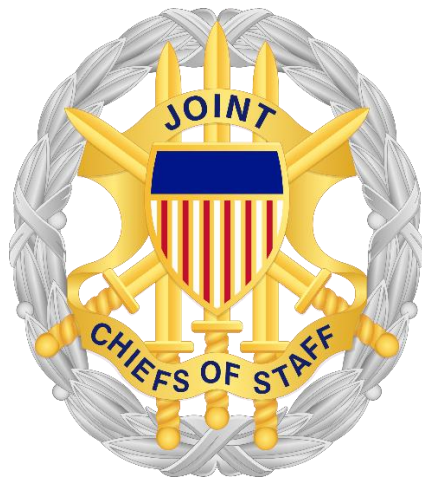


# Cyber Survivability Endorsement (CSE) Implementation Guide



**Version 3.0**  
**July 2022**

## **Joint Staff J6, Deputy Director for Information Warfare Requirements Division**

**Classification Determination:** This CSE Implementation Guide is UNCLASSIFIED. All specific vulnerability and threat references were taken from unclassified sources. Its guidance is generic, scenarios are notional, and exemplar language is intended to be tailored for each system. It does not include any specific information on any system, which would likely drive a CUI or classified determination, as would tailoring the exemplar language to describe threshold performance requirements for a specific DoD capability.

**Releasability:** This guide has been cleared for public release by the Office of the Chairman of the Joint Chiefs of Staff Public Affairs Office.

**UNCLASSIFIED**

INTENTIONALLY LEFT BLANK

**UNCLASSIFIED**

## Table of Contents

|  |    |
|--|----|
| <b>Summary of Changes</b> .....  | 5  |
| 1.0 Executive Summary .....  | 7  |
| 2.0 Intended Audience .....  | 9  |
| 3.0 Introduction .....   | 10 |
| 4.0 Background .....   | 14 |
| 5.0 Using CSE to Determine the Level of Cyber Sufficiency Throughout a Capability’s Lifecycle..... | 22 |
| 6.0 CSE in Alternative Acquisition Pathways .....  | 27 |
| 7.0 Overview of the Cyber Survivability Endorsement Process.....                                   | 30 |
| 8.0 Implementing the Cyber Survivability Endorsement Process.....                                  | 31 |
| 8.1 Step 1 –Mission Type (MT) .....  | 31 |
| 8.2 Step 2 – Adversary Threat Tier (ATT) .....   | 32 |
| 8.3 Step 3 – Cyber Dependency Level (CDL).....   | 34 |
| 8.4 Step 4 – Impact Level of System Loss or Compromise (IL) .....                                  | 38 |
| 8.5 Step 5 – Determine the Cyber Survivability Risk Category of the System .....                   | 40 |
| 8.6 – CSA Determination from the CSRC Selection.....   | 42 |
| 9.0 CSE Process Quick Start for Capability Requirement Documents.....                              | 45 |
| 10.0 Cyber Survivability in Capability Requirement Documents .....                                 | 46 |
| 11.0 ICD and CDD Exemplar Language for each Cyber Survivability Risk Category.....                 | 51 |
| 12.0 Cyber Survivability Requirements and Performance Measures .....                               | 62 |
| 13.0 Tailoring Cyber Survivability Attributes.....   | 63 |
| 14.0 CSE Support to Other DoD Initiatives .....  | 67 |
| 15.0 CSE Vignette.....   | 70 |
| 16.0 Joint Staff Gatekeeping .....   | 77 |
| 17.0 Annotated References.....   | 79 |
| 18.0 Acronyms .....  | 83 |
| 19.0 Glossary .....  | 87 |

**List of Figures:**

Figure 1: Integrated Cybersecurity Frameworks Leveraged by CSE .....15

Figure 2: Interactions of the JCIDS and Major Capability Acquisition Process .....19

Figure 3: The JCIDS SS KPP and CSE in All Capability Acquisition Processes .....19

Figure 4: Cyber Survivability Risk Category Determination.....28

Figure 5: Mission Types .....31

Figure 6: Adversary Threat Tiers.....30

Figure 7: Unclassified Adversary Cyber Threat Advisories .....31

Figure 8: Cyber Criticality Analysis .....32

Figure 9: Cyber Dependency Levels .....35

Figure 10: Degree of Connectivity and Operational Requirements.....36

Figure 11: Impact Levels and Criticality Analysis using CNSSI No 1253 Security Categorization .....36

Figure 12: Impact Levels of System Compromise .....39

Figure 13 Determining the Cyber Survivability Risk Category .....38

Figure 14: Cyber Survivability Risk Categories.....41

**List of Tables:**

Table 1: System Survivability KPP Pillars Mapped to Cyber Survivability Attributes .....43

Table 2: CSE Iterative Approach in Capability Requirement Documents .....46

Table 3: Vignette CDD Table .....73

## Summary of Changes

**Background:** Since the Cyber Survivability Endorsement (CSE) Implementation Guide (CSEIG) was first published in January 2017, the Joint Staff has reviewed over 340 Joint Capabilities Integration and Development System (JCIDS) requirements documents for cyber survivability in support of the JCIDS System Survivability Key Performance Parameter (SS KPP). These reviews included over 200 unique systems, encompassing mission critical systems and sea/land/air/space capabilities. The Joint Staff used lessons learned from these reviews to coordinate and align cyber survivability threshold performance requirement guidance, along with other DoD efforts to improve the cybersecurity and cyber resiliency of DoD weapon systems throughout their lifecycles. Over 80 DoD subject matter experts helped to define cyber survivability requirement exemplars, enabling a consistent understanding and expectation of the minimum viable levels of cyber survivability needed to support acquisition, engineering, testing, operation and risk acceptance decisions throughout a systems lifecycle.

**Way ahead:** CSE threshold performance requirements are referenced in DoD guidance, but a transition from a cybersecurity compliance mindset to cyber survivability focused deliverables will require a concerted effort to fully and formally coordinate all DoD cyber guidance roles and responsibilities. CSE starts with tailoring Initial Capabilities Document (ICD) and Capability Development Document (CDD) exemplar language for the Cyber Survivability Risk Category (CSRC) and Cyber Survivability Attributes (CSA), but program sponsors will need to continue to develop and mature Cyber Survivability Risk Posture (CSRP) metrics to improve the mission assurance of systems in any acquisition pathway. CSE is particularly well suited to rapid acquisition and should influence risk decisions throughout a systems lifecycle, including fielded mission critical systems in sustainment. Over the next two years, the Department is pursuing several initiatives to better integrate CSE's holistic framework of threshold performance requirements into DoD's cybersecurity risk management, acquisition, system security engineering, mission assurance, and testing processes. The initiatives include pilots to integrate OSD and Service efforts for defining consistent processes for determining a measurable and testable CSRP, which are expected to drive the next CSEIG version 4 updates.

### CSEIG version 3.0's most significant changes:

- Expanded Adversary Threat Tiers (ATT) and CSRC summary statements to 5 levels, based on 2021 unclassified Cybersecurity Advisories' nation-specific capabilities and countermeasures from the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and Department of Justice (DOJ). These changes also drive inputs to JCIDS requirement documents' Threat Summary, with an unclassified cyber threat prior to availability of a Validated Online Lifecycle Threat (VOLT) report.
- Expanded Mission Type (MT), Cyber Dependency Level (CDL) and Impact Level (IL) statements to better differentiate levels. A CSRC and CDL of zero were added for capabilities with no hardware (HW), software (SW) or firmware (FW) processing, sensors, or information exchange requirements.
- Included references to updated DoD, Service, Agency and National Institute of Standards and Technologies (NIST) guidance that have incorporated the CSE framework and helped align JCIDS, DoD instructions, and NIST definitions for cybersecurity, cyber resiliency, and cyber survivability.
- Updated CSA-07 to include a recommendation to implement and maintain a cyber survivability configuration baseline for its Government Off The Shelf (GOTS)/ Commercial Off The Shelf (COTS) HW, SW, FW and open source modules, by version number to ensure an operationally acceptable cyber risk posture 24/7. It also introduces the reporting considerations for its mission relevant terrain in cyberspace (MRT-C).
- Updated CSA-10 to include recommendation to consider a developer requirement to provide a machine-readable Bill of Materials (BOM) of the system's GOTS/COTS HW, SW, FW and open source modules for a

supply chain risk assessment prior to each milestone decision and supported release. It includes operator, defender and analyst inputs to enable cyber sufficiency risk assessments, and risk mitigation POA&Ms.

- Added how requirements for Artificial Intelligence, (AI), Machine Learning (ML), and unmanned systems could drive an early CDL determination for an ICD and consideration in its Analysis of Alternatives (AoA).

**CSE framework should lay the foundation for follow-on cyber risk posture activities:** This CSEIG also includes additional information on how cyber threshold performance requirements can enable the following activities (see Section 5.0 for details):

- ICD's CSRC summary statement and list of CSAs to be considered should drive the AoA study team guidance, and the Request for Information (RFIs) needed to differentiate cyber resource and mission risk implications between candidate capabilities and prevent pursuit of capabilities so flawed it would be inconceivable to cost-effectively mitigate known cyber risk to an operationally acceptable level.
- CDD's CSRC summary statement and subset of CSAs identified as most critical to system survivability should drive development of the Request for Proposal (RFP) and source selection criteria, helping prevent acquisition of foundationally flawed capabilities.
- Program Managers (PM) should use the CDD's subset of CSA threshold performance requirements to support operational risk trade-space decisions, selection, testing and effective implementation of Risk Management Framework (RMF) controls associated with the CSAs most critical to system survivability.
- System Security Engineers (SSE) should decompose the CDD's subset of CSA threshold performance requirements into specific minimum viable cybersecurity and cyber resiliency requirements.
- Program Management Offices (PMOs) and Developmental Test (DT) organizations should use the missions, threats, and CSA threshold performance requirements to plan to execute cyber T&E events, including developer/contractor testing, in the Test and Evaluation Master Plan or other document.
- Milestone Decision Authorities (MDA) should use cyber sufficiency status updates, from the developmental testing associated with the CSA threshold performance requirements, to determine if the program is on a path to achieve an operationally acceptable risk posture.
- Authorizing Officials (AO) should use cyber sufficiency status updates, from developmental testing associated with the CSA threshold performance requirements, to determine if the program has or could reasonably be expected to achieve an operationally acceptable risk posture, as part of the decision to grant an Authorization To Operate (ATO).
- CSE's CSRC and CSA threshold performance requirements should be leveraged to ensure an alignment with, and support to, Alternate Acquisition Pathways, RMF, Program Protection Plan (PPP) and related requirements critical to achieving and maintaining an operationally relevant cyber survivability risk posture for Combatant Commanders' Operational Plan (OPLAN) and mission success.
- CSE's framework of CSRC and holistic CSAs should enable a scalable governance and metric construct for a consistent assessment of cyber risk for DoD Congressional reviews and reporting requirements, such as Strategic Cybersecurity Program (SCP) reviews, other data reporting requirements related to the DoD CIO Top 10 Scorecard, Acquisition Milestone cyber sufficiency reviews, Developmental Test/Operational Test reports, Deep Cyber Resiliency Assessments (DCRAs), et al.

The Joint Staff J6 has a cyber survivability portal with links to CSE Frequently Asked Questions (FAQ), DoD initiatives, and related reference material that are helping to align cybersecurity and cyber resiliency with cyber survivability, so every organization can leverage the benefits and avoid unintended duplication from each other's efforts: <https://intelshare.intelink.gov/sites/cybersurvivability/>

## 1.0 Executive Summary

In 2015, the Deputy Secretary of Defense tasked the Joint Staff to improve requirements for weapon systems cybersecurity, which resulted in adding a Cyber Survivability Endorsement (CSE) to the Joint Capabilities Integration and Development System (JCIDS) Manual's System Survivability Key Performance Parameter (SS KPP).

The tasking was driven by the 2015 Director of Operations Test & Evaluation (OT&E) annual report highlighting the same high risk vulnerabilities that were being found in almost every tested system, and should have been fixed prior to OT&E. This happened because requirements documents did not include contractually-binding cybersecurity and cyber resiliency threshold performance requirements, and instead relied on compliance with a multitude of DoD, FISMA, NIST and CNSS guidance. Since these legacy systems' only cyber requirement was for enough cybersecurity compliance to obtain an Authorization to Operate (ATO), the OT&E identified recurring cyber risks to individual systems that would require significant reengineering and potentially be too costly to mitigate the risks to an operationally acceptable level. These conclusions foster a re-focus away from solely a system's approach to a more operational mission risk analysis process, and was a driving force for pursuing this CSEIG.

Although the DoD's Risk Management Framework (RMF) is necessary, compliance with it isn't sufficient to achieve and maintain an operationally relevant cyber risk posture. One of the reasons is RMF guidance does not leverage the JCIDS Manual (2018 and 2021) System Survivability KPP guidance on CSE, which holistically adds cyber resiliency considerations critical to mission assurance. JCIDS' addition of CSE has put cybersecurity and cyber resiliency minimum viable requirements on equal footing with all other system performance requirements, during cost, schedule and performance risk trade-space decisions. Program Managers (PMs) can use Cyber Survivability Attribute (CSA) threshold performance requirements to justify (resourcing) specific technical controls from FISMA, NIST and CNSS, but RMF guidance doesn't define how a linkage to the CSAs could be used to support a PM's efforts in pursuit of cyber survivability.

CSE targeted the predictable failure of the cybersecurity processes to build-in sufficiently robust cyber capabilities to prevent (resist/anticipate), mitigate (absorb/withstand), recover from, and adapt to the full spectrum of mission assurance cyber-events in plain language requirements that a program manager can understand. The Services have independently developed System Security Engineering guidance to decompose that plain language into cybersecurity technical controls for fielding survivable capabilities and have develop metrics for testing to define their system's Cyber Survivability Risk Posture (CSRP).

This CSE Implementation Guide (CSEIG) is purposely not prescriptive on how to determine a CSRP, but it has provided information to allow the Services and Agencies to mature their own processes. For example, the OUSD (A&S) Deep Cyber Resiliency assessment (DCRA), Army Cyberspace Operational Resilience Assessment – Platform (CORA-P), Air Force Measures of Performance Report, Air Force System Security Engineering (SSE) Cyber Guidebook version 4, Naval Air System Command's SSE Process Guide, DoD Cybersecurity Test & Evaluation Guidebook version 2, DoD Cyber Table Top Guide version 2, MITRE's use of the Air Force Research Lab's CSA Tool, and System Engineering Research Center's Cyberattack Resilient Systems Report are not sufficient to define a measurable CSRP for the DoD, but they all contribute to the processes for maturing the cyber resiliency, and survivability measurement. Work has begun for CSEIG version 4 to include their best practices. The current concept of the CSRP will continue to mature through

collaboration between OSD, JS, CCMDs, Services and Agencies into a repeatable, measurable and testable process that will yield a uniform CSRP.

CSE does not identify any new cybersecurity requirements. The CSE process helps requirement sponsors better understand the cyber risks to the capability's mission critical functions and performance requirements, in order to state those cybersecurity and cyber resiliency requirements as a reasoned set of cyber survivability threshold performance requirements. These threshold performance requirements are identified early enough in the acquisition process to inform engineering decisions and enable program managers to include them during operational risk trade-space decisions for fielding of a survivable minimum viable capability.

CSE can help requirement sponsors and program managers make defensible operational risk trade-space decisions for those cyber technical controls supporting the subset of CSAs identified as most critical for that system's survivability. Operational forces need systems that meet mission requirements, and are survivable in their respective operating environment. The warfighter deserves cyber survivability, and the CSE framework supports creation of threshold performance requirements that are designed to prevent, mitigate, recover from and adapt to cyber-events, by applying a risk-managed approach to building and maintaining systems.

Even though CSE is only mandatory for requirements going through the JCIDS process, the Services have seen resource and mission risk benefits to justify considering cyber survivability requirements in all acquisition pathways. CSE is particularly well suited to the higher technology readiness levels associated with rapid acquisition. However, if alternative acquisition pathways (such as Middle Tier of Acquisition and Joint Urgent/Emergent Operational Needs) do not effectively consider cyber survivability threshold performance requirements, they are at risk of not providing a survivable operational capability. It is recommended that all programs going through the all acquisition pathways consider, and sufficiently apply, the CSE concepts outlined in this guide in order to field survivable DoD capabilities.

CSE can reduce acquisition and sustainment total lifecycle costs and improve mission assurance. This is counterintuitive, since the cost of implementing cybersecurity into legacy weapon systems has historically been seen as cost-prohibitive. However, those costs were driven by the need to reengineer capabilities that were found to be flawed. When made contractually-binding, CSE's cyber threshold performance requirements have the potential to prevent the acquisition of capabilities that would be too costly to mitigate cyber risks to an operationally acceptable level.



## 2.0 Intended Audience

This SS KPP's CSEIG is primarily intended for requirements/resource sponsors developing an ICD, CDD, Information System ICD (IS-ICD), or IS-CDD that will be used in the JCIDS process. Resource sponsors and program office personnel should also use the CSEIG as a reference in:

- developing AoA study team guidance, including market research planning and RFIs;
- drafting RFP and source selection criteria;
- decomposing CSAs for system security engineering;
- assessing cyber sufficiency status for making milestone decisions;
- drafting developmental/operational test plans;
- drafting cybersecurity strategy and program protection plans;
- defining requirements for adaptive (DevOps) improvements throughout a capability's lifecycle; and
- making risk acceptance decisions.

CSE's non-prescriptive approach can also be used by Combatant Commands (CCMDs), Services, and Agencies to assess the cyber survivability risk posture of OPLANs and missions. The need to assess and mitigate cyber-risks in legacy and future systems is universal, and the CSEIG provides a mission-focused approach and holistic set of cyber survivability requirements that can support achieving and maintaining an operationally-relevant mission risk posture.

Requirements sponsors can seek support from the Joint Staff (J6 and J8), prior to formal capability submission through the Joint Staff's Knowledge Management and Decision Support (KM/DS) system, to help them understand and effectively apply the CSE process. This support is available regardless of the Acquisition Category, level of JCIDS interest, Service responsibility, or acquisition pathway selected. CSE is flexible enough to support non-JCIDS requirements, including all acquisition pathways, including Middle Tier of Acquisition, software development, and using DevOps practices.

### 3.0 Introduction

The CSE framework does not identify any new cybersecurity or cyber resiliency requirements. The CSE process was designed to help requirement sponsors better understand the cyber risks to the capability's functional performance requirements, in order to articulate a reasoned set of cyber survivability threshold performance requirements, early enough in the acquisition process to inform engineering decisions, and support operational risk trade-space decisions for fielding a survivable minimum viable capability.

It helps requirement sponsors identify and tailor the CSAs most critical to system survivability, balance performance tradeoffs, and to assess, achieve, and maintain an operationally-relevant risk posture commensurate with the capability's risk category. The exemplar statements provided in this guide are descriptive, and not prescriptive of specific engineering solutions. They are intended to describe a reasoned set of cyber attributes that can be placed on contract, decomposed and implemented by system security engineers, supported by program managers, and tested throughout the development phase, to ensure an acceptable level of mission assurance in the expected operational environment.

Contrary to popular belief, both acquisition and sustainment lifecycle costs could be reduced in future weapon systems, if cyber survivability is effectively factored into AoA/Capability Based Assessment (CBA), RFP/source selection criteria, and operational risk trade-space decisions throughout the system's lifecycle. This is because early consideration of cyber survivability requirements can prevent the selection of foundationally-flawed technologies and systems that have been rushed to market without incorporating best business practices for risk assessment of cybersecurity and cyber resiliency.

For example, anyone who has purchased the latest personal computer technologies, or first year of a new car redesign, has probably experienced the following:

- Low return on investment: ~30% greater component cost than the previous generation's now-mature capabilities, which could be considered this generation's threshold requirements.
- Software flaws: Down-time and unknown, emergent security risks, until early adopters have identified problems for eventually mitigating/fixing by the manufacturer.
- Buyer's remorse: Wishing they had not prioritized immature technologies (objective requirements), and instead acquired the hardware processing and storage flexibility to add them only when proven to be cost-effective, secure and resilient.

Initial acquisition costs may be lower, lifecycle total cost of ownership may be lower (if cost effective mitigations to achieve an operationally relevant risk posture are included), and mission assurance should be higher, through such an analytic trade-space approach, since functionality will only be acquired when it has proven to be survivable and cost-effective. There would also be less need to remove unacceptably risky functionality, or bolt-on costly and potentially performance-robbing, complex cybersecurity capabilities between it and the rest of the force.

