threat

CYBERSECURITY TESTING

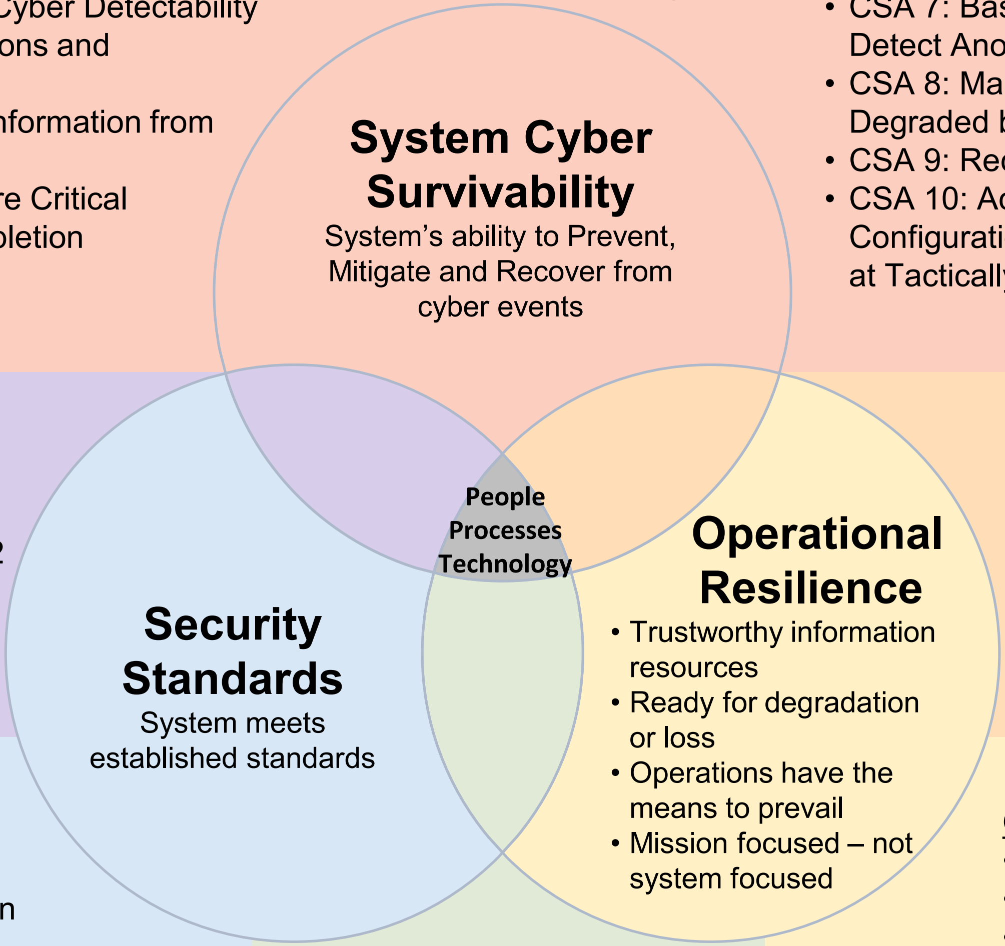
Performance: Cyber Survivability Attribute (CSA)

- CSA 1: Control Access
- CSA 2: Reduce System's Cyber Detectability
- CSA 3: Secure Transmissions and Communications
- CSA 4: Protect System's Information from Exploitation
- CSA 5: Partition and Ensure Critical Functions at Mission Completion Performance Levels

PHASE 3 & 4 Testing

Performance (continued):

- CSA 6: Minimize/Harden Attack Surfaces
- CSA 7: Baseline & Monitor Systems and Detect Anomalies
- CSA 8: Manage System Performance if Degraded by Cyber Events
- CSA 9: Recover System Capabilities
- CSA 10: Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds



System Cyber Survivability

System's ability to Prevent, Mitigate and Recover from cyber events

People
Processes
Technology

Operational Resilience

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

Security Standards

System meets established standards

PHASE 3 & 4 Testing

- Interoperability Standards
- Cyberspace Defense IAW DODI 8530.01 & ESM v9.2
  - (I)PDRR