Currently fielded systems have accepted risks and not allocated resources for cyber, because it was cost-prohibitive to add-on or re-engineer needed cyber risk mitigations. However, there are likely some risk mitigations that could still be applied to reduce the operational mission risk to an acceptable level. This is

why the DoD's most mission critical systems should consider resourcing to proactively adapt their capabilities to identify and address evolving cyber-risks by actively managing the system's configuration to achieve and maintain an operationally-relevant cyber survivability risk posture.

This CSEIG contains cyber survivability exemplar statements that should be considered for all capability requirement documents. Starting with the ICD, the CSEIG provides five categories of CSRC-level exemplar language that integrate anticipated adversary cyber threat and countermeasure requirements, even before a capability's specific technologies are known, and before a tailored cyber threat assessment can be made.

The Mission Type (MT) and Adversary Threat Tier (ATT) are the two factors that can almost certainly be determined at the ICD phase (From here, an initial CSRC can be determined). The CSEIG identifies the ten high-level CSAs that requirements sponsors must ensure the AoA study team considers, to ensure that the recommended capability solution is not inherently incapable of being made cyber survivable.

Unless the capability includes requirements for Artificial Intelligence, Machine Learning, continuous information exchange, or unmanned/autonomous control, there will likely not be sufficient information to determine the capability's Cyber Dependence Level (CDL) until after the AoA. After the solution is selected, the CDL and the estimated mission Impact Level (IL) of system loss or compromise can be determined, which will refine the program's CSRC level (CSRC factors are described in detail in section 7). However, the IL determination will not be fully rationalized until the CCMDs, including the assigned cyber defenders, are able to assess its risk implication to their OPLANs and missions. Nevertheless, this incomplete CSRC cyber threat and countermeasure requirements statement can be used until an operationally-relevant cyber threat assessment can be performed, to help identify and tailor an appropriate subset of the ten CSAs to support creation of system-specific, measurable, testable requirements in the draft CDD, IS-ICD or IS-CDD.

CSE and the SS KPP are only required for capabilities going through the JCIDS process, meaning those requirements identified as Joint Requirements Oversight Council (JROC) interest, Joint Capabilities Board (JCB) interest, or as Joint Information. However, its flexible approach can also support acquisition programs that are not subject to the JCIDS process, within the Adaptive Acquisition Framework's other pathways. Services and DoD component sponsors have been encouraged to use this guide, or develop similar guidance, to ensure their programs have an operationally acceptable level of cyber survivability to support mission assurance. The Services have seen the positive implications of applying CSE, and have published acquisition, system engineering and test guidance to support its use.

The CSRC uses a broad operational threat perspective and can help bound the number of CSAs critical to system survivability, since it provides a consistent perspective of the level of cyber survivability required throughout a capability's lifecycle. This consistency enables capabilities to be defined, acquired, engineered, tested, operated, and maintained using the same framework. While all ten CSAs must be considered during the AoA or CBA, the number of CSAs selected for implementation in a capability's development and testing varies by CSRC. The selected subset of CSAs should also support the development of capability requirements, including exemplar statements for the RFP, and for source selection criteria. The CSRC of a capability is also an indicator of the level of Cybersecurity Maturity Model Certification (CMMC)

required for the protection of the Controlled Unclassified Information (CUI) used in developing and testing the capability by Federal contractors.

Selecting more CSAs than necessary for a CSRC level, or not tailoring them to the capability, could lead to unintended costs. The CSA exemplars are system-agnostic and can be used as written, but it is important to perform a criticality analysis to identify and tailor a subset of CSAs most critical to the system's survivability and its move, shoot, and communicate functions. However, tailoring is NOT engineering. CSAs should be kept at a high level to allow developers the flexibility to be creative in meeting the intent of each cyber threshold performance requirement with new technologies and processes.

Although the level of detail in each tailored CSA will be different, the CSAs can be used during development to determine the progress in achieving system's required CSRC level, and during sustainment to determine if it has achieved, and is maintaining, an operationally acceptable risk posture commensurate with its CSRC. Assessing the risk posture requires analyzing the strength and the effectiveness of a system's procedural and technical control implementations to meet the intent of each CSA's threshold performance requirement. The likely operational scenarios for the system's employment are the relevant lenses for viewing its risk category.

Constructing, and regularly reviewing, the system's plan for analyzing, prioritizing, and mitigating mission risks is the means for achieving and maintaining an acceptable risk posture. Together, the CSRC, CSAs, and CSRP provide the foundation for cyber survivability, which can be considered as part of the system's operational risk trade-space, along with other functional requirements.

Assessing and updating a system's risk posture should ideally be done several times a year during its development phase, prior to any version update or sprint release, and in response to increasing cyber adversary capabilities or intent. It should also be done during its operational phase, and reported to the operational chain of command. This guide is intended to support the incorporation of a CSRP as one aspect of a system's risk posture. System survivability assessments, and mitigation plans to prioritize vulnerabilities with the greatest mission risk, are responsibilities of both the capability owners and the senior echelon officials, as part of their implicit duty to field effective and survivable military capabilities. If they are not survivable, then they have little operational relevance in a cyber-contested environment.

As will be shown in this guide, CSA-10 is the most critical attribute, due to:

- a system's evolving and potentially expanding cyber-attack surface;
- constantly increasing adversary cyber capabilities;
- complexity of identifying vulnerability risks from connected and supporting systems; and
- the requirement to assess and prioritize mitigation of vulnerabilities with the greatest mission risk.

Although CSA-10 was designed to improve and maintain the risk posture of future capabilities, it should be considered for implementation by the DoD's most mission critical legacy capabilities. No matter what risks were accepted by an Authorizing Official (AO) on day 1 of a new ATO, the use of CSA-10 will enable agile changes to systems in response to evolving threats and missions, making risk assessment and acceptance more adaptive to operational needs.

The resources required to support efforts associated with CSA-10 are not a management reserve. There is always a known list of cybersecurity and cyber resiliency risks that need to be assessed, prioritized and mitigated, since there are no 100% RMF-compliant ATOs. A signed ATO does not negate the residual risk being accepted or imply an operationally acceptable cybersecurity or cyber resiliency risk posture. In addition, new adversary cyber threats continue to be identified that elevate the mission risk of previously accepted risks or new vulnerabilities which may pose an unacceptable risk. CSA-10 is a defined requirement to actively manage the system's configuration, and defensibility, to achieve and maintain an operationally relevant cyber risk posture.

This proactive approach will require a cultural change, since most programs view an ATO as giving sufficient cyber protections, and do not include an ongoing, sustained process, or funding, to actively manage its cyber survivability risk posture throughout the lifecycle of the system. We know that when an adversary builds a more capable surface-to-air missile that we will need to respond with improvements to our aircraft or its defenses, but these physical/kinetic risks change more slowly, and the long timelines for iterative resourcing to fund those improvements can meet operational requirements. Unfortunately, those same one to three year timelines to devise, design, fund, produce, test and field cyber risk mitigations do not meet cyber-risk-to-mission requirements. Having a support team in place and funded to proactively act will dramatically reduce that delay and provide an operationally timely level of mission assurance.

Support for systems' implementation of CSA-10 is needed, because known/unknown system/mission risks are being accepted on the first day any new capability is deployed, while the adversaries' increasing capabilities, addition of new system functionality and connection to external capabilities are adding known/unknown system/mission risks or increasing the risks of previously accepted vulnerabilities to an unacceptable operational level. Getting an ATO needs to be viewed as the beginning of a system's risk management process, not the end, in achieving and maintaining an operationally-relevant risk posture. For example, CSA-07, CSA-08 and CSA-10 could be tailored to support requirements for a cATO determination.

Mission-Based Cyber Risk Assessments (MBCRAs), such as Cyber Table-Top (CTT) exercises, and cooperative and adversarial testing performed during system development, should help the PMO determine a cyber sufficiency level in support of each milestone decision or knowledge point, and postulate if the system is on a path to achieving an operationally-relevant cyber risk posture before Initial Operating Capability (IOC). These activities can also generate the data used to assess a mitigation POA&M's potential to improve the cyber risk posture, if effectively implemented. See DoDI 5000.89 ["Test and Evaluation"] for more information on MBCRAs and other cyber testing.

Although the level of detail and artifact granularity will be different, planners for CCMD wargames and exercises could use the CSAs in a similar way to determine a CCMD's OPLAN and mission risk posture, by assessing the risks associated with the risk posture of each of the systems and supporting infrastructure critical to OPLAN and mission success. System owners for systems identified as critical to OPLAN/mission success and with significant cyber survivability risk, should consider requesting resources to support implementing a CSA-10 capability to actively manage the system's configuration to achieve and maintain an operationally acceptable cyber risk posture, and increase mission assurance.

## 4.0 Background

The CSE was created with representatives from the Joint Staff, OUSD (A&S), OUSD (R&E), DoD CIO, NSA, DIA, DOT&E, OUSD (I&S), and the Services. The group focused on improving cybersecurity requirements in CDDs; however, the Services and OSD representatives confirmed that cyber threat and requirements statements would have greater impact if the CSAs were included in ICDs and considered during AoAs, and if the CSAs better articulated cyber resiliency requirements.

The 2018 JCIDS Manual update added Joint Staff reviews of ICDs, and more guidance on requirements for identifying the CSRC and CSAs. The early inclusion of specific cyber survivability requirements in these acquisition documents was intended to allow for more cost-effective, timely, and survivable solutions. Otherwise, solutions might be pursued that are more difficult and costly to implement than survivable options that would also meet operational requirements.

Although CSE is aligned with the SS KPP's cybersecurity intent to Prevent and cyber resiliency's intent to Mitigate, Recover and Adapt from a cyber-related event, CSE had to overcome the cultural paradigm that if the capabilities are inexpensive enough, you can provide sufficient mission assurance and resiliency by acquiring more of them. However, the perspective that one, or more, kinetic bullets are required to achieve one kinetic weapon system kill does not apply to cyber capabilities, where one cyber bullet (one exploitable vulnerability) can potentially kill ALL similarly configured and connected systems.

**Integration of DoD Cybersecurity Frameworks Applicable to Weapon Systems:** The CSE was developed to ensure alignment with existing and evolving DoD and National guidance, including the implementation of the NIST Cyber Resiliency frameworks, the JCIDS SS KPP, DoD instructions for cybersecurity (RMF) and cyber resiliency, and cyber threat intelligence products. Figure 1 visually depicts how CSE integrates with these frameworks, and how the SS KPP terminology connects cyber to kinetic functionality, for enabling consideration of both sets of threshold performance requirements within the same operational risk trade-space with all of the systems other functional requirements.

There is no longer a need to push for Cost, Schedule, Performance *and* Security. JCIDS has defined Cyber Survivability as a performance attribute, and cybersecurity and cyber resiliency requirements are holistically included in cyber survivability. There is no need to add security as a fourth factor.

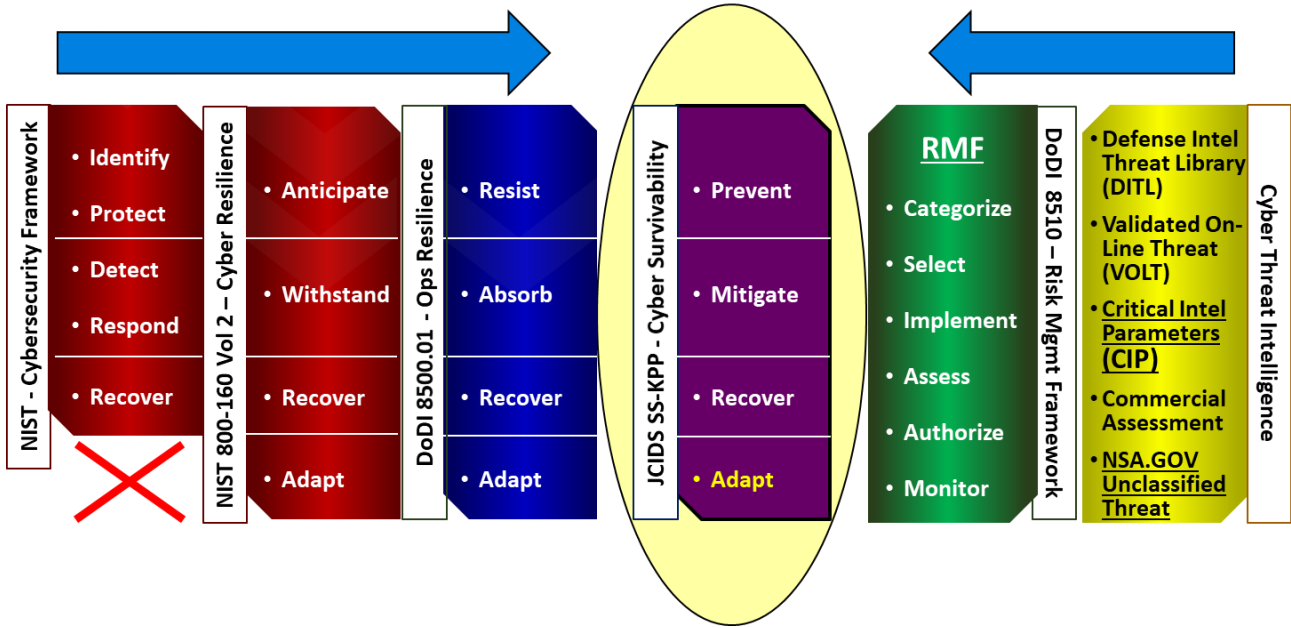


Figure 1: Integrated Cybersecurity Frameworks Leveraged by CSE

Implementation of CSE has helped to begin alignment of cyber terminology across the Department. The latest iteration of the cyber survivability definition aligns well with, and is intended to integrate, the definitions of cybersecurity and cyber resiliency in recent changes to NIST SP 800-160 Volume 2, DoD Dictionary of Military and Associated Terms, DoDI 8500.01 and the JCIDS Manual, that makes references to “Cyber Survivability Considerations (cybersecurity and cyber resiliency)”.

- **Cyber Survivability** – 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. *Source: JCIDS Manual, para 2.5.1.4*
- **Cybersecurity** - Prevention of damage to, protection of, and restoration of computers, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. *Source: DoD Dictionary of Military and Associated Terms, DoDI 8500.01*
- **Security** - A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach. *Source: CNSSI 4009*
- **Cyber Resiliency** - 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. *Source: NIST SP 800-160 volume 2, Revision 1 (1 Dec 2021)*

The NIST cyber resiliency principles in SP 800-160 Volume 2, and DoDI 8500.01, include the adapt component for addressing the evolving and emerging threats to support cyber resiliency. The JCIDS SS KPP helps requirement sponsors to understand and holistically articulate these cybersecurity and cyber resiliency requirements in cyber survivability terms for warfighting systems. CSRC helps define the strength of cybersecurity and cyber resiliency required for these systems, and can be viewed as the on-ramp and partner to RMF.

The cyber threat intelligence support products inform capability owners and RMF AOs, as well as the Joint Staff reviewers evaluating the requirements documents, concerning the level of ATT expected in the intended mission's operational environment. Intelligence cyber threat assessments must be actionable, timely, and released at a classification level usable by requirement sponsors to drive cyber survivability requirements. NSA's unclassified Cybersecurity Advisories have provided a sufficient level of threat information for an ICD and draft CDD, and form the basis for defining the cyber threshold performance requirements and a strength of mechanism measurement of cyber defenses. These threat intelligence products should be reviewed regularly during operations and sustainment so that both the system developers and the operational chain of command maintain awareness of evolving system and mission risk.

Satisfactorily meeting the JCIDS SS KPP CSE requirement does not result in a system's ATO. However, it does define the subset of CSAs determined to be most critical to system survivability. They should enable a program's System Security Engineers to decompose measurable and testable threshold requirements for the RFP to identify source selection criteria. This will enable program managers to use the CSAs, flowed down into the Work Breakdown Structure (WBS), to support justification of specific NIST SP 800-53 security controls during operational risk trade-space decisions. Instead of relying exclusively on RMF's Confidentiality, Integrity, and Availability (C, I, A) categorizations for a program, the system's CSRC value enables program managers to identify the most critical capabilities supporting move, shoot, and communicate functions requiring cyber survivability.

The NIST Cybersecurity Framework organizes basic cybersecurity functions at their highest levels. The framework focuses on using business priorities to guide cybersecurity activities, and considering cybersecurity risks as part of the organization's risk management practices. They help an organization express its management of cybersecurity risk by organizing information, enabling risk management decisions, and addressing threats. The functions also align with existing methodologies for deficiency and incident management, and to show the impact of investments in cybersecurity. CSE integrates with this framework to leverage their value and the benefits of their guidance.

- ***NIST Identify and Protect (Anticipate)*** (CSE Prevent) – organizational understanding of what is required to manage cybersecurity risk to systems, assets, data, and capabilities; safeguards to ensure delivery of critical infrastructure services
- ***NIST Detect and Respond (Withstand)*** (CSE Mitigate) – activities to identify the occurrence of a cybersecurity event; appropriate actions to take regarding a detected cybersecurity event
- ***NIST Recover and Adapt*** (CSE Recover and Adapt) – activities to maintain resiliency and restore capabilities and/or services that were impaired due to a cybersecurity event



For information on the NIST Cybersecurity Framework, see <https://www.nist.gov/cyberframework/>

For the Committee on National Security Systems Instruction (CNSSI) 4009 definition of “cyber incident”, see the glossary, or review the document at the Cyber Survivability SharePoint site on the NIPRNet at <https://intelshare.intelink.gov/sites/cybersurvivability/>

The SS KPP pillars are mapped to attributes that contribute to the survivability of a system’s capabilities. These include Prevent attributes that support reduced likelihood of being hit by these fires, reduced vulnerability and impact if hit by these fires (including in cyberspace), and resiliency of the system and overall force (broader than a single system architecture) to complete the mission. The Mitigate attributes support completing the mission despite the loss of some cyber functionality, with a minimum cyber capability remaining. The Recover attribute supports restoring the system to a known good condition to fight another day. The Adapt attribute enables the constant monitoring and maintenance of the capability over its lifecycle. The cyber requirements of the SS KPP must be feasible to implement, be measurable, and be testable. The requirements are based on the mandatory SS KPP pillars for cyber-event effects:

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

The Protection Functional Capability Board (FCB) is the office of primary responsibility for the SS KPP. The Chair of the Protection FCB endorses the SS KPP in accordance with the Gatekeeping process described in Appendix C to Enclosure A of the 2021 JCIDS Manual. The SS KPP endorsement is applicable to CDDs, IS-ICDs and IS-CDDs. Certain precursor steps and requirement development activities are applicable to ICDs.

**Cybersecurity and RMF for DoD Information Technology:** The CSAs are supported by a subset of the DoD’s RMF and its NIST SP 800-53 controls. Each of the CSAs and their strength of implementation must be considered to appropriately address cyber risk. For information on RMF controls, refer to DoDI 8510.01, RMF for DoD Information Technology (IT), available on the Cyber Survivability SharePoint site. For information on strength of implementation, see CNSSI 1253, also available on the Cyber Survivability SharePoint site. CSAs provide the outcome of defined cyber threshold performance requirements that should drive development of the RFP and source selection criteria, support system engineering decomposition, and a program manager’s operational risk trade-space decisions for resourcing RMF Security Controls.

**System Security Engineering (SSE):** The SS KPP pillars, and their CSA categories, provide a foundation for developing an architecture to support cyber security and cyber resiliency requirements. Early determination of a system’s CSRC and selecting a tailored subset of CSAs in a requirement’s criticality analysis and design provides the engineers with options to support decisions prior to establishing the

solution architectures. This maximizes the trade-space available for cybersecurity solutions, which is necessary to ensure the SS KPP is achievable within identified priorities and constraints.

The CSE Community of Interest teamed with the Air Force Research Laboratory (AFRL) to produce an automated CSA Tool to assist requirements sponsors. The tool helps to determine a system's CSRC statement for an ICD, recommend AoA guidance to understand the resource and mission risk implications of each CSA, refine the CDD's CSRC statement, and identify the subset of CSAs most critical to system survivability. The tool also identifies NIST SP 800-53 security controls that could support the decomposition of CSAs for each CSRC level. This enables sponsors to perform a what-if, intrinsic assessment of the system's potential CSRP based on the technical controls selected. Vulnerabilities with system and mission risk can be mapped to the CSAs to begin to assess the overall CSRP for the system and the mission.

The Department of Defense Chief Information Officer (DoD CIO) drafted a CSEIG Volume II to supplement this guide that supports implementation of the cyber survivability requirements and follow-on acquisition and testing community efforts. In this document, the Deputy DoD CIO for Cybersecurity, through collaboration with the Joint Staff/J6, the DIA, and the NSA's (then-named) Information Assurance Capabilities Office, organized the CSAs into a Systems Engineering/Systems Security Engineering (SE/SSE) view. This illustrates how the SS KPP cyber survivability requirement should be addressed in a logical deconstruction of the capabilities documents. AFRL has integrated this Volume II information into the CSA Tool. Its automated integration has also met the intent of NSA's Volume III supplement to help define a suggested strength of implementation for the CSAs, so that the cyber threshold performance requirements are commensurate with the MT, ATT, CDL, and IL in the expected operational environment. The Air Force's Cyber Resiliency of Weapons Systems (CROWS) team of System Security Engineers is also supporting CSA Tool development using the content of their SSE Cyber Guidebook with workflow processes and artifacts.

All references cited in this guide are available on the Cyber Survivability SharePoint sites:

<https://intelshare.intelink.gov/sites/cybersurvivability/>

<https://intelshare.intelink.sgov.gov/sites/cybersurvivability/>

**Cyber Supply Chain Risk** – Supply Chain Risk Management (SCRM) presents a greater impact on system survivability with recent discoveries of nation-state threat actors' involvement in the global supply chain for hardware, software and firmware (HW, SW, FW). Cyber SCRM encompasses a range of risk management activities that go beyond traditional configuration management best practices. Cyber SCRM influences multiple CSAs, but should be addressed in CSA-10 to address Cyber SCRM across the system's lifecycle. CSA-07 and CSA-10 have been updated with functional requirements that should drive Contract Deliverable Requirements List (CDRL) requirements for a Bill of Materials configuration baseline of the GOTS/COTS HW, SW, FW and open source modules by version number, along with their associated supply chain risk assessment information, for each milestone decision and supported release.

**Cyber Threat Intelligence** –The cyber-contested environment should be described within all capability requirement documents, and the Intelligence Community (JS J2, NSA and DIA) has worked closely on CSE to ensure the availability of actionable cyber threat information earlier in the acquisition process. The threat environment characterization should include data informing Critical Intelligence Parameters (CIPs). The IC

should drive requirement changes to account for the integration of the classified cyber threat with the commercially-available cyber threat data, and make it available for the acquisition and operational communities. If possible, threat details should be inclusive of state actors or countries in which threats are expected to emanate. The threat should include Cyber, Foreign Intelligence Entities, and supply chain threats. The 2021 NSA/CISA/DOJ Cybersecurity Advisories provided unclassified descriptions of nation specific capabilities and mitigations, which drove an expansion of the ATTs and CSRCs to 5 levels. This is the most actionable cyber threat information to date at the unclassified level and is sufficient for an ICD and draft CDD, prior to availability of a VOLT report for the capability's final CDD.

The CSE framework recommends inclusion of an unclassified, integrated, and threat-informed cyber countermeasures requirements statement in the ICD, AoA guidance, IS-ICD, IS-CDD and CDD. Selection of the appropriate statement is based on a CSRC determination. The high-level threat information included in the CSRC exemplars may be all that is available for an ICD, until an AoA is completed and identification of a preferred solution can define the specific technologies of interest, needed for development of a more detailed and system specific cyber threat assessment. In support of a Materiel Development Decision (MDD) and conducting an AoA, sponsors should use relevant cyber threat intelligence from the Defense Intelligence Threat Library (DITL). Commercial sources for threat assessments should be considered, to provide an unclassified threat that can be used to augment DoD-sourced classified threat intelligence and justify increased cyber survivability countermeasures. After a preferred solution is identified or significant technology changes integrated into new releases, the program should request a VOLT report to align the current cyber threat intelligence to the solution's attack surfaces or technical attributes.

The DITL is a collection of threat modules that are produced and updated by the Defense Intelligence Enterprise to support the intelligence needs of DoD acquisition programs throughout their lifecycles, from requirements development through sustainment. The Cyber Threat Modules (CTMs) are produced by Intelligence Community subject matter experts under the Defense Intelligence Analysis Program, and validated by the DIA.

A VOLT report can serve as the primary threat reference supporting a requirement document, and answers specific intelligence questions or requests raised by the program, capability developer, or test representatives. The VOLT report is a living online document that embeds the most current threat documents. A VOLT report will include links to relevant DITL threat modules. Program system security engineers should use the VOLT report to shape and tailor the system specifications for cyber countermeasures within each CSA. Additionally, they will specify applicable Critical Intelligence Parameters (CIP) for Intelligence Community (IC) monitoring. CIPs are defined as adversary key performance thresholds (established collaboratively by the requirements sponsor and the component capability developer) that, if exceeded, could compromise mission effectiveness, and could critically impact the survivability of the proposed system. CIPs should be included for capabilities in development that are determined to be threat-sensitive; requirements sponsors should coordinate with DIA or their supporting Service intelligence center to determine CIP applicability. CIPs will be tasked as production requirements in accordance with DIA Directive 5000.200 (available on the CSE SIPRNet SharePoint). For information about DITL, VOLT reports, and CIPs, see: [https://intellipedia.intelink.sgov.gov/wiki/Defense\\_Intelligence\\_Threat\\_Library](https://intellipedia.intelink.sgov.gov/wiki/Defense_Intelligence_Threat_Library)

The JCIDS process, the Major Capability Acquisition pathway process, and the capability requirements documents shown in Figures 2 and 3 illustrate the opportunities for cyber survivability's potential benefit to mission assurance within these processes. Early in the lifecycle, with emphasis on supporting CDD development, programs conduct systems engineering trade-off analyses, showing how cost varies as a function of system requirements (including KPPs), major design parameters, and schedule. CSAs should be evaluated as part of these early efforts to inform selection and refinement of CSAs through the development of capability documents that are incorporated into acquisition strategies and RFPs. MITRE research identified tremendous potential for the tools such as the CSA Tool to conduct what-if analyses. The document (Cyber Resiliency Framework and Cyber Survivability Attributes: Mapping Cyber Resiliency to the CSEIG CSAs, 2021) identified synergies with cyber resiliency that can articulate augmentations to the CSAs. This further illustrates methods for implementing the CSAs.

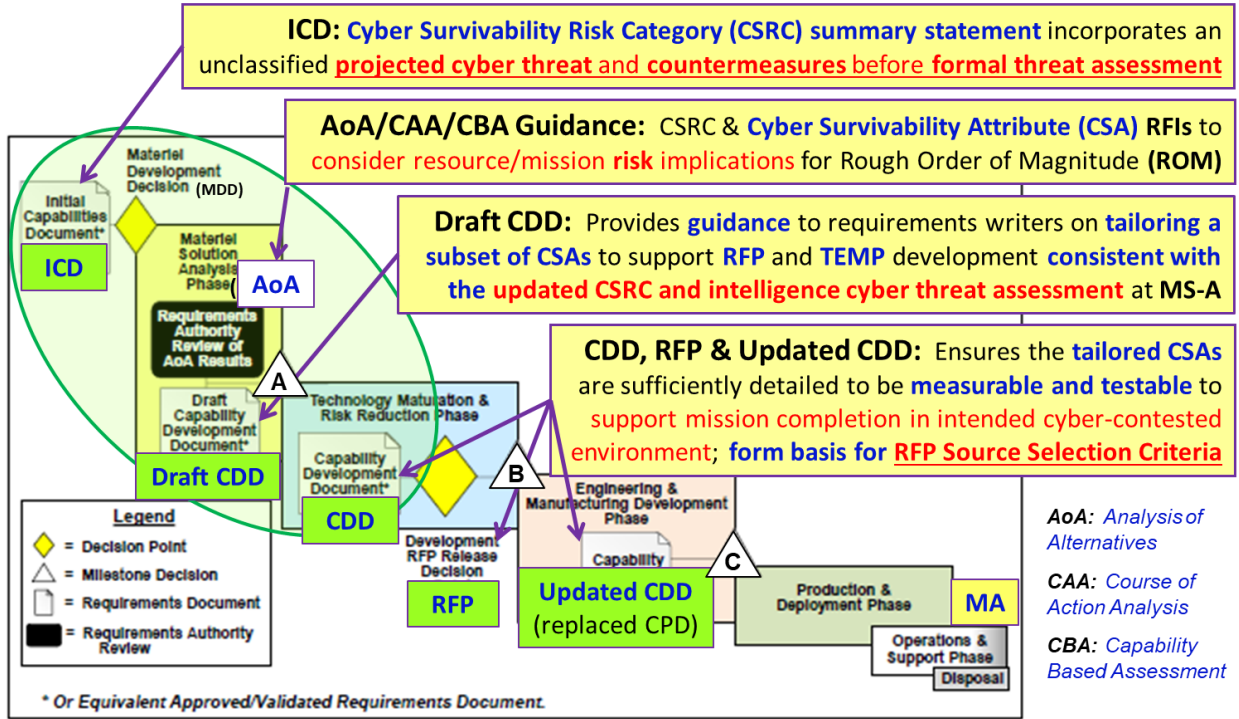


Figure 2: Interactions of the JCIDS and Major Capability Acquisition Pathway Processes

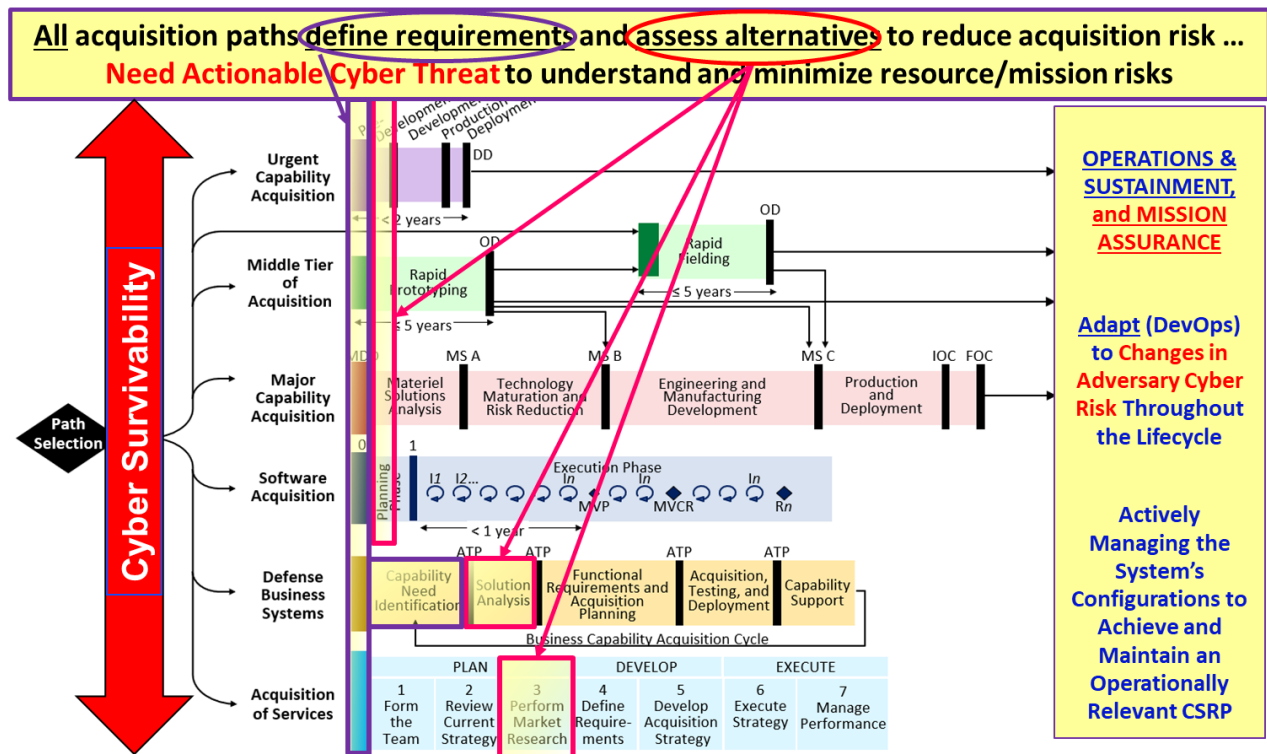


Figure 3: The JCIDS SS KPP and CSE in all Capability Acquisition Pathways

## 5.0 Using CSE to Determine the Level of Cyber Sufficiency Throughout a Capability's Lifecycle

CSE enables requirement sponsors to holistically articulate the cybersecurity and cyber resiliency threshold performance requirements for ensuring a system's minimum viable capabilities can effectively move, shoot, and communicate at an operationally acceptable mission assurance level. Beginning with capability identification and throughout development, system engineering, testing, and operations, the need to field and maintain an effective, survivable military capability requires attention at all stages of its lifecycle.

Other DoD cyber dependent processes can benefit from CSE, if their cybersecurity and cyber resiliency requirements are aligned with and can be linked to contractually binding cyber survivability threshold performance requirements. No matter how many DoDIs are created to provide cybersecurity guidance or identify hundreds of cybersecurity requirements, if the terminology isn't consistent and specifically stated in requirement documents as cyber threshold performance requirements and RFP source selection criteria, they aren't contractually binding.

CSE's CSAs can be used by a capability owner to create measurable and testable cyber threshold performance requirements. They are intended to be tailored for each capability and provide a consistent understanding of the level of cyber survivability required throughout its lifecycle, and their flexibility is well suited to all acquisition pathways. It is easier to apply CSE to rapid acquisition efforts, where the technologies are more mature and the vulnerabilities/threats make it easier to determine the potential resource and system risk implications.

Resource sponsors and program managers make risk assessments and capability trade-off decisions throughout capability selection and development. Milestone Decision Authorities should consider reviewing the level of cyber sufficiency at each Knowledge Point and Milestone. Such risk assessments and decisions should inform and support critical requirements within the following documents:

**MDD Requirements Development:** based on a validated capability requirement document (ICD or equivalent), directing execution of an AoA, with cyber survivability guidance included in the AoA Study Plan. The ICD's CSRC summary statement of adversary cyber threat and associated countermeasures, along with a list of CSAs to be considered can drive any acquisition pathway's analysis of alternatives study team guidance, and for the RFIs needed to differentiate cyber resource and mission risk implications between candidate capabilities and prevent pursuit of capabilities so flawed it would be inconceivable to cost-effectively mitigate known cyber risk to an operationally acceptable level.

- ICD CSRC driven by Cyber Threat Intel: Does the Adversary Threat Tier and Mission Type identified match the expected cyber threat environment, and does the information provide an unclassified threat and required countermeasures sufficient for the ICD's CSRC Summary Statement? Does the ICD identify requirements for artificial intelligence, machine learning or autonomous capabilities that would by themselves drive a high Cyber Dependency Level and increase the CSRC? In order to proactively maintain an operationally relevant cyber survivability risk posture, has a frequency of adversary cyber threat updates been identified for the IC to report changes in adversary cyber threat to the GOTS/COTS

HW, SW, FW and open source modules proposed to be integrated into the DoD capability, or within the commercial capability being considered for acquisition?

- AoA: Did the ICD CSRC and CSAs drive AoA RFI guidance, and did review of the RFIs associated with each of the ten CSAs during the AoA provide a sufficient understanding of the resource/mission risk implications to each alternative if the capability is unable to meet the intent of each CSA, in any acquisition pathway, and support a rough order of magnitude (ROM) determination and differentiation between capabilities?
- MDD Cyber Sufficiency Assessment/Status (ICD, AoA): Did the ICD define a CSRC, CSAs and provide AoA guidance for RFIs, and provide sufficient information for a comparative analysis to determine potential resource/system risk implications if the capability itself, hosting system or expected enterprise service would not meet intent of all the CSAs? Did the RFIs request sufficient information to determine if a CSA is/isn't critical to the system's survivability, in order to drive the CDD's identification of a subset of CSAs most critical to system survivability?

**Milestone A (Material Solution Analysis approval):** The CDD's updated CSRC summary statement and subset of CSAs identified as most critical to system survivability can drive development of the Request for Proposal (RFP) and source selection criteria, helping prevent acquisition of capabilities so flawed it would be inconceivable to cost-effectively mitigate known cyber risk to an operationally acceptable level.

- Draft CDD CSRC driven by Cyber Threat Intel: Was a specific cyber threat assessment requested based on results of the AoA? Did a VOLT, commercial threat assessment or cyber threat countermeasure update drive tailoring of the CSRC summary statement? In order to proactively maintain an operationally relevant cyber survivability risk posture, has a frequency of adversary cyber threat updates been identified for the IC to report changes in adversary cyber threat to the GOTS/COTS HW, SW, FW and open source modules proposed to be integrated into the DoD capability, or within the commercial capability being considered for acquisition?
- RFP Source Selection Criteria: Did the CDD's CSRC summary statement and subset of CSAs identified as most critical to system survivability drive development of the RFP and source selection criteria to help differentiate between the capabilities being considered?
- MS A cyber sufficiency status (AoA, draft CDD's CSAs, draft Program Protection Plan (PPP), Cybersecurity Strategy (CSS), Test and Evaluation Master Plan (TEMP), System Engineering Plan (SEP), Statement of Work (SOW), et al): Were the cyber survivability adversary threat and countermeasures updated in the draft CDD's CSRC? Did the results of the AoA identify a subset of CSAs determined to be most critical to system survivability, and were they consistently articulated within the RFP technical evaluation Measures of Performance and Measures of Effectiveness criteria, draft PPP/CSS, TEMP, SEP and SOW?

**Milestone B (Technology Maturation & Risk Reduction / Preliminary Design Review):** Program Managers (PM), System Engineers (SE), and System Security Engineers (SSE) should decompose the subset of CSA threshold performance requirements to prioritize operational risk trade-space decisions for engineering-in

specific cybersecurity and cyber resiliency design concepts associated with the CSAs most critical to system survivability.

- Did a VOLT report, commercial threat assessment or cyber threat countermeasures update identify significant changes to the expected adversary cyber threat capabilities, and in turn drive a reconsideration and prioritization of cyber threshold performance requirements, in order to achieve and maintain an operationally relevant risk posture?
- Did PM use the CDD's subset of CSA threshold performance requirements to prioritize operational risk trade-space decisions, selection, testing and effective implementation of cybersecurity and cyber resiliency controls associated with the CSA most critical to system survivability?
- Did SEs and SSEs decompose the CDD's subset of CSA threshold performance requirements into specific minimum viable cybersecurity and cyber resiliency requirements, and include these requirements in the specification flow-down?
- Did the PMO and DT organization use the missions, threats, and CSA threshold performance requirements to document (in the PMO's TEMP or other T&E strategy document) the plan to execute cyber T&E events, beginning with the system developer/contractor through government-led testing?
- MS B cyber sufficiency status (RFP and updated PPP, CSS, TEMP): Did the PMO and DT organization use the data generated during DT associated with the CSA threshold performance requirements to determine if the program is on a path to achieve an operationally acceptable risk posture by IOC?

**Milestone C (Engineering & Manufacturing Development / Critical Design Review):**

- Did an adversary cyber threat update drive a reconsideration and prioritization of cyber threshold performance requirements, in order to achieve an operationally relevant risk posture?
- To proactively maintain an operationally relevant cyber survivability risk posture, has a frequency of adversary cyber threat updates been coordinated/validated with the IC to report changes in adversary cyber threat to the COTS/GOTS HW, SW, FW and open source modules integrated into the DoD capability?
- Did Resource Sponsor, PM, and SE make operational risk trade-space decisions, effectively balancing functional and cyber performance requirements with POA&Ms to pursue threshold performance capabilities, to achieve an operationally-relevant cyber risk posture?
- Did the AO use cyber sufficiency status updates from developmental testing associated with the CSA threshold performance requirements; OT reports to determine residual risk; POA&M mitigation status; and if the program is resourced to be able to achieve and maintain an operationally acceptable cyber risk posture, ATO and MA assessment rating (within an operationally acceptable timeline) to support risk acceptance decision?
- Has a requirement for a continuous ATO been identified, based upon a high CSRC and high mission criticality, and are CSA-07 (baseline, monitor and detect anomalies), CSA-08 (manage system performance if degraded by cyber-events) and CSA-10 (adapt system configuration to counter



changes in adversary threat and connected vulnerabilities) sufficiently defined to meet the intent of proposed continuous ATO (cATO) requirements?

- MS C cyber sufficiency status (CDD update, Design, Develop, Test, validate PPP/CSS): Does the CDD update, Developmental Test/Operational Test (DT/OT) reports, PPP/CSS and AO risk determination support a full rate production decision and deployment?
- Have supply chain risks to the cyber survivability of the GOTS/COTS HW, SW, FW and open source components been informed by cyber threat intelligence provided by the IC, and does the system design incorporate means to mitigate those risks during operation?
- Was the MS C decision authority provided with artifacts from the early cyber survivability considerations, and the results of cyber survivability sufficiency assessment status/reports to support a MS C decision?