PHASE 3 & 4 Testing

- Interoperability Standards
- Cyberspace Defense IAW DODI 8530.01 & ESM v9.2
  - (I)PDRR

PHASE 3 Testing

- RMF
- Interoperability Standards
  - NR KPP Certification
- COMSEC
- TEMPEST Certification
- NSA Certification
- STIG Compliance/ SRGs
- Configuration Guides
- Workforce Requirements
- Secure Code Design Standards

PHASE 3 & 4 Testing

- Interoperability Standards
- Cyberspace Defense IAW DODI 8530.01 & ESM v9.2
  - (I)PDRR

PHASE 4 Testing

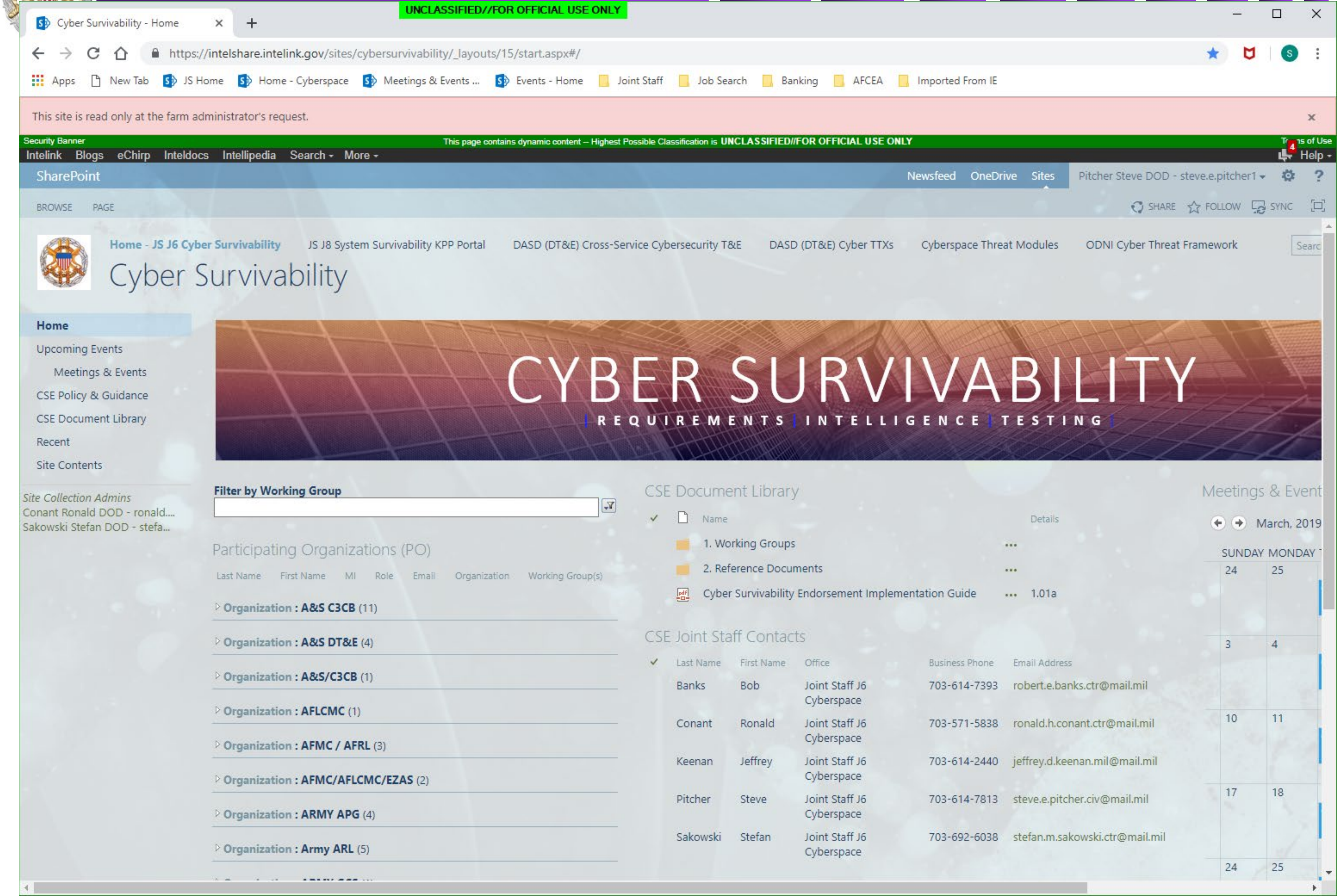
Operational Resilience:

- PDRR
- COOP
- Preserve TRANSEC
- Use of Automation
- Incident Response

JCIDS Prevent, Mitigate and Recover directly translates to (I)PDRR = Identify, Protect, Detect, React, and Restore
Underlined areas addressed as policy under DODI 8500.01

NIPR -- https://intelshare.intelink.gov/sites/cybersurvivability/

SIPR -- https://intelshare.intelink.sgov.gov/sites/cybersurvivability/



This site is read only at the farm administrator's request.

This page contains dynamic content – Highest Possible Classification is UNCLASSIFIED//FOR OFFICIAL USE ONLY

Cyber Survivability

Site Collection Admins
Conant Ronald DOD - ronald....
Sakowski Stefan DOD - stefa...

Filter by Working Group

Participating Organizations (PO)

Last Name	First Name	MI	Role	Email	Organization	Working Group(s)

- Organization : **A&S C3CB** (11)
- Organization : **A&S DT&E** (4)
- Organization : **A&S/C3CB** (1)
- Organization : **AFLCMC** (1)
- Organization : **AFMC / AFRL** (3)
- Organization : **AFMC/AFLCMC/EZAS** (2)
- Organization : **ARMY APG** (4)
- Organization : **Army ARL** (5)

CSE Document Library

✓	Name		Details
	1. Working Groups	...	
	2. Reference Documents	...	
	Cyber Survivability Endorsement Implementation Guide	...	1.01a

CSE Joint Staff Contacts

Last Name	First Name	Office	Business Phone	Email Address
Banks	Bob	Joint Staff J6 Cyberspace	703-614-7393	robert.e.banks.ctr@mail.mil
Conant	Ronald	Joint Staff J6 Cyberspace	703-571-5838	ronald.h.conant.ctr@mail.mil
Keenan	Jeffrey	Joint Staff J6 Cyberspace	703-614-2440	jeffrey.d.keenan.mil@mail.mil
Pitcher	Steve	Joint Staff J6 Cyberspace	703-614-7813	steve.e.pitcher.civ@mail.mil
Sakowski	Stefan	Joint Staff J6 Cyberspace	703-692-6038	stefan.m.sakowski.ctr@mail.mil

Meetings & Event

March, 2019

SUNDAY	MONDAY
24	25
3	4
10	11
17	18
24	25

Questions?

J6 – Cyber Survivability

Mr. Steve Pitcher, GS-15, CISSP
JS Senior Cyber Survivability Analyst
(Steve.E.Pitcher.civ@mail.mil)

CAPT George D. Davis III,
Chief, JS Cybersecurity Branch
(George.D.Davis8.mil@mail.mil)

Col Oscar "Oz" Delgado,
Chief, JS Cyberspace Division
(Oscar.Delgado3.mil@mail.mil)