#### **Alternative Acquisition Pathways**

- Was cyber survivability considered early, to ensure a reasoned expectation the capability could be sufficiently cyber survivable in the intended operational environment? Was a CSRC requirement determination made?
- Were CSA RFIs sent to and reviewed to make a ROM determination on the potential resource and mission risk implications if the capability could not meet the intent of the CSAs?
- Did the CSA RFIs provide sufficient information to determine if it was conceivable to cost effectively mitigate the known risks to an operationally acceptable level?
- Was a subset of the ten CSAs identified as critical to system survivability and its move, shoot, and communicate functions?
- Was government and/or contractor testing performed on the subset of CSAs identified as critical to system survivability, and were the results provided to the MS decision authority and RMF AO?

#### **IOC/ Full Operating Capability (FOC): Operations & Sustainment**

- Did an adversary cyber threat update drive a reconsideration and prioritization of cyber vulnerability mitigations with the greatest CCMD OPLAN/Mission risk, in order to achieve and maintain an operationally relevant cyber survivability risk posture?
- Has the IC provided timely cyber threat updates, based on technical/TTP, supply chain, intent/likelihood and assessed emerging capabilities, for the GOTS/COTS HW, SW, FW and open source modules (by version number) integrated into WS and CI, required to maintain a POA&M timeline for an operationally-relevant risk posture?
- Have Services' updates on cyber assessments and mitigation POA&Ms improved the cyber risk posture of their systems?
- Has a consistent cyber risk posture self-assessment process been coordinated with the Services to consolidate cybersecurity and cyber resiliency data calls into a single quarterly cyber survivability data call? A consolidated data call could ensure consistent reporting requirements for various

Department reviews and reports, such as NDAA 1637, SCP, CIO Top Ten Scorecard, Acquisition Milestone cyber sufficiency, DT/OT, DCRA's, et al.

- Have CCMD's received periodic cyber risk posture reports and cyber threats associated with the capabilities critical to/determine a cyber risk posture for their OPLANs/Missions, make risk acceptance decisions, identify mitigation priorities, and support annual integrated priority list submissions?

**DoD Mitigation Priorities:** CSE provides a shared understanding of the cybersecurity and cyber resiliency levels required throughout a system's lifecycle, and lays the foundation for a CCMD OPLAN/Mission-focused and scalable governance process. The CSE framework of adversary cyber threat, CSRC, CSAs and CSRP, along with Service mitigation POA&Ms and CCMD priorities helps to ensure accountability and align the many entities with a hand in cyber survivability. Capability owners can use the CSE framework of CSAs to actively manage their HW/SW/FW configuration baselines, with links to current configuration data and vulnerabilities, mitigations options, and threats, for operational risk trade-space decisions.

The following steady-state processes demonstrate how the DoD could orchestrate organizations deliverables within existing authorities, roles and responsibilities for assessing, prioritizing, resourcing and mitigating vulnerabilities with the greatest CCMD OPLAN/Mission risks.

- IC for reporting adversary threat capabilities against DoD weapon systems (WS) and critical infrastructure (CI), by GOTS/COTS HW/SW/FW version integrated within them;

Deliverables - Adversary Capabilities Assessment: Meet intent of Cyber CIPs, with a scalable and relevant process that supports both acquisition and operations. Provide adversary cyber threat update, based on technical/TTP, supply chain, intent/likelihood, and assess emerging adversary capabilities against the GOTS/COTS HW, SW, FW version number integrated into DoD WS and CI, required for operationally-relevant POA&M timeline.

- Service/Agency for defining, acquiring, building, testing and maintaining survivable WSs and associated CI, and reporting WS and CI cyber risk posture and mitigation POA&Ms to CCMDs and OSD/JS;

Deliverables - System cyber risk posture Assessment: Capability owners use the CSE framework of CSAs to actively manage their HW/SW/FW configuration baselines, with links to current configuration data and vulnerabilities, mitigations, and threat for operational risk trade-space decisions, and self-reporting WS and CI cyber risk posture with POA&M (e.g., NDAA 1640/1637, CIO Top 10 Cyber Scorecard). Capability development contracts must include CSE requirements, testing, and CDRLs to support assessment of these requirements.

- CCMD for reporting OPLAN/Mission cybersecurity and cyber resiliency risk posture, based on adversary cyber threat capabilities against the WS/CI required for OPLAN/Mission success, prioritized vulnerabilities with the greatest CCMD OPLAN/Mission risk, and CCMD risk acceptance of cyber vulnerability mitigation POA&Ms to OSD/JS;

Deliverables - OPLAN/Mission cyber risk posture Assessment: CCMDs review the Service/Agency CS cyber risk posture RP reports on the legacy WS and CI supporting their missions/OPLANs, by integrating systems vulnerabilities and threats into CCMD Exercises/Wargames (e.g., A&S Mission Resilience identify legacy systems with critical risks to OPLAN success and drive cyber “Adapt” resourcing), Deep Cyber Resiliency Assessments (DCRA), and Cyber Table Top Exercises (CTTXs) to determine their CCMD OPLAN/Missions’ cyber risk posture, and determine acceptability of mitigation POA&Ms to identify Service/Agency disconnects. Systems with unacceptable mission risk implications, such as demonstrated adversary cyber threat capabilities to systems with unmitigated vulnerabilities, and mission dependencies without adequate alternatives, need to consider pursuit of JROC validation and forwarding the requirement to expeditiously address this situation.

- OSD/JS for arbitrating/prioritizing programmatic disconnects between Service/Agency mitigation POA&Ms and CCMD OPLAN/Mission requirements.

Deliverables - DoD-wide Mission cyber risk posture mitigation: Cyber sufficiency reviews at acquisition milestones. SCP reviews of Intel, Service/Agency and CCMD cyber survivability risk reports to reconcile disconnects and provide programmatic mitigation recommendations as required to the JROC (to validate updated legacy cyber threshold performance requirements), OPSDEPS, 3-Star Programmers and Deputies’ Management Action Group. This may require updating charters to support reporting expectations for deliverables, and responsibility/authority to prioritize programmatic recommendations.

A list of acquisition documents and submission timelines is included in DoDI 5000.02. This guide provides Cyber Survivability exemplar language for use in ICDs, AoAs, RFPs, and CDDs, based on CSRC levels.

## 6.0 CSE in Alternative Acquisition Pathways

Of all the JCIDS KPP requirements, system survivability should be a critical consideration for any acquisition. No matter how quickly a capability needs to be fielded, if it is not reasonable to expect it to be cyber survivable in the expected operational environment, then it is of no operational utility and should not be pursued. CSE’s simple and flexible framework works for any acquisition pathway, and could apply an approach similar to an AoA’s review of RFIs associated with a capability’s ability to support each of the CSAs. It is easier to apply CSE to rapid acquisition capabilities, because more is known about the maturity level, vulnerabilities, and threats to those systems for a ROM determination of the potential resource and mission risk implications of not meeting the intent of the CSAs critical to the system’s survivability and its move, shoot, and communicate functions.

If an ICD, AoA, CDD and RFP consider cyber survivability early in the acquisition process, there is a greater likelihood of identifying solutions that can cost effectively mitigate cyber risks and meet operational requirements. CSAs are intended to be tailored for each capability and provide a consistent understanding

of the level of cyber survivability required throughout its lifecycle. CSE's flexibility is well suited to all acquisition pathways.

The adoption of the CSEIG in the Adaptive Acquisition Framework's Major Capability Acquisition pathway, and including a cyber sufficiency status report at each milestone and knowledge point, have the potential to increase the survivability of new weapons systems and reduce costs associated in the development and acquisition of those systems. However, alternative acquisition pathways such as Middle Tier of Acquisition and Joint Urgent/Emergent Operational Needs are not subject to JCIDS requirements, including the SS KPP, and are thus vulnerable to the fielding of a capability which may not be survivable in a cyber-contested environment. Because of CSE's flexibility and benefits, stakeholders in alternative acquisition pathways are encouraged to adopt the parameters outlined in the JCIDS SS KPP and the CSEIG to assess, and strengthen, system survivability.

Rapidly fielding an unsurvivable capability is of limited, or no, long term operational utility. The CSAs are minimum viable parameters that enable the Combatant Commands, Services, and Agencies to align and rationalize their efforts from the identification of a requirement, development of a solution, prototyping, testing, production and deployment of a survivable weapon system in a cyber-contested environment.

JROCM 009-17 encouraged Services to use the Joint Staff CSE Implementation Guide, or develop their own guidance. Cyber survivability is a performance attribute and supports operational risk trade-space decisions in JCIDS requirements. CSE's framework can help sponsors streamline requirements generation and articulate a reasoned set of risk mitigations, to ensure an improved level of mission assurance, to be placed on contract and tested throughout development.

Instances of acquiring costly cutting-edge functionality that is later found to be insecure, and subsequently delay fielding until redesigns attempt to address the vulnerabilities, drive up acquisition costs, delay fielding of survivable capabilities, and increase mission risk from acceptance of systems too costly to remediate. Additional cybersecurity measures which are added to these systems to attempt to make them secure have been found to rob performance, thus preventing the fielding of an operationally effective capability.

CSE's holistic approach aligns well with the Department's alternative acquisition efforts, by providing:

- Flexibility to focus on effectively implementing cybersecurity and cyber resiliency requirements most critical to system survivability and mission accomplishment in the expected cyber-contested environment.
- Comprehensive threshold performance requirements to prevent the most likely cyber risks, mitigate cyber-event effects to complete the mission or return to base, recover to a known good condition to fight another day, and adapt to future changes in cyber risk.
- An "adapt" component, with a process enabling program managers to actively manage their system's configuration to maintain an operationally-relevant cyber risk posture throughout its lifecycle.

CSE's process can help requirement sponsors understand and articulate the cyber risk, and provide a set of mitigations to support the acquisition of survivable capabilities, if the:

## UNCLASSIFIED

- Resource and mission risk implications of a capability's ability to meet the intent of each CSA are effectively considered during analysis of alternatives, prototyping or development of technologies.
- Threshold RFP/source selection criteria are defined for CSAs most critical to a system's survivability and its move, shoot, and communicate functions.
- CSAs are decomposed into specific cybersecurity and cyber resiliency requirements, engineered in during development, tested and adapted to counter cyber risk throughout the systems lifecycle.
- System configuration is actively managed to prioritize the mitigation of vulnerabilities with the greatest mission risk, and support an operationally-relevant Cyber Survivability Risk Posture.

## 7.0 Overview of the Cyber Survivability Endorsement Process

The CSE process is a risk-managed framework to develop mission impact-focused cyber survivability requirements, based on holistically including its cybersecurity and cyber resiliency requirements. The CSE does this by defining a CSRC that guides the strength of cybersecurity requirement implementation levels to promote operational resiliency, system survivability and mission assurance. As shown in figure 4, the CSRC is a function of:

- Step 1: Selecting the system’s MT
- Step 2: Selecting the expected ATT actor(s)
- Step 3: Selecting the system’s CDL
- Step 4: Selecting the IL of system compromise to supported missions
- Step 5: Determining the capability’s CSRC

At the ICD level, MT and ATT are understood sufficiently to determine an initial CSRC. After the AoA, the CDL and IL can also be determined to refine the CSRC level for the selected capability development.

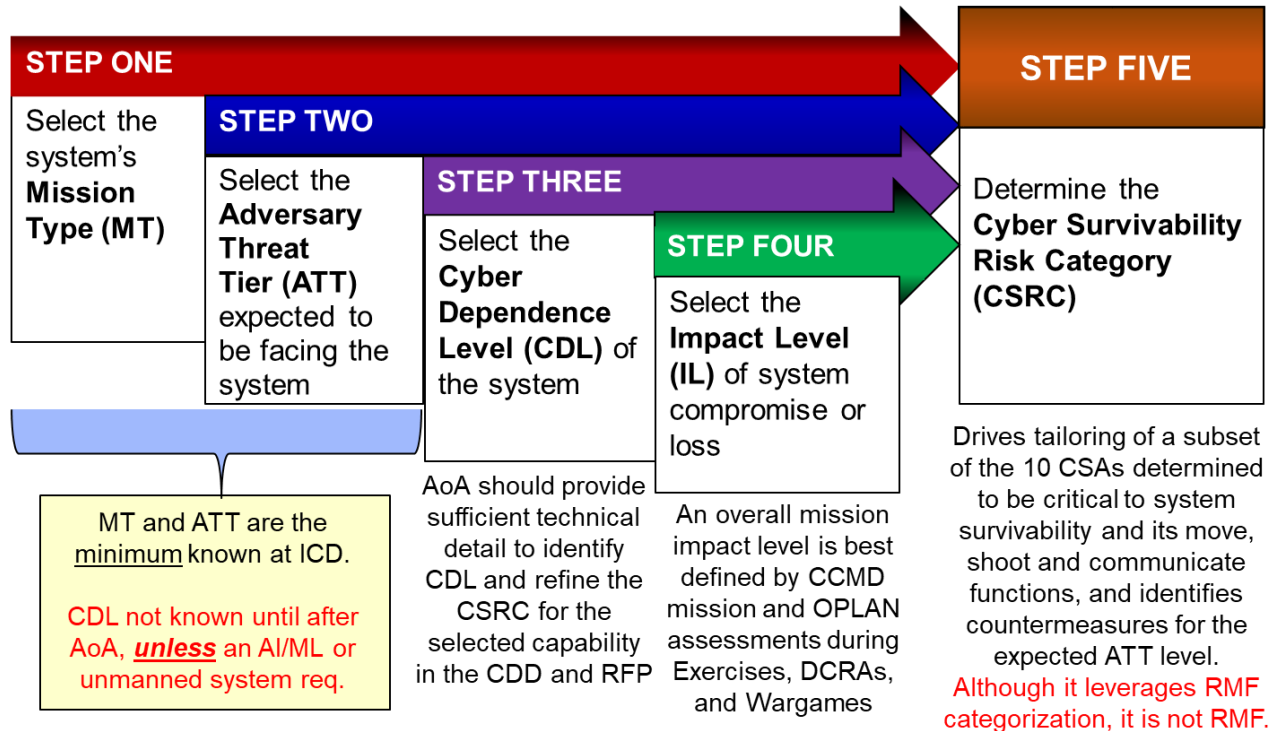


Figure 4: Cyber Survivability Risk Category Determination

## 8.0 Implementing the Cyber Survivability Endorsement Process

### 8.1 Step 1 –Mission Type (MT)

Step one identifies the most stressing MT for which the system is intended to be used.

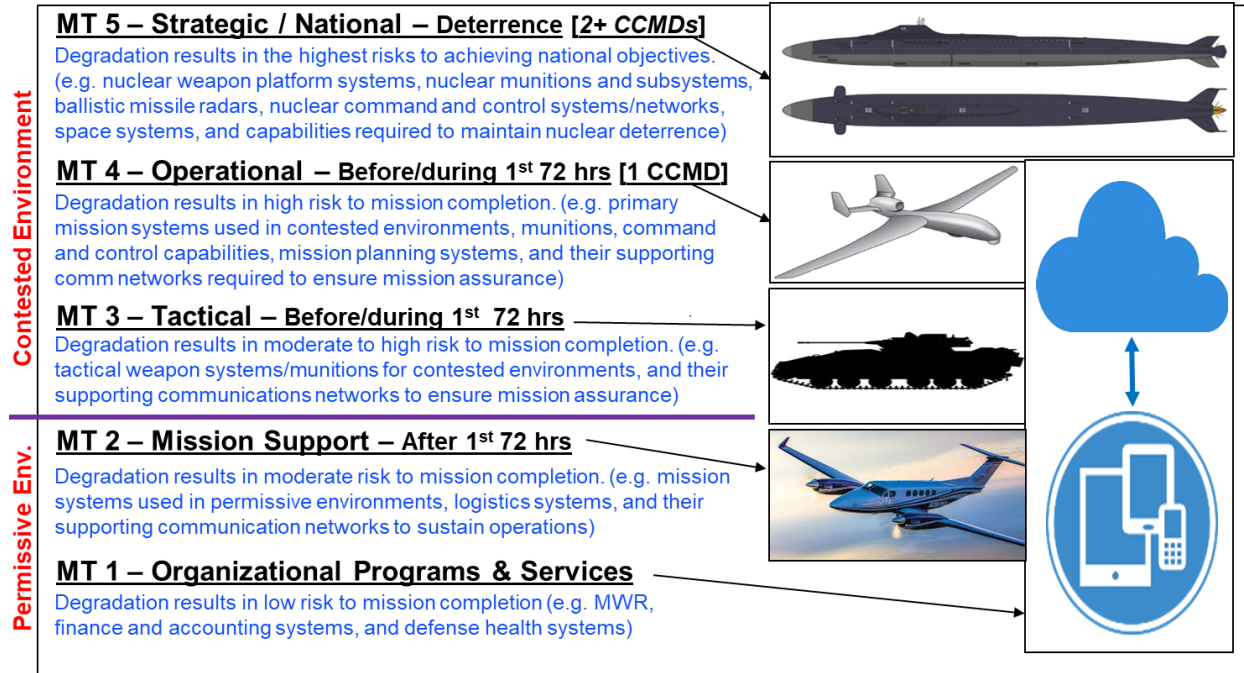


Figure 5: Mission Types

For information on resiliency, see NIST SP 800-160 Volume 2 (revision 1) and Annex C to Appendix G to Enclosure B of the JCIDS Manual (SS KPP Guide). For information on C, I, A, see CNSSI 1253 on the Cyber Survivability SharePoint or at: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

## 8.2 Step 2 – Adversary Threat Tier (ATT)

Step 2 requires assessing system-specific threats and determining an ATT. The ATT is an estimate of the most likely, greatest risk to be expected in a capability’s operational environment, which may change as the requirement matures to a CDD, and throughout the lifecycle, but the ATT helps to bound the cyber risk and approximate the level of mitigations required to counter the anticipated threat. Capability requirement sponsors should initiate this step with research of all-source intelligence applicable to their sponsored system. This guide recommends several intelligence product lines and provides ATT criteria/descriptions. A useful starting point for research is the DITL, described in section 4.0 of this guide.





|   |   |
|---|---|
|    | <p><b>ATT 5 – Extreme:</b> (e.g., <a href="#">Russia SVR</a>, <a href="#">APT-29</a>). Uses a range of initial exploitation techniques that vary in sophistication, coupled with ‘stealthy’ intrusion tradecraft to cause denial, degradation, deception, disruption, and destruction of mission capabilities. Uses custom tools, compromised accounts, and system misconfiguration to blend in with normal/unmonitored traffic to move undetected in victim networks. Demonstrated capability to target cloud resources and supply chain (e.g., SolarWinds).</p> |
|    | <p><b>ATT 4 – Advanced:</b> (e.g., <a href="#">Russia GRU</a>, <a href="#">APT-28</a>; <a href="#">China APT-41</a>). Conducts complex, long-term cyber attack operations combining multiple intelligence sources to obtain access to high-value networks. After gaining access, combines well known TTPs to move laterally, evade defenses and collect additional info. Uses tools to conduct widespread, distributed and anonymized ‘brute force’ access to cloud services. Develops detailed target technical knowledge for more damaging attacks.</p>         |
|    | <p><b>ATT 3 – Moderate:</b> Sophisticated, persistent, and well-resourced adversaries at nation-state level. Capable of advanced cyber tradecraft to use publicly available tools, develop/use customized malware, and acquire access to some ATT-4/ATT-5 tools to stealthily implant malware/vulnerabilities, conduct wide-ranging intelligence collection operations, gain access to more isolated networks, and in some cases, create limited effects against defense critical infrastructure networks.</p>  |
|  | <p><b>ATT 2 – Limited:</b> Capable of limited advanced cyber tradecraft using publicly available and customized tools to exploit known and unknown vulnerabilities. Able to identify -- and target-for espionage or attack -- easily accessible unencrypted networks running common operating systems using publicly available tools. Possesses some limited strategic planning.</p>  |
|  | <p><b>ATT 1 – Nascent:</b> Little-to-no organized cyber capabilities, with no knowledge of a network's underlying systems beyond publicly connected open-source information. Willing to exploit known vulnerabilities.</p>  |

Figure 6: Adversary Threat Tiers

If the acquisition program is dependent on DoD intelligence (also known as Intelligence Mission Data [IMD]) for programming platform mission systems in development, testing, operations, and sustainment, then the program requires a Lifecycle Mission Data Plan (LMDP). The LMDP is a statement of program needs applied throughout the lifecycle; it is key to identifying gaps in mission -critical IMD prior to system deployment.



Cybersecurity  
Advisory

## Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments

**Executive Summary**

Since at least 2018, the Russian Foreign Intelligence Service (SVR) has been conducting a global brute force campaign to compromise enterprise and cloud environments. This brute force campaign includes the use of a variety of tools, including enterprise and cloud environments, to gain access to sensitive information. The campaign is ongoing and is expected to continue for some time.

**Technical Details**

The actors also used misconfiguration to support multi-factor authentication and to gain access to sensitive information.

NSA's Top Ten Cybersecurity  
Mitigation Strategies

March 2018

NSA's Top Ten Mitigation Strategies counter a broad range of exploitation techniques used by Advanced Persistent Threat (APT) actors. NSA's mitigations set priorities for enterprise organizations to minimize mission impact. The mitigations also build upon the NIST Cybersecurity Framework functions to manage cybersecurity risk and promote a defense-in-depth security posture. The mitigation strategies are ranked by effectiveness against known APT tactics. Additional strategies and best practices will be required to mitigate the occurrence of new tactics.

The cybersecurity functions are keyed as: ■ Identify, ■ Protect, ■ Detect, ■ Respond, ■ Recover

- 1. Update and Upgrade Software Immediately** ■ Identify, ■ Protect
 

Apply all available software updates, automate the process to the extent possible, and use an update service provided directly from the vendor. Automation is necessary because threat actors study patches and create exploits, often soon after a patch is released. These "N-day" exploits can be as damaging as a zero-day. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to assure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender's patch cycle.
- 2. Defend Privileges and Accounts** ■ Identify, ■ Protect
 

Assign privileges based on risk exposure and as required to maintain operations. Use a Privileged Access Management (PAM) solution to automate credential management and fine-grained access control. Another way to manage privilege is through tiered administrative access in which each higher tier provides additional access, but is limited to fewer personnel. Create procedures to securely reset credentials (e.g., passwords, tokens, tickets). Privileged accounts and services must be controlled because threat actors continue to target administrator credentials to access high-value assets, and to move laterally through the network.
- 3. Enforce Signed Software Execution Policies** ■ Protect, ■ Detect
 

Use a modern operating system that enforces signed software execution policies for scripts, executables, device drivers, and system firmware. Maintain a list of trusted certificates to prevent and detect the use and injection of illegitimate executables. Execution policies, when used in conjunction with a secure boot capability, can assure system integrity. Application Whitelisting should be used with signed software execution policies to provide greater control. Allowing unsigned software enables threat actors to gain a foothold and establish persistence through embedded malicious code.
- 4. Exercise a System Recovery Plan** ■ Identify, ■ Respond, ■ Recover
 

Create, review, and exercise a system recovery plan to ensure the restoration of data as part of a comprehensive disaster recovery strategy. The plan must protect critical data, configurations, and logs to ensure continuity of operations due to unexpected events. For additional protection, backups should be encrypted, stored offsite, offline when possible, and support complete recovery and reconstitution of systems and devices. Perform periodic testing and evaluate the backup plan. Update the plan as necessary to accommodate the ever-changing network environment. A recovery plan is a necessary mitigation for natural disasters as well as malicious threats including ransomware.
- 5. Actively Manage Systems and Configurations** ■ Identify, ■ Protect
 

Take inventory of network devices and software. Remove unwanted, unneeded or unexpected hardware and software from the network. Starting from a known baseline reduces the attack surface and establishes control of the operational environment. Thereafter, actively manage devices, applications, operating systems, and security configurations. Active enterprise management ensures that systems can adapt to dynamic threat environments while scaling and streamlining administrative operations.

Content classification derived from Government Accountability Office (GAO) analysis of DoD information, GAO-19-128; and NSA/CISA/DOJ Cyber Security Advisories, April-July 2021. The nation listed is just one example of capability levels. Check with your IC representative to determine the cyber ATT of the expected adversaries.

Figure 7: Unclassified Adversary Cyber Threat Advisories

### 8.3 Step 3 – Cyber Dependency Level (CDL)

Cyber dependency is defined by its degree of connectivity, technical exposure (origin, export, open system architecture), and operational requirements. The CDL can be determined using various methods. All combinations of connectivity and technical exposure are not mapped to a specific CDL (e.g., extreme access, restricted exposure); when such situations are encountered, the requirement sponsor should identify their CDL using one of the methods described here. Criticality analysis provides a basis for intrinsic cyber survivability assessment of Mission Critical Functions (MCF), Critical Components (CC), and Critical Program Information (CPI) exchanges, going beyond an assessment of C, I, A:

- Cyber is digital, 0 or 1; it does not degrade on a continuous analog scale.
- Unrealistic to expect to maintain, or restore, 100% of a system's (cyber) functions.
- What system functionality must be sustained (to complete mission or safely return to base for restoral to a known good condition), and what are its cyber dependencies and cyber threshold requirements?



*Figure 8: Cyber Criticality Analysis*

A system's cyber dependence is the degree to which the mission critical functions of move (sustaining flight or maneuverability), shoot (performing offensive and defensive activities of its mission), and communicate (communications needed to accomplish its mission) require cyberspace.

- Technical exposure (origin, export, system architecture) combines with degree of connectivity (based on operational requirements) to define a system's CDL
- Criticality analysis provides basis for intrinsic cyber survivability assessment of critical functions, components and information exchanges -- beyond C, I, A
- Cyber dependence is the degree to which the mission critical functions (move, shoot, and communicate) require cyberspace. Cyber Dependence is based upon the intrinsic cyber survivability risks associated with performing its mission critical functions of move, shoot, and communicate

The degree of connectivity required, and the associated technical exposure, is categorized in figure 9.

**Technical Exposure + Degree of Connectivity/Dependence = CDL**

| Technical Exposure   | Degree of Connectivity & Dependence<br>(Operational requirements for internal & external information exchange)   | CDL Level    |
|--|--|--------------|
| <b>Broad</b>   | <b>Extreme</b> - Systems are entirely dependent on cyber connectivity and functionality, reliant on other systems, and will likely not function at all without full, high-bandwidth wired and wireless network support. e.g., Artificial Intelligence / Machine Learning (automated response) HW/FW/SW, unmanned vehicle, “uninterrupted” comms over networks, with no human in the loop (e.g., robotic/autonomous system) | <b>CDL 5</b> |
| <b>Limited</b>   | <b>High</b> - Systems are dependent on cyber connectivity and functionality, but are able to function to a limited extent with intermittent or low-bandwidth wired and wireless network support. e.g., AI/ML (human in the loop, with non-automated response)  | <b>CDL 4</b> |
| <b>Restricted</b>  | <b>Moderate</b> - Systems are somewhat dependent on cyber connectivity and functionality, but can operate effectively with intermittent or low-bandwidth wired and wireless network support.   | <b>CDL 3</b> |
| <b>Narrow</b>  | <b>Low</b> - Systems have little dependence on cyber connectivity and functionality, and can operate effectively for long periods without wireless network support.  | <b>CDL 2</b> |
| <b>Narrow to None</b>  | <b>Very Low</b> - Systems have no external communication requirements during operations, and can operate effectively with no network support.  | <b>CDL 1</b> |
| <b>None</b>  | <b>No Cyber Dependence</b> - No electronic sensors, no electronic processing/storage, and no internal/external information exchange requirements   | <b>CDL 0</b> |
| <b>Technical Exposure (origin, export, sys architecture) combined with Degree of Connectivity (based on operational requirements) define a system’s Cyber Dependency Level</b> |  |              |

*Figure 9: Cyber Dependency Levels*

**Degree of Connectivity** – The methods in which the system is engineered to integrate its internal electronic architecture with external support systems. The following examples of technical risk should be considered, but may not apply to every capability. In addition, there may be other risk considerations based on the operational requirement. Critical mission functionality (move, shoot, communicate) must be segregated from all others to complete a mission or return to base, to be recovered to a known good condition to fight another day. Another connectivity consideration is that when weapon systems return to installations, the supporting infrastructure may have control systems with integrated connectivity to those weapon systems. The supporting installation infrastructure supports the mission, and needs to be considered from a system engineering perspective.

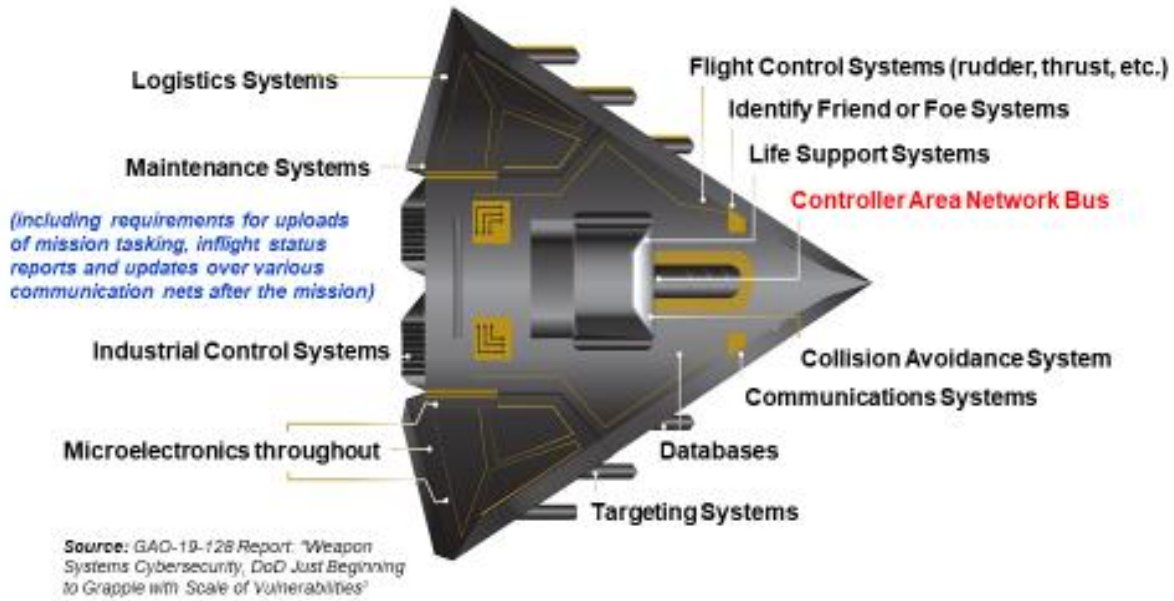


Figure 10: Degree of Connectivity and Operational Requirements

#### Internal Connectivity:

- What connectivity is required to support the internal information exchange requirements between system components (fire control (engage), propulsion, position/navigation/timing, self-protection (non-kinetic and kinetic), target search and acquisition (find/fix), target tracking (track), common operating tactical picture, battle damage assessment, etc.)?
- What is the required frequency of internal connectivity between components (always connected to support information system, on-receive (subscribe to) pushed data, on-demand (mission support data), once-per-mission data transfer)?
- How does data move between these components (Controller Area Network Bus, Local Interconnect Network, Media Oriented System Transport, FlexRay, wireless, etc.)?
- Are technical interfaces sufficiently hardened and monitored for anomalies to prevent adversary lateral movement or cross-component events and effects?

#### External Connectivity:

- What external connectivity is required to support the system's internal information requirements?
- What are the external network connectivity/transmission requirements (open/commercial internet, commercial satellite communications (SATCOM), INMARSAT, Multifunctional Information Distribution System, Joint Link-16/Link-11, Global Positioning System (GPS), NIPRNet, Secret Internet Protocol Router Network (SIPRNet), military SATCOM, Special Access Program (SAP)/ Joint Worldwide Intelligence Communication System (JWICS), cross-domain data transfer to/from those networks, etc.)?
- What system function requirements are performed remotely (mission updates, mission planning, pre-mission data uploads, post-mission data downloads, mission analysis, system maintenance, fire control (engage), propulsion, position/ navigation/timing, self-protection (non-kinetic), self-protection (kinetic),

target search and acquisition (find/fix), target tracking (track), common operating tactical picture, battle damage assessment, etc.)?

- What frequency of external connectivity (always connected to support information system, on-receive (subscribe) to pushed data, on-demand (mission support data), per-mission data transfer)?
- What types of enclaves make up the external architecture of the system (Command, Control, Communication, Computers and Intelligence (C4I); Combat Systems; Mission Package; Facilities; Control Systems; development/maintenance network)?
- How does data move between enclaves (satellite, landline, radio, WiFi, Bluetooth, etc.)?
- Are external network interfaces sufficiently hardened and monitored for anomalies to prevent adversary lateral movement or events and effects between enclaves?
- What is the strength and type of encryption used (none, commercial, allied crypto, US-only crypto)?

**Technical Exposure** – The adversary’s understanding of, and access to, the system’s hardware and software intellectual property will enable them to identify and exploit vulnerabilities.

- Has the Requirement Sponsor requested a Multi-Discipline Counter-Intelligence Threat Assessment for counter-intel products in accordance with DoDI O-5240.24?
- How much is known of the system (vulnerabilities, open architecture, open standards, purpose or proprietary characteristics, etc.)?
- What is the origin of the system’s technology (non-US production, other allies, Five Eyes, production partnerships, etc.)?
- Has the technology been exported to coalition partners, allies, Five Eyes, or other?
- Have US-specific manuals been released, or compromised?
- Has there been a Defense Intelligence Agency SCRM Threat Analysis Center (SCRM TAC) assessment performed on the system? Supply chain assessments should include analyses for critical components, parts, subsystems, systems, and support infrastructure (down to chip-level where possible), and information on foreign ownership or influence, once likely suppliers of those components are known.
- Are there known collection attempts or supply chain threats against the technology or against technologies similar to it? Are there known exfiltrations, or threat R&D efforts?
- Are there any high-confidence efforts known to have developed a countermeasure to impact the C, I, A of the capability?
- Have any potential adversaries demonstrated the ability, or the intent, to use such a capability?

### 8.4 Step 4 – Impact Level of System Loss or Compromise (IL)

What is the CCMD’s mission and OPLAN impact if a weapon system’s critical functions (move, shoot, communicate) are cyber-compromised? The next step is to determine the impact of cyber compromise to:

- the mission that the system executes or supports;
- to the system itself and its functions; and
- to the information that the system produces, uses, stores, or shares.

The Impact Levels rely on CNSSI 1253, as well as Protection Failure Criticality Analysis levels as defined in the Program Protection Plan. For more information on Criticality Analysis, see the Annotated References section. CNSSI 1253 defines three security objectives for information and information systems as C, I, A:

- A loss of **confidentiality** is the unauthorized disclosure of information.
- A loss of **integrity** is the unauthorized modification or destruction of information.
- A loss of **availability** is the disruption of access to or use of information or an information system.

The impact level of system compromise is the consequence of the failure of C, I, A on the system’s ability to perform its mission. Below are factors related to C, I, A that should be considered when determining the impact level of system loss or compromise.

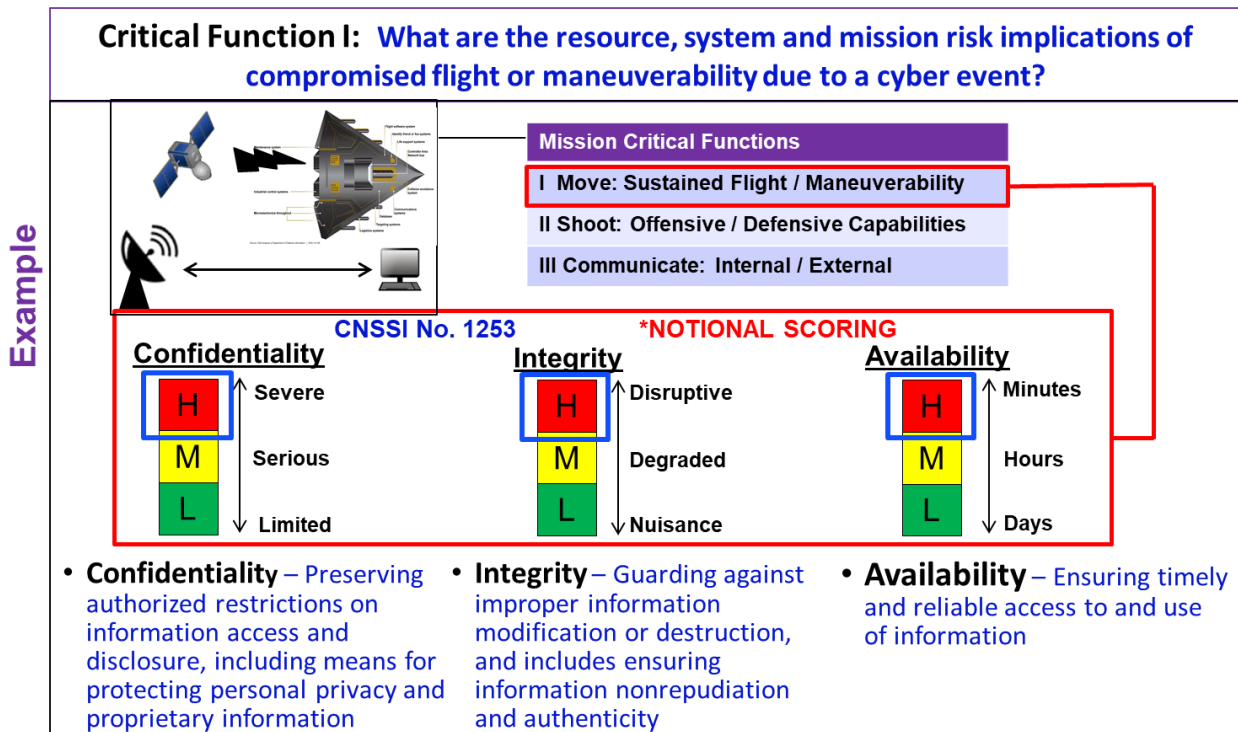


Figure 11: Impact Levels and Criticality Analysis Using CNSSI No. 1253 Security Categorization

Overall mission Impact Level (IL) of system loss or compromise of system confidentiality, integrity and/or availability would have \_\_\_\_\_ adverse effect on the capability. The C, I, A factor questions below will assist in determining the mission impact level (above):

|  |
|--|
| <p><b>IL 5: Catastrophic</b> – Catastrophic effects on National objectives or severe adverse effects on mission accomplishment of multiple CCMDs, and on Services or Allies’ assets / personnel, resulting in complete mission failure with few, if any, mission objectives accomplished, and likely heavy friendly force losses.</p>  |
| <p><b>IL 4: Severe</b> – Severe adverse effect on CCMD mission accomplishment, on CCMDs, Services or Allies assets or personnel, resulting in seriously degraded mission performance leaving some mission objectives unaccomplished and endangering friendly forces. A severe or catastrophic adverse effect means that the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration so that the CCMDs, Services or Allies are not able to perform one or more primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals, involving loss of life or serious life-threatening injuries.</p>                |
| <p><b>IL 3: Moderate</b> – Serious adverse effect on CCMD mission accomplishment and on CCMDs, Services or Allies assets or personnel, resulting in partially degraded mission performance, requiring more time/resources to accomplish mission objectives and endangering friendly forces. The threat event might: (i) cause a significant degradation in mission capability to an extent and duration that if the CCMDs, Services or Allies are able to perform its primary functions, the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in harm to individuals that does not involve loss of life or serious life-threatening injuries.</p> |
| <p><b>IL 2: Limited</b> – Limited adverse effect on CCMDs mission accomplishment, on CCMDs, Services or Allies’ assets or personnel. The threat event might: (i) cause a degradation in mission capability to an extent and duration the CCMDs, Services or Allies are able to perform its primary functions, but effectiveness of functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.</p>   |
| <p><b>IL 1: Negligible</b> – Negligible adverse effect on CCMDs mission accomplishment, and would likely not endanger CCMDs, Services or Allies’ assets or personnel.</p>  |

Figure 12: Impact Levels of System Loss or Compromise

**Confidentiality Factors**

- What is the impact of adversary use of the unauthorized disclosure of system information to do harm to the mission of the system?
- What is the impact to broader National Security, DoD, or other communities of interest/ stakeholders from unauthorized disclosure or dissemination of elements of the information type, to include violation of laws, Executive Orders, or agency regulations, or other trusts for information sharing restriction?

**Integrity Factors**

- What is the impact of adversary/unauthorized modification or destruction of system information, or functions to the mission?
- What is the impact to broader National Security, DoD, or other communities of interest/stakeholders from unauthorized modification or destruction of system information or functions, to include violation of laws, Executive Orders, or agency regulations, or other impacts on their ability to trust in the integrity of the system?