CSE Backup Slides

x

What we "think" we need - *Adversary Threat*

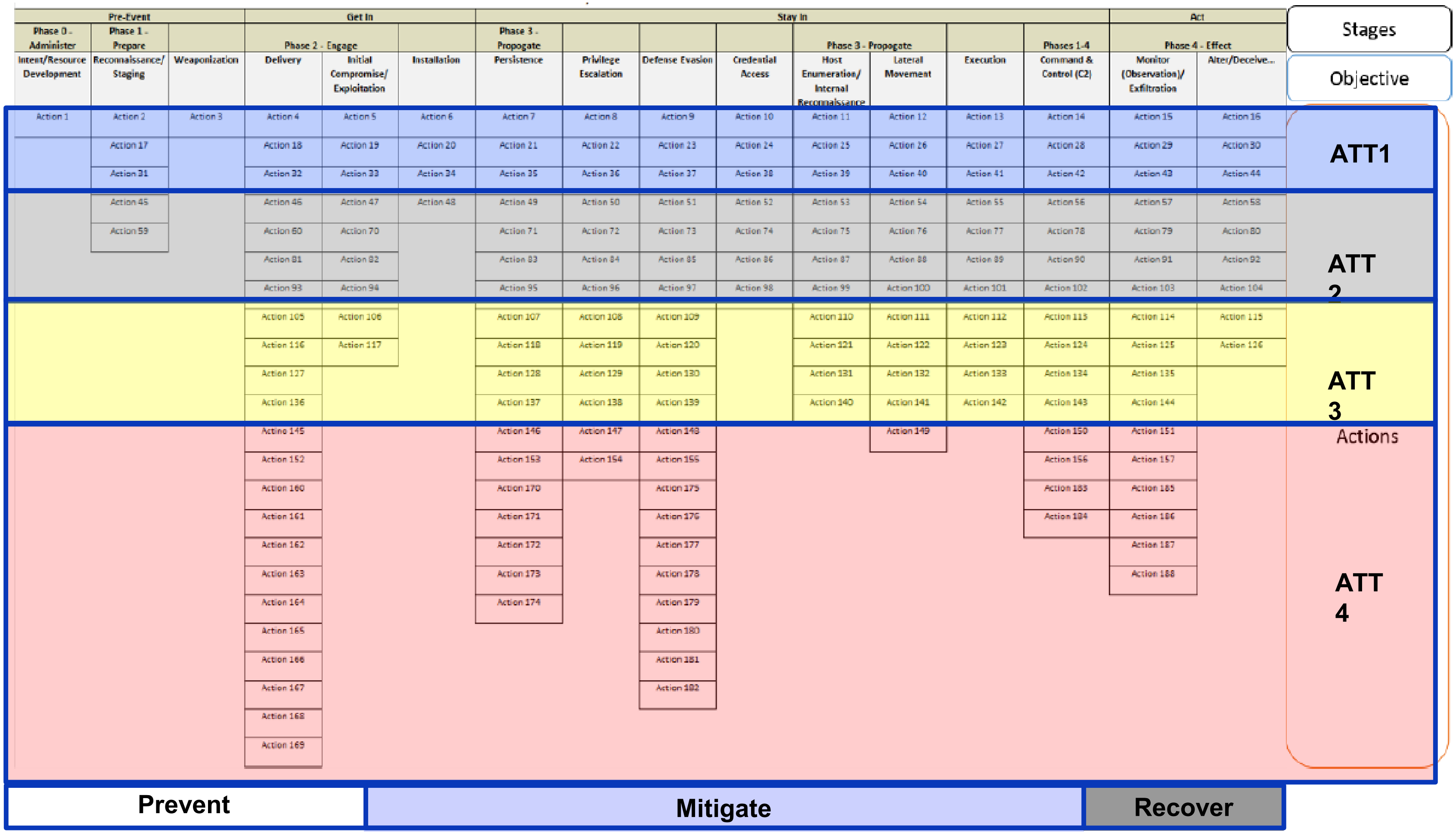
- **Help define "demand signals" for IC to differentiate ATT capabilities**
  - – Operational community doesn't know all of what IC can provide…
  - – Intelligence community doesn't understand all that we need…
  - – 50-80% solution … list things to be considered and who can help tailor
- **Help us improve CSE IG and Intel/Threat support to acquisition, by capturing and building upon what is already being done…**
  - – Standardize ATT Taxonomy/Criteria/Capability and CSRC exemplars
    - – Develop classified versions of ATT mapping and CSRC exemplars (Annex)
  - – Recommend changes to the intelligence cyber threat assessment reports (DITL, VOLT, DoDCAR and MITRE ATTACK) to provide an Integrated Adversary Capabilities Framework → actionable cyber threat info
  - – Help define drivers to enable RMF and PPP to be effective
  - – Help define a set of generic Cyber CIP exemplars for consideration
    - – Breach of WS CDC or sub, with exfil of design/arch info
    - – Breach of WS or cyber component
    - – Identification of known counterfeit HW/SW in WS supply chain
    - – Increase in adversary capability: increasing risk to accepted WS vulnerabilities, or identifying risk or new vulnerability risk driving update to mitigation prioritization