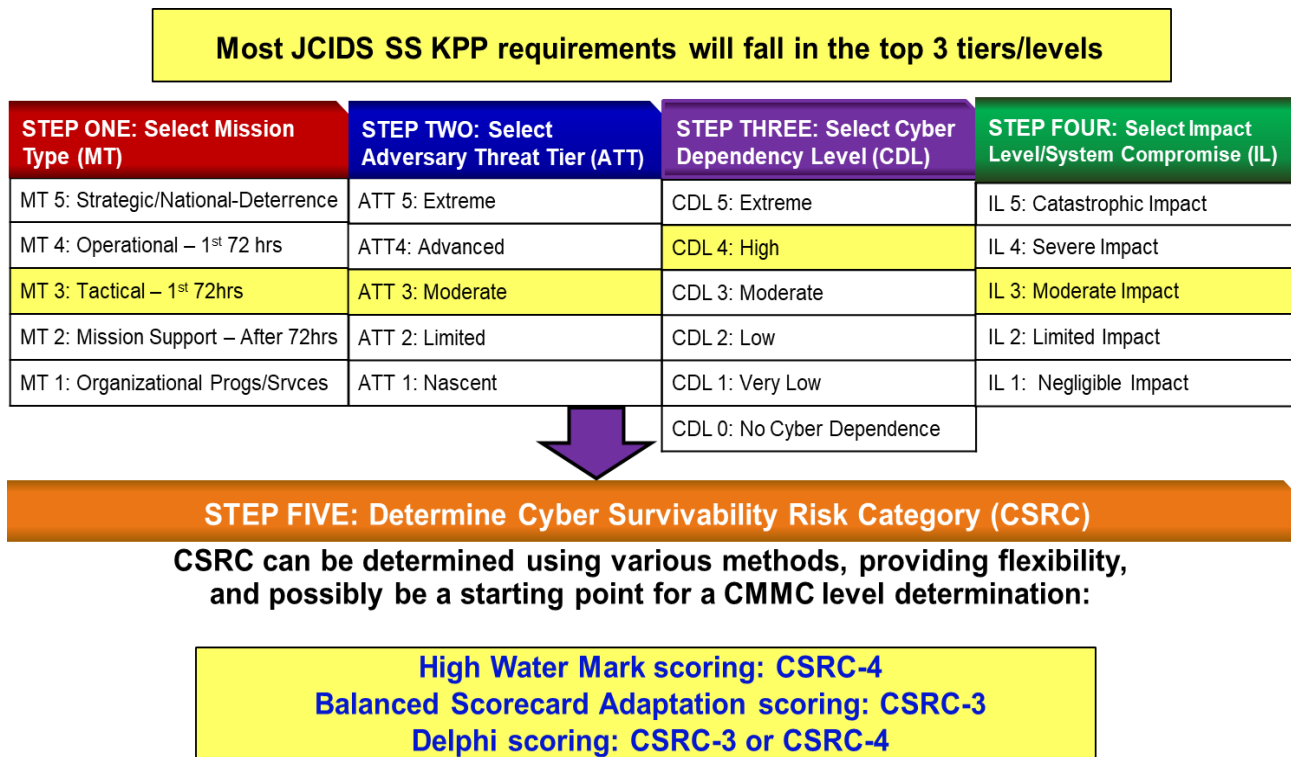
**Availability Factors**

- What is the impact of adversary disruption of our access to/use of system information, or functions to the mission?
- What portion of system-level operational availability is allocated to cyber subsystems?
- What is the impact to broader National Security, DoD, or other communities of interest/stakeholders from denial, disruption, or damage to system information or functions, to include DoD’s ability to meet requirements of laws, Executive Orders, or agency regulations, or on impact to their missions from the denial, disruption, or damage of our system, on which they may rely?

### 8.5 Step 5 – Determine the Cyber Survivability Risk Category of the System

Figure 13 illustrates the process by which the requirements document sponsor can use MT, ATT, CDL and IL to determine the CSRC. The requirements sponsor can leverage expertise across DoD, from the Joint Staff, DoD CIO, NSA, and Program Executive Offices, throughout this process.

The CSRC can be determined using various scoring methods. These methods are discussed in section 8.6.1 and the following. The process is more important than exactness; understanding the risk, assessing the resource/system risk implications, and defining cyber threshold performance requirements for operational risk trade-space decisions are the most critical.



*Figure 13: Determining the Cyber Survivability Risk Category*

The CSRC leads to the use of an integrated cyber threat and cyber requirements exemplar statement for the ICD and AoA guidance. It also helps define a consistent understanding of the level of cyber survivability required during development, testing and operations.

The CSRC, and the selected CSAs, provide a foundation for developing system security requirements and architecture. Early consideration of CSAs in a system requirements analysis and design provides the System Security Engineer with options to determine decisions prior to establishing the solution architectures. This maximizes the trade-space available for cyber survivability solutions, which is necessary to achieve system survivability within identified priorities and constraints.



|   |
|---|
| <b>CSRC 5: Extreme</b> - Same as CSRC-4 below, except include specific ATT 5 level threats and mitigations.   |
| <b>CSRC 4: Very High</b> - System must implement best available mitigations to prevent/mitigate effects of cyber-events to maintain a minimum functionality to complete the mission or recover/adapt to fight another day. Implement NSA's Top 10 Cybersecurity mitigations to ensure Confidentiality, Integrity, & Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; DoD-developed cyber protections (including protections inherited from the operational environment); and as required specific custom protections to actively manage the system's configuration to achieve and maintain an operationally-relevant CSRP. Quarterly request classified adversary specific cyber threat updates for the system and its HW/SW/FW by version number integrated into each supported capability release, to develop POA&Ms for continuously mitigating the greatest system risks and achieving/maintaining an operationally relevant CSRP. See NSA.GOV for updated unclassified ATT 4 level mitigation recommendations.   |
| <b>CSRC 3: High</b> - System must implement mitigations to prevent/mitigate effects of cyber events, to maintain a minimum functionality to complete the mission or recover/adapt to fight another day. Implement NSA's Top 10 Cybersecurity Mitigations to ensure Confidentiality, Integrity, & Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; DoD-developed cyber protections (including protections inherited from the operational environment); and as required specific custom protections to actively manage the system's configuration to achieve and maintain an operationally-relevant CSRP. Quarterly request classified adversary specific cyber threat updates for the system and HW/SW/FW by version # integrated into each supported capability release, to develop POA&Ms for continuously mitigating greatest system risks and achieving/maintaining operationally relevant CSRP. See NSA.GOV for Cybersecurity Advisories with latest unclassified ATT-3 level threat and recommended mitigations. |
| <b>CSRC 2: Moderate</b> - Mitigations include both COTS and GOTS best practices, including DoD-specific threat signatures, layered defenses, TTPs and selective DoD technologies. Implement NSA's Top 10 cyber mitigations.   |
| <b>CSRC 1: Low</b> - Mitigations include COTS with best practices (if commercially hosted), or strong DoD layered defenses and possible use of DoD technology (if DoD-hosted). As appropriate, implement NSA's Top 10 cyber mitigations.  |
| <b>CSRC 0: None</b> - No info exchange, no HW/SW/FW processing/sensors, no wired/wireless network connections.  |

*Figure 14: Cyber Survivability Risk Categories*

The CSRC provides a consistent understanding of the level of requirements during design, testing, and operations.

CSE exemplar statements incorporate the projected cyber threat based on a CSRC level assessment. Selecting a CSRC aims to assess the overall risk to the system from the capabilities of the cyber threat actor, to allow for mitigation of unacceptably high risk. The selection recognizes that programs may need to implement multiple or differentiated trust domains within the system, and include some stronger protections, by trust domain, for different subsystems, functions, or information.

As each factor is considered, some systems (and their MCF, as defined in CNSSI 4009) will intuitively fit into a particular CSRC. The mission type of a system may automatically drive the level of Threat Tier adversary anticipated and the corresponding CSRC, due to the impact to mission and if the system's C, I, A can be compromised. Even if a Strategic/National system has a CDL of 2, MT of 5, IL of 4, and ATT of 5, it could still drive a CSRC of 5, and the highest strength of cyber survivability requirements.

At the other end of the scale, systems at a lower level of mission criticality may have different results. An Organizational Support system's CDL of 4, MT of 1, IL of 1, and ATT of 1, could drive a CSRC of 1, and a strength of cybersecurity requirements that could be sufficiently supported by COTS/GOTS products and services, and good cyber practices. A CDL of 0 would lead to a CSRC of 0.

Some systems may require greater analysis for a balanced, risk-based determination of the CSRC, to ensure that the system can support the mission in a cyber-contested environment. Additional concepts discussed below can assist the requirement sponsor in determining the system's CSRC.

## 8.6 – CSA Selection based on the CSRC

CSAs are traceable to the SS KPP pillars of Prevent, Mitigate, Recover, and Adapt. The CSAs are intended to be decomposed to justify engineering-in cybersecurity and cyber resiliency requirements, with appropriate levels of strength of implementation, to ensure the resulting system can be cyber-survivable in its intended operational environment. The exemplars in this guide provide requirement sponsors with a starting point for tailoring appropriate cyber survivability requirements that support acquisition process artifacts (e.g., ICD, AoA, RFP/source selection criteria, PPP/CSS, CDD, SEP, TEMP). The number and type of CSAs required to achieve an acceptable level of system survivability is primarily based upon its CSRC level; however, the system’s mission type, adversary threat tier, cyber dependence level, and impact level of system compromise can each influence specific CSA selections. The requirements embodied in the CSAs should be technology and solution-agnostic, and considered as early as possible in the program’s planning and analysis phases.

CSAs are mapped to the SS KPP pillars as depicted in Table 1 below; most CSAs primarily support just one of the SS KPP pillars, but CSA-10 supports all four pillars, and requires resourcing of an adaptive approach such as DevOps throughout the system’s lifecycle. The span of CSA-10 makes it the most critical and comprehensive CSA. It is also applicable to legacy systems that did not consider CSAs during system design, development, and testing. It and CSAs 7 through 9, co-exists well with the RMF System Level Continuous Monitoring phase of recurring, periodic monitoring of a system’s existing risk status following the issuance of an ATO. Assessing a system’s progress in mission risk analysis, prioritization, and mitigation efforts is how the system owner can quantify its cyber risk posture, for reporting to operational commanders, and effectively apply operations and sustainment funding to address the greatest risks to mission assurance. Assessing and prioritizing risk is critical for practical purposes too; there will never be enough resources to address all risks, so it makes sense to prioritize mitigating MCF vulnerability risks with the greatest impact on a CCMD’s OPLAN/Mission.

The threshold performance definitions for each CSA, including testability and measurability considerations, are listed on pages 47-48.

- **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, understand, and respond** to cyber-events, intrusions, and attacks making it through defenses; **enabling operational resiliency** (to complete the mission)
- **Recover** – Design requirements to **recover** to a known good condition after a cyber-event; at a minimum, restore partial-to-full mission capability (to fight another day)
- **Adapt** – Enables a support effort to **adapt** to changes in adversary threat and vulnerabilities, and changes in mission needs (to win this war and the next war)

| SS KPP Pillars<br>(Mandatory)                    | Cyber Survivability Attributes (CSAs)<br>(All are to be considered; tailor and implement those that are applicable)  |
|--|--|
| <b>Prevent</b>                                   | CSA 01 - Control Access  |
|  | CSA 02 - Reduce System's Cyber Detectability   |
|  | CSA 03 - Secure Transmissions and Communications   |
|  | CSA 04 - Protect System Information from Exploitation  |
|  | CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels  |
|  | CSA 06 - Minimize and Harden Cyber Attack Surfaces   |
| <b>Mitigate</b>                                  | CSA 07 - Baseline & Monitor Systems, and Detect Anomalies  |
|  | CSA 08 - Manage System Performance and Enable Cyberspace Defense   |
| <b>Recover</b>                                   | CSA 09 - Recover System Capabilities   |
| <b>Adapt for Prevent, Mitigate &amp; Recover</b> | CSA 10 - Actively Manage System's Configurations to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture; also applicable to legacy systems that did not consider CSAs during development |

*Table 1: System Survivability KPP Pillars Mapped to Cyber Survivability Attributes*

CSA exemplars in this guide provide requirement sponsors with a starting point for tailoring appropriate cyber survivability requirements throughout the acquisition process, including ICD, AoA, and CDD development. The number and type of CSAs required to achieve an acceptable level of system survivability is primarily based upon the system's CSRC level; however, the system's MT, ATT, CDL and IL can influence specific CSA selections. The requirements embodied in the CSAs should be technology and solution agnostic and should be considered as early as possible in the program's planning and analysis phases.

**8.6.1 High-Water Mark (HWM)** – within NIST SP 800-53, a concept is detailed for identifying the highest impact value for each of a system's key factors Confidentiality, Integrity and Availability (C, I, A), and protecting the overall system based upon the highest level identified for any of its multiple factors. Using this concept for the CSRC, systems would be protected at CSRC 4 if any of the cyber survivability factors (MT, ATT, CDL, IL) were 4. (The direction in CNSSI 1253 for National Security Systems to use discrete scores for C, I, A categorization and for security controls, vice HWM, does not preclude its use in determining a CSRC.) Additional information is provided in NIST SP 800-53 and CNSSI 1253.

**8.6.2 Balanced Scorecard** – this technique identifies and assesses key performance requirements and risks to system functions and information flows. It identifies what mitigations at the mission, system, and individual information flow would reduce the risk to each mission critical function to acceptable levels. This requires a mission decomposition and criticality analysis of the system, with an emphasis on assessing its Mission Critical Function requirements, information flows, and cyber dependency risks. The ensures that functional and information dependencies are considered in protecting some of the system at different levels. Additional information is available at <https://ieeexplore.ieee.org/document/1489066> and other open sources.

**8.6.3 Delphi Scoring** – originally developed by the RAND Corporation, the Delphi scoring construct leverages the collective sense of the community, leaders, and stakeholders to assess as many factors and

perspectives as useful to arrive at a judgment through 'effective use of informed intuitive judgment in long-range forecasting. In its simplest form, it solicits the opinions of experts through carefully designed questionnaires interspersed with information and opinion feedback.' Additional information is at <https://www.rand.org/pubs/papers/P3558.html>.

**8.6.4 Choice of methods** - These scoring methods are not meant to be all inclusive. Whichever method, or hybrid combination of processes or analytics is used, the sponsor leadership's risk tolerance must be considered in deciding the CSRC for the system. Another consideration is whether the capability's CSRC is lower than the ATT; if so, the resource sponsor must include a statement in the CDD that the risk of fielding the capability, with the expected ATT being greater than the capability's CSRC, is acknowledged and accepted. All known, unmitigated risks must be accepted by the capability owner, and communicated to the CCMD for assessment of the risk implication to their OPLANs and missions.

## 9.0 CSE Process Quick Start for Capability Requirement Documents

This describes the process for including CSE analysis, CSRC level, and associated requirements exemplar language in capabilities documents, AoA planning, and RFPs. The reader should be familiar with the CSEIG to more readily use this process, and should refer to the Vignette section starting on page 63 to aid in understanding how to apply the information.

### For an ICD:

- Determine MT and ATT to identify the capability's initial CSRC level. Unless the ICD includes requirements for artificial intelligence, machine learning, continuous information exchange over the internet, or unmanned/autonomous control, there will likely not be sufficient information to determine the capability's CDL until after the AoA.
- Ensure the cyber ATT is referenced in the Threat Summary section, to support the CSE requirements for intelligence cyber threat support, and to ensure threat consistency. If the requirements document is classified Secret or higher, recommend working with the IC to include more specific classified nation states' threat capabilities recommended countermeasure requirements.
- Select the CSRC exemplar statement associated with the CSRC level and place it in the ICD, along with the list of ten CSAs that must be considered during the AoA. Recommend not tailoring the CSRC exemplar statement for the ICD.

### For a CDD, IS-ICD or IS-CDD:

- Use the results of the AoA to determine the CDL and refine the CSRC level. If an assessment includes CCMD input, it can be used to help refine the IL and CSRC. Recommend tailoring the CSRC exemplar statement for a CDD, IS-ICD and IS-CDD.
- Ensure the cyber ATT, cyber CIPs, and a current VOLT report (or request for a VOLT report) are referenced in the Threat Summary section, to support the CSE requirements for intelligence cyber threat support and to ensure threat consistency. If the requirements document is classified Secret or higher, recommend working with the IC to include more specific classified nation states' threat capabilities recommended countermeasure requirements.
- Based upon the CSRC level and AoA RFIs, identify a subset of the 10 CSAs determined to be most critical to the capability's system survivability.
- As shown in the sample table on pages 46-48, add a CSA table ("Cyber Survivability Threshold and Objective Performance Requirements") into the CDD, IS-ICD and IS-CDD, and include:
  - how the CSRC was determined;
  - a tailored CSRC threat/requirements exemplar statement associated with the CSRC level; and
  - the subset of the CSAs that were identified as most critical to system survivability, and their associated development threshold values.

The table is also required for an IS-ICD, because more information is available for an IS-ICD than an ICD, and because an IS-ICD may not necessarily be followed by the creation of an IS-CDD.

## 10.0 Cyber Survivability in Capability Requirement Documents

The CSE is an evolutionary and iterative process. Table 2 illustrates how Cyber Survivability exemplar statements and CSAs should be used, and tailored, within capability requirement documents.

| Capability Requirement Document      | CSRC Exemplar Statements   | Cyber Threat  | CSA Exemplar Statements   |
|--------------------------------------|--|---|---|
| ICD                                  | Appropriate CSRC exemplar, with <u>list</u> of CSAs at the end, to be directly inserted or tailored. | Adversary Threat Tier needs to be identified, stated in the Threat Summary section, and an initial cyber threat and requirements statement needs to be integrated within the ICD's CSRC statement.  | List of CSA titles by SS KPP pillar at the end of the CSRC statement. CSA table and exemplars are not required for ICD.   |
| IS-ICD                               | Appropriate CSRC exemplar should be inserted/ tailored.  | Adversary Threat Tier needs to be identified, stated in the Threat Summary section, and an initial cyber threat and requirements need to be integrated within the ICD's CSRC statement.   | CSA table must identify a subset of the CSAs, which should be tailored for the system-specific implementation. CSAs must be used to support creation of measurable and testable requirements in the intended operational environment, are reusable as source selection criteria, support DT&E system verification and operational assessment of cyber survivability requirements.                         |
| CDD<br>(including CDD updates)       | Appropriate CSRC exemplar should be inserted/ tailored.  | Development-specific cyber threat information needs to be included within the CDD Requirements and stated in the Threat Summary section, based on the Defense Intelligence Threat Library and other DIA, Service or commercial intelligence generated threat assessments. | CSA table must identify a subset of the CSAs, which should be tailored for the system-specific implementation and updated cyber threat. CSAs must be used to support creation of measurable and testable requirements in the intended operational environment, be reusable as source selection criteria, support DT&E system verification and operational assessment of cyber survivability requirements. |
| IS-CDD<br>(including IS-CDD updates) | Appropriate CSRC exemplar should be inserted/ tailored.  | Development-specific cyber threat information needs to be included within the CDD Requirements and stated in the Threat Summary section, based on the Defense Intelligence Threat Library and other DIA, Service or commercial intelligence generated threat assessments. | CSA table must identify a subset of the CSAs, which should be tailored for the system-specific implementation and updated cyber threat. CSAs must be used to support creation of measurable and testable requirements in the intended operational environment, be reusable as source selection criteria, support DT&E system verification and operational assessment of cyber survivability requirements. |

**Table 2: CSE Iterative Approach in Capability Requirement Documents**

The following is a sample table, numbered “5.1” in accordance with JCIDS requirements documents nomenclature, showing the CSRC rationale, threat/requirements summary, and the subset of CSAs, with threshold and objective requirements. The CSRC and CSA exemplars should be tailored to reflect the system’s characteristics. For an ICD, the threat/requirements summary exemplar language is followed by a list of CSAs by pillar, that must be considered during the AoA/CBA, to help avoid recommending flawed capability solutions. For all other documents, the exemplar language is followed by the CSA table, with the subset of the ten CSAs that have been determined to be critical for the system’s survivability, tailored to define the capability’s threshold requirements. It can be copied from this guide and pasted into the IS-ICD, CDD or IS-CDD.

**(U) Table 5.1 - Cyber Survivability Attribute (CSA) Threshold and Objective Requirements**

*[sample table for a JCIDS CDD with CSRC of 4]*

|                       |  |
|-----------------------|--|
| <b>CSRC Rationale</b> | <p><b>(U) CSRC Rationale:</b> The system’s Cyber Survivability Risk Category (CSRC) level 4 was determined by assessing its Mission Type (MT) of 3, Adversary Threat Tier (ATT) of 4, Cyber Dependency Level (CDL) of 4 and Impact Level (IL) of system compromise of 3.</p>   |
| <b>CSRC Summary</b>   | <p><b>(U) CSRC 4 Summary:</b> The system’s mission criticality and impact of system compromise requires the capability must survive and operate in an advanced cyber-contested environment (e.g., Russia GRU, APT-28, China APT-41). This level of adversaries uses detailed target technical knowledge to conduct complex, long-term cyber-attack operations combining multiple intelligence sources to obtain access to high-value networks. After gaining access, they combine well known TTPs to move laterally, evade defenses and collect additional info (e.g., widespread, distributed and anonymized ‘brute force’ attacks on cloud services). Recognizing this cyber threat will increase and eventually gain access to even greater capabilities, the system must implement best available mitigations to “prevent/mitigate” effects of cyber-events to maintain a minimum functionality to complete the mission, and “recover/adapt” to fight another day, including: implement NSA’s Top 10 Cybersecurity Mitigations to ensure Confidentiality, Integrity, &amp; Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; DoD-developed cyber protections, including protections inherited from the operational environment; and as required, specific custom protections to actively manage the system’s configuration to achieve and maintain an operationally-relevant cyber risk posture.</p> <p><b>(U) System Survivability Critical CSAs:</b> The following subset of the 10 CSAs in the table below have been determined to be most critical for (capability’s name) cyber survivability, and should drive development of the RFP and Source Selection Criteria. These CSAs have been tailored to define the capability’s threshold requirements, with CSA-10 enabling adaptive, incremental improvements for countering advances in adversary capabilities, and newly identified vulnerabilities, to maintain an operationally relevant cyber risk posture:</p> <p>[Unless otherwise stated, CSAs are threshold performance requirements to prevent, mitigate, recover from and adapt to cyber-events. The CSAs are sufficiently detailed to be support creation of measureable and testable requirements, but not so detailed as to limit the ability of system security engineers to meet indirect and implied requirements for other system functionality. With modification, these CSAs also lend themselves to be used as source selection criteria.]</p> |

|         | Cyber Survivability Attribute (CSA)  | Developmental Threshold   | Objective  |
|---------|--|---|------------|
| Prevent | <b>CSA-01 – Control Access</b>   | (U) “System shall only allow identified, authenticated, and authorized persons and non-person entities (including all assigned cyber defenders and their tools) access or interconnection to system or sub-system elements. The capability shall enforce a validation mechanism to protect the C, I, A of system resources (e.g., memory, files, interfaces, logical networks). The system shall employ anti-tamper measures that include features for protection of critical system components, information technologies, and maintenance of technology/program protection. Physical access to the system shall also be controlled.” | <b>T=O</b> |
| Prevent | <b>CSA-02 – Reduce System’s Cyber Detectability</b>  | (U) “System survivability requires signaling and communications (both wired and wireless) implemented by the system (or state “supported by system/capability”) shall minimize the ability of an adversary to monitor and/or target system and/or supported DoD weapon systems through its emanations, which may include deception.”  | <b>T=O</b> |
| Prevent | <b>CSA-03 – Secure Transmissions and Communications</b>  | (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.” [if a National Security System, add: “System shall develop, coordinate and maintain a System TRANSEC Plan (STP) and a Key Management Plan throughout the system’s lifecycle.”]  | <b>T=O</b> |
| Prevent | <b>CSA-04 – Protect System’s Information from Exploitation</b>                                   | (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).”  | <b>T=O</b> |
| Prevent | <b>CSA-05 – Partition and Ensure Critical Functions at Mission Completion Performance Levels</b> | (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.”   | <b>T=O</b> |



|          |   |   |            |
|----------|---|---|------------|
| Prevent  | <b>CSA-06 – Minimize and Harden Attack Surfaces</b>                     | (U) “System shall automatically disable all unauthorized ports, protocols, and services (PPS), including access points, by default. Open PPS should be filtered, to the greatest extent practical, so as to block communication to/from the system by unauthorized parties. 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.”  | <b>T=O</b> |
| Mitigate | <b>CSA-07 – Baseline &amp; Monitor Systems and Detect Anomalies</b>     | (U) “System shall implement and maintain a cyber survivability configuration baseline for its GOTS/COTS HW, SW, FW and open source modules, by version number, to ensure an operationally acceptable cyber risk posture 24/7 (note: drives CDRLs). System shall monitor, detect and report system health status and anomalies indicative of cyber events, based on its current adversary cyber threat intelligence, CONOPS and Mission Relevant Terrain in Cyberspace (MRT-C). Applicable report detail shall be provided to users, system operators and assigned cyber defenders (e.g., system shall report anomalies such as configuration changes, cyber-related event indicators, slowed processing, or loss of functionality within T = (# of seconds/minutes) [specified by sponsor]).” | <b>T=O</b> |
| Mitigate | <b>CSA-08 – Manage System Performance and Enable Cyberspace Defense</b> | (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. The system shall enable assigned cyber defenders to impose effects on adversaries to counter their operations and objectives. Alternatively, the mission commander shall be able to selectively disconnect/disable subsystems that are not critical as well as isolate the system from integrated platform systems and/or Department of Defense Information Network (DoDIN).”              | <b>T=O</b> |
| Recover  | <b>CSA-09 – Recover System Capabilities</b>                             | (U) “After a cyber-event, the system shall be capable of being restored to full functionality from a trusted source; at a minimum, being restored to partial mission capability, between mission cycles or within xx hours [specified by sponsor], to fight another day. System recovery shall prioritize cyber operational resiliency functions.”  | <b>T=O</b> |

|  |   |  |                   |
|--|---|--|-------------------|
| <p style="writing-mode: vertical-rl; transform: rotate(180deg);">Adapt: Supports All 3 Pillars</p> | <p><b>CSA-10 – Actively Manage System’s Configurations to Achieve and Maintain an Operationally-relevant Cyber Risk Posture</b></p> | <p>(U) “Throughout a system’s lifecycle and within one standard mission cycle of <b>xx hours [specified by sponsor]</b> of identification of a drop in cyber risk posture below its commensurate CSRC level, the system shall have a configuration management process, supported by automated capabilities and technology refresh options, to achieve and continuously maintain an objectively assessed and operationally-relevant risk posture. The process shall include inputs from operators, defenders and intel analysts to continuously assess changes in adversary threat, and include a machine readable Bill of Materials (BOM) of the system’s GOTS/COTS HW, SW, FW and open source modules for a supply chain risk assessment prior to each milestone decision and supported release. The process shall determine the sufficiency of system cyber survivability, and support a DevOps framework to prioritize vulnerability mitigation and remediation in the system and connected infrastructure with greatest mission risks.” (note: drives CDRLs)</p> | <p><b>T=O</b></p> |
|--|---|--|-------------------|

## 11.0 ICD and CDD Exemplar Language for each Cyber Survivability Risk Category

The following CSRC exemplar language sections include integrated adversary cyber threat and cyber countermeasure requirements statements for all ICDs, before a system-specific and technology-specific threat assessment can be made to further define cyber survivability requirements, and for all IS-ICDs, CDDs and IS-CDDs, which will include evaluation of all the CSRC factors. The following statements may appear similar or repetitive, but they progressively elaborate upon unclassified adversary threat capabilities and applicable cyber survivability requirements. These statements can be used as-is within ICDs, but they should be tailored and refined in the draft CDD at Milestone A, in the validated CDD at the development's RFP decision point, and in CDD updates at Milestone C or beyond.

- Fundamental to the CSE construct is enabling a requirement sponsor to select and articulate CSA choices to achieve each SS KPP pillar. If the ICD effectively introduces the cyber survivability requirements, then there is a greater likelihood of identifying a preferred solution that meets requirements and including sufficient cybersecurity to enable the capability to be cyber survivable, commensurate with a risk-managed approach to countering a capable and determined adversary.
- Although not all CSAs are applicable to all requirements, ICDs must list all ten CSAs at the end of the CSRC exemplar statement to ensure they are considered for applicability during a program's AoA, CBA, or analogous process. This helps to ensure an understanding of the intrinsic cyber capabilities and risks associated with each alternative, along with the potential resource implications to mitigate unacceptable risks. Since more is known about the cyber dependencies of the technologies associated with IS-ICDs, IS-CDDs, and CDDs, these requirements documents must include an appropriate subset of the ten CSAs for the system-specific architectures and include them in the document's CSA Threshold and Objective requirements table.
- Although requirement sponsors are encouraged to tailor the CSAs, care should be taken to not over-engineer the requirements -- and instead allow the developer the ability to creatively meet the intent. They should also be written with the perspective that the CSAs can be reused:
  - By acquisition professionals to drive development of source selection criteria
  - By system engineers to support analyses and their application of cybersecurity and cyber resiliency techniques
  - By system security engineers to support implementation of specific cybersecurity controls
  - By program managers to support operational risk trade-space decisions
  - By capability owners and by testers to determine the system's as-is cyber risk posture
  - By RMF AOs to support risk acceptance decisions
  - By capability owners to feed into Combatant Commander missions' cyber risk posture

## 11.1 Cyber Survivability Risk Category 1 Exemplar Language

**[For an ICD, CDD, IS-ICD and IS-CDD] "CSRC Rationale:** The system's Cyber Survivability Risk Category (CSRC) level of 1 was determined by assessing its Mission Type (MT) of X, Adversary Threat Tier (ATT) of X, Cyber Dependency Level (CDL) of X and Impact Level (IL) of system compromise of X." These values should reflect the assessed factors that are known at the time of the document's preparation. CDL and IL are typically not known for an ICD, prior to completion of a AoA and selection of a materiel capability for development. If the capability is determined to be a CSRC 1, the requirement sponsor could tailor the following high-level cyber threat statement, and corresponding cyber countermeasure requirements statement:

**"CSRC 1 Summary Statement:** The system's mission criticality and impact of system compromise requires the capability must survive and operate in a limited cyber-contested environment. This level of expected adversaries is willing to exploit known vulnerabilities, but possess little-to-no organized cyber capabilities and no knowledge of a network's underlying systems beyond publicly connected open-source information. Recognizing this cyber threat will increase and may eventually gain access to even greater capabilities, system must implement defensive capabilities and mitigations to prevent/mitigate effects of cyber-events, to maintain a minimum functionality to complete the mission, or recover/adapt to fight another day (e.g., implement NSA's Top 10 Cybersecurity Mitigations to ensure an appropriate level of Confidentiality, Integrity, & Availability for internal and external information flows; COTS best practices (if commercially hosted) or strong DoD layered defenses and possible use of DoD technology (if DoD-hosted))."

**[For an ICD] "Cyber Survivability Attributes (CSAs) to be considered:** The following ten 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:

- 1) Prevent cyber-event effects: CSA-01: Control Access; CSA-02: Reduce System's Cyber Detectability; CSA-03: Secure Transmissions and Communications; CSA-04: Protect System Information from Exploitation; CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels; CSA-06: Minimize & Harden Attack Surfaces.
- 2) Mitigate the effects of cyber-events: CSA-07: Baseline and Monitor Systems and Detect Anomalies; CSA-08: Manage System Performance and Enable Cyberspace Defense.
- 3) Recover from the effects of cyber-events: CSA-09: Recover System Capabilities.
- 4) Support adapting to changing threats throughout the system's lifecycle: CSA-10: Actively Manage System's Configurations to Achieve and Maintain an Operationally-Relevant cyber risk posture."

**[For a CDD, IS-ICD and IS-CDD] "System Survivability Critical CSAs:** The following subset of the 10 CSAs in the table below have been determined to be most critical for *(capability's name)* cyber survivability, and should drive development of RFP and source selection criteria. These CSAs have been tailored to define the capability's threshold requirements:" (IF CSA-10 APPLIES TO THIS CAPABILITY, ADD:) "with CSA-10 enabling adaptive, incremental improvements for countering advances in adversary capabilities, and newly identified vulnerabilities, to maintain an operationally relevant cyber risk posture:"

**For CSRC 1 capabilities, requirement sponsors should specify:**

- one to three CSAs, probably all prevent CSAs;
- probably implement a replacement strategy; and
- probably no mitigate, recover or adapt CSAs

to ensure a reasoned and risk-managed approach to address the SS KPP requirements.

It is unlikely that a CSRC 1 capability will be able to implement Mitigate, Recover, and Adapt CSAs.

## 11.2 Cyber Survivability Risk Category 2 Exemplar Language

**[For an ICD, CDD, IS-ICD and IS-CDD]** **CSRC Rationale:** The system’s Cyber Survivability Risk Category (CSRC) level of 2 was determined by assessing its Mission Type (MT) of X, Adversary Threat Tier (ATT) of X, Cyber Dependency Level (CDL) of X and Impact Level (IL) of system compromise of X.” These values should reflect the assessed factors that are known at the time of the document’s preparation. CDL and IL are typically not known for an ICD, prior to completion of a AoA and selection of a materiel capability for development. If the capability is determined to be a CSRC 2, the requirement sponsor could tailor the following high-level cyber threat statement, and corresponding cyber countermeasure requirements statement:

### **CSRC 2 Summary Statement:**

“The system’s mission criticality and impact of system compromise requires the capability must survive and operate in a limited cyber-contested environment. This level of expected adversaries possesses some limited strategic planning and are capable of limited advanced cyber tradecraft, using publicly available and customized tools to exploit known and unknown vulnerabilities. Able to identify and target-for espionage or attack easily accessible unencrypted networks, running common operating systems. Recognizing this cyber threat will increase and may eventually gain access to greater capabilities, system must implement some defensive capabilities and mitigations to prevent/mitigate effects of cyber-events, to maintain a minimum functionality to complete the mission or recover/adapt to fight another day (e.g., implement NSA’s Top 10 Cybersecurity Mitigations to ensure an appropriate level of Confidentiality, Integrity, & Availability for internal and external information flows; and both COTS and GOTS best practices, including DoD specific threat signatures, layered defenses (including a defined hierarchy of assigned human defenders), TTPs and selective DoD technologies).”

**[For an ICD]** **“Cyber Survivability Attributes (CSAs) to be considered:** The following ten CSAs must be assessed for each AoA/CBA alternative to understand the resource and risk implications if the capability itself, the hosting system or enterprise services are unable to provide each CSA’s intent:

- 1) Prevent cyber-related event effects: CSA-01: Control Access; CSA-02: Reduce System’s Cyber Detectability; CSA-03: Secure Transmissions and Communications; CSA-04: Protect System Information from Exploitation; CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels; CSA-06: Minimize & Harden Attack Surfaces.
- 2) Mitigate the effects of cyber-events: CSA-07: Baseline and Monitor Systems and Detect Anomalies; CSA-08: Manage System Performance and Enable Cyberspace Defense.
- 3) Recover from the effects of cyber-events: CSA-09: Recover System Capabilities.
- 4) Support adapting to changing threats throughout the system’s lifecycle: CSA-10: Actively Manage System’s Configurations to Achieve and Maintain an Operationally-Relevant cyber risk posture.”

**[For a CDD, IS-ICD and IS-CDD]** **“System Survivability Critical CSAs:** The following subset of the 10 CSAs in the table below have been determined to be most critical for **(capability’s name)** cyber survivability, and should drive development of RFP and source selection criteria. These CSAs have been tailored to define the

capability's threshold requirements:" (IF CSA-10 APPLIES TO THIS CAPABILITY, ADD:) "with CSA-10 enabling adaptive, incremental improvements for countering advances in adversary capabilities, and newly identified vulnerabilities, to maintain an operationally relevant cyber risk posture:"

**For CSRC 2 capabilities, requirement sponsors should specify:**

- two to five CSAs;
- probably one to three Prevents;
- possibly one Mitigate and one Recover, or a replacement strategy;
- and probably no Adapt

to ensure a reasoned and risk-managed approach to address the SS KPP requirements.

### 11.3 Cyber Survivability Risk Category 3 Exemplar Language

**[For an ICD, CDD, IS-ICD and IS-CDD] "CSRC Rationale:** The system's Cyber Survivability Risk Category (CSRC) level of 3 was determined by assessing its Mission Type (MT) of X, Adversary Threat Tier (ATT) of X, Cyber Dependency Level (CDL) of X and Impact Level (IL) of system compromise of X." These values should reflect the assessed factors that are known at the time of the document's preparation; the above values are an example. CDL and IL are typically not known for an ICD, prior to completion of a AoA and selection of a materiel capability for development. If the capability is determined to be a CSRC 3, the requirement sponsor could tailor the following high-level cyber threat statement, and corresponding cyber countermeasure requirements statement:

**"CSRC 3 Summary Statement:** The system's mission criticality and impact of system compromise requires the capability must survive and operate in a moderate cyber-contested environment. This level of adversaries is sophisticated, persistent, and well-resourced nation-state actors capable of advanced cyber tradecraft to gain access to some isolated networks, create limited effects against defense critical infrastructure networks and conduct wide-ranging intelligence collection operations, using publicly available tools and internally developed customized malware. Recognizing this cyber threat will increase and may eventually gain access to even greater capabilities, system must implement defensive capabilities and mitigations to "prevent/mitigate" effects of cyber-events, to maintain a minimum functionality to complete the mission or recover/adapt to fight another day (e.g., implement NSA's Top 10 Cybersecurity Mitigations to ensure Confidentiality, Integrity, & Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; a defined hierarchy of assigned human defenders, equipped with specialized tools as needed; DoD developed cyber protections, including protections inherited from the operational environment; and as required specific custom protections to actively manage the system's configuration to achieve and maintain an operationally-relevant cyber risk posture)."

**[For an ICD] "Cyber Survivability Attributes (CSAs) to be considered:** The following ten 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:

- 1) Prevent cyber-related event effects: CSA-01: Control Access; CSA-02: Reduce System's Cyber Detectability; CSA-03: Secure Transmissions and Communications; CSA-04: Protect System Information from Exploitation; CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels; CSA-06: Minimize & Harden Attack Surfaces.
- 2) Mitigate the effects of cyber-events: CSA-07: Baseline and Monitor Systems and Detect Anomalies; CSA-08: Manage System Performance and Enable Cyberspace Defense.
- 3) Recover from the effects of cyber-events: CSA-09: Recover System Capabilities.
- 4) Support adapting to changing threats throughout the system's lifecycle: CSA-10: Actively Manage System's Configurations to Achieve and Maintain an Operationally-Relevant cyber risk posture."



**[For a CDD, IS-ICD and IS-CDD]** “**System Survivability Critical CSAs:** The following subset of the 10 CSAs in the table below have been determined to be most critical for *(capability’s name)* cyber survivability, and should drive development of RFP and source selection criteria. These CSAs have been tailored to define the capability’s threshold requirements, with CSA-10 enabling adaptive incremental improvements for countering advances in adversary capabilities, and newly identified vulnerabilities to maintain an operationally-relevant cyber risk posture:”

**For CSRC 3 capabilities, requirement sponsors should specify:**

- five to seven CSAs;
- probably two to four Prevents;
- possibly one Mitigate, one Recover; and one Adapt;
- and probably not a replacement strategy

to ensure a reasoned and risk-managed approach to address the SS KPP pillars’ requirements and to ensure mitigations are identified, implemented, patched and maintained throughout the system’s lifecycle.

## 11.4 Cyber Survivability Risk Category 4 Exemplar Language

**[For an ICD, CDD, IS-ICD and IS-CDD] "CSRC Rationale:** The system's Cyber Survivability Risk Category (CSRC) level of 4 was determined by assessing its Mission Type (MT) of X, Adversary Threat Tier (ATT) of X, Cyber Dependency Level (CDL) of X and Impact Level (IL) of system compromise of X." These values should reflect the assessed factors that are known at the time of the document's preparation. CDL and IL are typically not known for an ICD, prior to completion of a AoA and selection of a materiel capability for development. If the capability is determined to be a CSRC 4, the requirement sponsor could tailor the following high-level cyber threat statement, and corresponding cyber countermeasure requirements statement:

**[For an ICD, CDD, IS-ICD and IS-CDD] "CSRC 4 Summary Statement:** The system's mission criticality and impact of system compromise requires the capability must survive and operate in an advanced cyber-contested environment (e.g., Russia GRU, APT-28, China APT-41). This level of adversaries uses detailed target technical knowledge to conduct complex, long-term cyber-attack operations combining multiple intelligence sources to obtain access to high-value networks. After gaining access, they combine well known TTPs to move laterally, evade defenses and collect additional info (e.g., widespread, distributed and anonymized 'brute force' attacks on cloud services). Recognizing this cyber threat will increase and eventually gain access to even greater capabilities, the system must implement best available defensive capabilities and mitigations to "prevent/mitigate" effects of cyber-events to maintain a minimum functionality to complete the mission, or "recover/adapt" to fight another day (e.g., implement NSA's Top 10 Cybersecurity Mitigations to ensure Confidentiality, Integrity, & Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; a defined hierarchy of assigned human defenders, equipped with specialized tools as needed; DoD-developed cyber protections, including protections inherited from the operational environment; and as required, specific custom protections to actively manage the system's configuration to achieve and maintain an operationally-relevant cyber risk posture)."