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

UNCLASSIFIED

DoDCAR with NOTIONAL Overlay of the SS KPP Prevent, Mitigate and Recover Pillars and CSE Adversary Threat Tiers (ATT)

Figure 3: DODCAR Technical Architecture and the Cyber Threat Framework's High-Level View



Pre-Event			Get In			Stay In								Act		Stages
Phase 0 - Administer	Phase 1 - Prepare		Phase 2 - Engage			Phase 3 - Propogate				Phase 3 - Propogate			Phases 1-4	Phase 4 - Effect		
Intent/Resource Development	Reconnaissance/ Staging	Weaponization	Delivery	Initial Compromise/ Exploitation	Installation	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration/ Internal Reconnaissance	Lateral Movement	Execution	Command & Control (C2)	Monitor (Observation)/ Exfiltration	Alter/Deceive...	Objective
Action 1	Action 2	Action 3	Action 4	Action 5	Action 6	Action 7	Action 8	Action 9	Action 10	Action 11	Action 12	Action 13	Action 14	Action 15	Action 16	ATT1
	Action 17		Action 18	Action 19	Action 20	Action 21	Action 22	Action 23	Action 24	Action 25	Action 26	Action 27	Action 28	Action 29	Action 30	
	Action 31		Action 32	Action 33	Action 34	Action 35	Action 36	Action 37	Action 38	Action 39	Action 40	Action 41	Action 42	Action 43	Action 44	
	Action 45		Action 46	Action 47	Action 48	Action 49	Action 50	Action 51	Action 52	Action 53	Action 54	Action 55	Action 56	Action 57	Action 58	ATT 2
	Action 59		Action 60	Action 70		Action 71	Action 72	Action 73	Action 74	Action 75	Action 76	Action 77	Action 78	Action 79	Action 80	
			Action 81	Action 82		Action 83	Action 84	Action 85	Action 86	Action 87	Action 88	Action 89	Action 90	Action 91	Action 92	
			Action 93	Action 94		Action 95	Action 96	Action 97	Action 98	Action 99	Action 100	Action 101	Action 102	Action 103	Action 104	
			Action 105	Action 106		Action 107	Action 108	Action 109		Action 110	Action 111	Action 112	Action 113	Action 114	Action 115	ATT 3
			Action 116	Action 117		Action 118	Action 119	Action 120		Action 121	Action 122	Action 123	Action 124	Action 125	Action 126	
			Action 127			Action 128	Action 129	Action 130		Action 131	Action 132	Action 133	Action 134	Action 135		
			Action 136			Action 137	Action 138	Action 139		Action 140	Action 141	Action 142	Action 143	Action 144		
			Actino 145			Action 146	Action 147	Action 148			Action 149		Action 150	Action 151		Actions
			Action 152			Action 153	Action 154	Action 155					Action 156	Action 157		
			Action 160			Action 170		Action 175					Action 183	Action 185		
			Action 161			Action 171		Action 176					Action 184	Action 186		
			Action 162			Action 172		Action 177						Action 187		
			Action 163			Action 173		Action 178						Action 188		ATT 4
			Action 164			Action 174		Action 179								
			Action 165					Action 180								
			Action 166					Action 181								
			Action 167					Action 182								
			Action 168													
			Action 169													

Prevent	Mitigate	Recover

How do we define "demand signals" to the IC to differentiate ATT capabilities

UNCLASSIFIED