**[For an ICD] "Cyber Survivability Attributes (CSAs) to be considered:** The following ten 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:

- 1) Prevent cyber-related event effects: CSA-01: Control Access; CSA-02: Reduce System's Cyber Detectability; CSA-03: Secure Transmissions and Communications; CSA-04: Protect System Information from Exploitation; CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels; CSA-06: Minimize & Harden Attack Surfaces.
- 2) Mitigate the effects of cyber-events: CSA-07: Baseline and Monitor Systems and Detect Anomalies; CSA-08: Manage System Performance and Enable Cyberspace Defense.
- 3) Recover from the effects of cyber-events: CSA-09: Recover System Capabilities.
- 4) Support adapting to changing threats throughout the system's lifecycle: CSA-10: Actively Manage System's Configurations to Achieve and Maintain an Operationally-Relevant cyber risk posture."

***[For a CDD, IS-ICD and IS-CDD]*** “System Survivability Critical CSAs: The following subset of the 10 CSAs in the table below have been determined to be critical for ***(capability’s name)*** cyber survivability, and should drive development of RFP and source selection criteria. These CSAs have been tailored to define the capability’s threshold requirements, with CSA-10 enabling adaptive incremental improvements for countering advances in adversary capabilities and newly identified vulnerabilities to maintain an operationally-relevant cyber risk posture:”

**For CSRC 4 capabilities, requirement sponsors should specify:**

- six to nine CSAs;
- probably three to five Prevents;
- one to two Mitigates;
- one Recover;
- and Adapt

to ensure a reasoned and risk-managed approach to address the SS KPP pillars’ requirements and to ensure mitigations are identified, implemented, patched and maintained throughout the system’s lifecycle.

## 11.5 Cyber Survivability Risk Category 5 Exemplar Language

**[For an ICD, CDD, IS-ICD and IS-CDD] "CSRC Rationale:** The system's Cyber Survivability Risk Category (CSRC) level of 5 was determined by assessing its Mission Type (MT) of X, Adversary Threat Tier (ATT) of X, Cyber Dependency Level (CDL) of X and Impact Level (IL) of system compromise of X." These values should reflect the assessed factors that are known at the time of the document's preparation. CDL and IL are typically not known for an ICD, prior to completion of a AoA and selection of a materiel capability for development. If the capability is determined to be a CSRC 5, the requirement sponsor could tailor the following high-level cyber threat statement, and corresponding cyber countermeasure requirements statement:

**[For an ICD, CDD, IS-ICD and IS-CDD] "CSRC 5 Summary Statement:** The capability's mission criticality and impact of system compromise requires the capability must survive and operate in an extreme cyber-contested environment (e.g., threatened by Russian SVR, APT-29). This level of adversaries uses a range of initial exploitation techniques that vary in sophistication, coupled with 'stealthy' intrusion tradecraft of custom tools, compromised accounts, and system misconfigurations to blend in with normal/unmonitored traffic and move undetected in victim networks for denial, degradation, deception, disruption, and destruction of mission capabilities. They have demonstrated capabilities to target cloud resources and supply chain (e.g., SolarWinds). Recognizing these cyber threats will increase, the system must implement best available defensive capabilities and mitigations to prevent/mitigate effects of cyber-events to maintain a minimum functionality to complete the mission and recover/adapt to fight another day, including: implement NSA's Top 10 Cybersecurity Mitigations to ensure Confidentiality, Integrity, & Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; a defined hierarchy of assigned human defenders, equipped with specialized tools as needed; DoD developed cyber protections, including protections inherited from the operational environment; and as required specific custom protections; to actively manage the system's configuration to achieve and maintain an operationally-relevant cyber risk posture."

**[For an ICD] "Cyber Survivability Attributes (CSAs) to be considered:** The following ten 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:

- 1) Prevent cyber-related event effects: CSA-01: Control Access; CSA-02: Reduce System's Cyber Detectability; CSA-03: Secure Transmissions and Communications; CSA-04: Protect System Information from Exploitation; CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels; CSA-06: Minimize & Harden Attack Surfaces.
- 2) Mitigate the effects of cyber-events: CSA-07: Baseline and Monitor Systems and Detect Anomalies; CSA-08: Manage System Performance and Enable Cyberspace Defense.
- 3) Recover from the effects of cyber-events: CSA-09: Recover System Capabilities.
- 4) Support adapting to changing threats throughout the system's lifecycle: CSA-10: Actively Manage System's Configurations to Achieve and Maintain an Operationally-Relevant cyber risk posture."

**[For a CDD, IS-ICD and IS-CDD]** “**System Survivability Critical CSAs:** The following subset of the 10 CSAs in the table below have been determined to be critical for *(capability’s name)* cyber survivability, and should drive development of RFP and source selection criteria. These CSAs have been tailored to define the capability’s threshold requirements, with CSA-10 enabling adaptive incremental improvements for countering advances in adversary capabilities, and newly identified vulnerabilities, to maintain an operationally-relevant cyber risk posture:”

**For CSRC 5 capabilities, requirement sponsors should specify:**

- nine to ten CSAs;
- including five to six Prevents;
- two Mitigates;
- one Recover; and
- one Adapt

to ensure a reasoned and risk managed approach to address the SS KPP pillars’ requirements and to ensure mitigations are identified, implemented, patched and maintained throughout the system’s lifecycle.

## 12.0 Cyber Survivability Requirements and Performance Measures

CSAs must be traceable with the ICD, AoA, and CDD. This will ensure that the cyber survivability requirements enable the system to operate in its anticipated cyber contested environment, and complete the mission, even if impacted by a cyber-event. Within the AoA, the CSE will ensure JCIDS ICD guidance points to the exemplar CSAs sufficiently to enable comparative measures to identify solutions that meet functional requirements and are more likely to be affordable, feasible, and cyber survivable.

Based on the ICD-identified CSRC, the study team should attempt to assess each alternative's performance degradation, recovery times for mission critical functions, and information support against specified and documented threat capabilities. These cyber survivability operational requirements, along with the expected threat, CONOPS, use cases, and Operational Mode Summary/Mission Profile (OMS/MP), inform the operational and the operational test environment, including threat, critical operational issues in the TEMP, and abuse/misuse cases in operational test plans/procedures.

For the AoA, cyber survivability requirements (as a component of the mandatory SS KPP) must be included in consideration of possible tradeoffs among life-cycle cost, schedule and performance objectives for each alternative considered, based upon the JCIDS SS KPP pillars of Prevent, Mitigate, Recover, and Adapt, and their associated CSAs. AoA guidance should include RFIs describing if/how each alternative meets the intent of each of the 10 CSAs, and if it is not necessary to ensure system survivability. To ensure that cybersecurity, survivability, and cyber resiliency analyses among the alternatives are informed on technical matters, the cyber aspects of the AoA RFIs should be supported and reviewed by, competent technical authority and/or subject matter experts from relevant organizations.

In all cases, requirement sponsors must specify an appropriate subset of CSAs to support the determined CSRC in the draft CDD.

### 13.0 Tailoring Cyber Survivability Attributes

The integrated cyber threat and survivability statement in the ICD, based on exemplar ICD language of CSRC guidance in this document, is intended to be built on and included in the draft CDD, the validated CDD, and CDD updates. At the draft CDD/TEMP stage, the CSE will provide guidance to the requirements community to ensure tailored CSAs in the draft CDD, TEMP, RFP, and source selection criteria are consistent with the ICD and the AoA recommendations, and to support a specific cyber threat assessment and cyber sufficiency status report at Milestone A.

In the CDD, the CSE will support creation of cyber threshold requirements that are sufficiently detailed to be measurable and testable. The AFRL CSA Tool provides additional assistance in developing cyber survivability performance measures, and associated cybersecurity and cyber resiliency controls. The J6 CSE team can advise any resource sponsor or program office representative on how to obtain access to the CSA Tool. The strength of implementation for the CSAs are required to be at the level that allows the system to meet the cyber survivability expectation for mission assurance for the capability's CSRC (1 through 5). Beginning with the development of the draft CDD, and continuing through the validated CDD and CDD updates, the cyber aspects of the capability documents should be supported by, and reviewed by, competent technical authority and/or subject matter experts from recognized cyber engineering authoritative sources and organizations.

The following statements provide additional details for the CSAs. The statements are recommended as written for the ICD, but need to be assessed for applicability, but should be tailored for an IS-ICD, CDD or IS-CDD. They should be traceable to the SS KPP's mandatory pillars (Prevent, Mitigate, Recover and Adapt). The CSAs are high-level and intended to provide guidance for system security engineers and program, resource, and functional sponsors to make informed decisions for technical and resource-based risk trade-space decision within the system security architecture.

The CSAs are useable as-is at the ICD and AoA level, but should be tailored starting with the draft CDD to be system-specific and to be testable, measurable, and affordable, commensurate with the system's CSRC level. The CSAs can also form the basis for RFP specifications, and for source selection criteria.

**CSA-01 – Control Access (not all inclusive or required):** “System shall only allow identified, authenticated, and authorized persons and non-person entities (including all assigned cyber defenders and their tools) access or interconnection to system or sub-system elements. The capability shall enforce a validation mechanism to protect the C, I, A of system resources (e.g., memory, files, interfaces, logical networks). The system shall employ anti-tamper measures that include features for protection of critical system components, information technologies, and maintenance of technology/program protection. Physical access to the system shall also be controlled.”

**CSA-01 Testability and measurability considerations when writing performance attribute:** Attributes that must be defined include: WHO may access the system, under WHAT conditions, from WHERE, and HOW that access can be made. For example, a high-criticality system may have limits on WHO may access it (such as only specific operators or defenders with specific clearances and read-ins) and

management of the system may also be subject to controls (such as for specific tasks), WHERE authorized people may access (such as specific administrative consoles in restricted areas) and the HOW may be also constrained (e.g., password strength, Common Access Card (CAC), token, two-person control, mandatory record keeping, cyber defender entry port). An example of a high-criticality program with these types of limits might be the Navy's Aegis Weapons System, and a low-criticality program might be the Defense Travel System.

**CSA-02 – Reduce System's Cyber Detectability (not all inclusive or required):** "System survivability requires signaling and communications (both wired and wireless) implemented by the system (or state "supported by system/capability") shall minimize the ability of an adversary to monitor and/or target system and/or supported DoD weapon systems through its emanations, which may include deception."

**CSA-02 Testability and measurability considerations when writing performance attribute:**

Attributes that must be defined include: the media in which detectability should be limited, the maximum distance/signal strength, and non-operational signature items (e.g., waste heat, sidelobe radiation, IP mapping).

**CSA-03 Secure Transmissions and Communications (not all inclusive or required):** "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."

[if a National Security System (NSS), add: "System shall develop, coordinate and maintain a System TRANSEC Plan (STP) throughout the system's lifecycle."]

**CSA-03 Testability and measurability considerations when writing performance attribute:**

Attributes that must be considered include: the level of NSA-approved encryption required, including hash strength, encryption type, waveform verification methods, wireless communications techniques, checksums, etc. Derived attributes shall comply with current DoD Cryptographic Modernization (Crypto Mod) standards. Consult the Annotated References section of this guide for current cybersecurity/cyber cryptographic modernization policy references.

**CSA-04 Protect System's Information from Exploitation (not all inclusive or required):** "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-04 Testability and measurability considerations when writing performance attribute:**

Attributes that must be defined include: requirement for encryption of data at rest, limits on system privileges, password strength requirements, use of tokens, conformance with patches and Security Technical Implementation Guides (STIGs).

**CSA-05 – Partition and Ensure Critical Functions at Mission Completion Performance Levels (not all inclusive or required):** "System partitioning shall implement technical/logical mitigations including logical and physical segmentation. The system shall be able to maintain mission critical functions



at minimum performance thresholds identified within the system's CONOPS. Compromise of non-critical functions shall not significantly impact system mission capability."

***CSA-05 Testability and measurability considerations when writing performance attribute:***

Attributes that must be defined include: degree of partitioning, segmentation and diversity (physical and logical), permissibility of cloud use for system or data, availability of war reserve modes, protection of media and removable storage. As an example to measure mission performance and related success, availability with respect to mission and systems can be used as a function of up-time and down-time.

**CSA-06 – Minimize and Harden Attack Surfaces (not all inclusive or required):** "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."

***CSA-06 Testability and measurability considerations when writing performance attribute:***

Attributes that must be defined include limits on open ports, portable media, exposure outside the assigned enclave, trusted connections for maintenance/logistics, etc.

**CSA-07 – Baseline & Monitor Systems and Detect Anomalies (not all inclusive or required):** (U) "System shall implement and maintain a cyber survivability configuration baseline for its GOTS/COTS HW, SW, FW and open source modules, by version number to ensure an operationally acceptable cyber risk posture 24/7 (note: drives CDRLs). System shall monitor, detect and report system health status and anomalies indicative of cyber events, based on its current adversary cyber threat intelligence, CONOPS and Mission Relevant Terrain in Cyberspace (MRT-C). Applicable report detail shall be provided to users, system operators and assigned cyber defenders (e.g., system shall report anomalies such as configuration changes, cyber-related event indicators, slowed processing, or loss of functionality within **T = (# of seconds/minutes) [specified by sponsor]**)."

***CSA-07 Testability and measurability considerations when writing performance attribute:***

Attributes that must be defined include: types of anomalies expected to be detected and the speed/time of detection; the means of detection and reporting (to drive CDRLs); standard for automation of these tasks; data types and information flows for elevation to assigned cyber defenders.

**CSA-08 – Manage System Performance and Enable Cyberspace Defense (not all inclusive or required):** "If anomalies are detected and/or cyber-events degrade system capability, the system shall be sufficiently resilient to mitigate cyber-related event effects through orderly, structured and prioritized system responses, in order to ensure minimum mission functionality requirements **[system functionality threshold specified by sponsor]** to complete the current mission or return for recovery. The system shall enable assigned cyber defenders to impose effects on adversaries to counter their operations and objectives. Alternatively, the mission commander shall be able to selectively disconnect/disable subsystems that are not critical as well as isolate the system from integrated platform systems and/or Department of Defense Information Network (DoDIN)."

***CSA-08 Testability and measurability considerations when writing performance attribute:***

Attributes that must be defined include: prioritization of functions to be preserved, minimum functionality, alternate capabilities to ensure minimum functionality, time to restore minimum functionality to complete the mission.

**CSA-09 – Recover System Capabilities (not all inclusive or required):** "After a cyber-event, the system shall be capable of being restored to a known good configuration from a trusted source; at a minimum, restored to partial mission capability, between mission cycles or within **xx** hours [specified by sponsor], to fight another day. System recovery shall prioritize cyber operational resiliency functions [specified by sponsor]."

***CSA-09 Testability and measurability considerations when writing performance attribute:***

Attributes that must be defined include: speed of recovery, prioritization of functions to be recovered first, quality/quantity of data/functionality required, updates to prevent newly identified risks, and capability to replace or reconfigure capabilities to mitigate new threat vectors. The time to restore mission is the minimum level of acceptable risk that a mission can afford, also directly related to down-time in the availability mission performance measure. Another metric to inform mission capability analysis is the duration (or up-time) a mission needs to perform its desired function.

**CSA-10 – Actively Manage System’s Configurations to Achieve and Maintain an Operationally-relevant Cyber Risk Posture (not all inclusive or required):**

(U) "Throughout a system’s lifecycle and within one standard mission cycle of **xx** hours [specified by sponsor] of identification of a drop in cyber risk posture below its commensurate CSRC level, the system shall have a configuration management process, supported by automated capabilities and technology refresh options, to achieve and continuously maintain an objectively assessed and operationally-relevant risk posture. The process shall include inputs from operators, defenders and intel analysts to continuously assess changes in adversary threat, and include a machine readable Bill of Materials (BOM) of the system’s GOTS/COTS HW, SW, FW and open source modules for a supply chain risk assessment prior to each milestone decision and supported release. The process shall determine the sufficiency of system cyber survivability and support a DevOps framework to prioritize vulnerability mitigation and remediation in the system and connected infrastructure with greatest mission risks." (note: drives CDRLs)

***CSA-10 Testability and measurability considerations when writing performance attribute:***

Attributes that must be defined include: how patches are authenticated, how quickly they must be applied, how they are verified once installed, the tolerance for types and quantities and delay, during development and throughout the system’s lifecycle.

## 14.0 CSE Support to Other DoD Initiatives

As discussed in section 5.0, CSE is applicable to many efforts in the DoD, in addition to acquisition and sustainment. A prudent resource sponsor, program manager, or decision authority will consider the principles of CSE at the inception of a capability need analysis and as part of the analysis' requests for information; as part of the request for proposals and in the source selection criteria; in the draft Test and Evaluation Plan; as part of the draft Program Protection Plan (including the Cybersecurity Strategy); at each acquisition milestone, and throughout the knowledge points; and in evaluating the capability's development and testing efforts, to regularly assess progress, and maximize the likelihood of delivering a capability that will be able to attain an operationally-relevant level of system survivability and effectiveness in the expected cyber-contested operating environment. The implementation and continued monitoring of the CSAs should be included in the Continuous Monitoring strategy as part of RMF.

The mission risks associated with cybersecurity and cyber resiliency vulnerabilities are driving criticality analyses and mission risk assessments throughout the Department. Their results are also driving implementation of zero trust architectures to better protect access to applications and environments; scrutiny of hardware and software supply chains; application of Cybersecurity Maturity Model Certification to protect CUI and Controlled Technical Information in the Defense Industrial Base; and broad emphasis going beyond cybersecurity and the Risk Management Framework for DoD systems and critical infrastructure. CSE can help with all these efforts, and more.

Incomplete RMF implementation in DoD, has historically focused on obtaining a system's ATO, but current efforts now focus on more effective monitoring of risk once authorization has been given, instead of a static status. The memorandum signed by the DoD SISO, DoD CIO Memorandum, "Continuous Authorization to Operate (cATO)" on "Continuous Authorization to Operate (cATO)" was signed on February 2, 2022. This memo emphasizes the continuous monitoring phase of RMF required to enable a cATO. Key elements of the memo identify: 1) relevant RMF security controls used to achieve the CSAs listed, and 2) a discussion of organization's use of the Prepare Step to establish organizational understanding of risks and monitoring requirements for the system. System or program leadership must review the requirements for a cATO (presently limited to the DoD CIO memo) to request inclusion.

cATO identifies RMF and ATO requirements that enable the cyber survivability threshold requirements defined by the Joint Staff's SS KPP to be effectively implemented for any IT capability. In order to achieve a cATO, the RMF AO may wish that the system or capability be able to demonstrate how the system has effectively implemented several CSA threshold requirements, particularly:

- 1) CSA-07, Baseline and Monitor Systems and Detect Anomalies: cATO's specific requirement is a cybersecurity baseline, with on-going visibility of key cybersecurity activities inside of the system boundary for Continuous Monitoring (ConMon) of RMF controls and active defenses. The RMF requires a ConMon strategy for each system, describing how the system will continuously monitor all of the controls in the security control baseline for that system, including inherited controls. Automated monitoring should be as near-real-time as feasible. For manual controls, those timelines must be included in the overall monitoring

strategy. It is critical that systems demonstrate the ability to effectively automate and monitor necessary cybersecurity controls prior to entering into cATO. DoD Compliance to Connect capabilities can support this requirement.

Systems are no longer produced or deployed as a singular system; they operate as a system of systems. The goal of a cATO is to formalize the trust relationships across a system of systems to help deliver more responsive, resilient capabilities to warfighters. ConMon acknowledges that an AO needs the ability to monitor the cumulative set of system-level controls that span the AO's responsibility boundary.

For cATO, system-level controls will need to be fed into a dashboard view. Using this information, the AO will be better positioned to make informed risk decisions as to the threat posed to the system, and it will also enable defensive cyber operations elements to conduct necessary response actions.

2) CSA-08, Manage System Performance and Enable Cyberspace Defense: cATO's requirement is the ability to conduct active cyber defense to effectively respond to cyber-events. As the Department shifts towards a data centric model, so too must cyber defenses, using threat-driven dashboards and metrics to establish patterns and discern threats before they create havoc on DoD terrain. This goes beyond scans and patching; systems must be able to show a real/near-real-time ability to deploy countermeasures. Constant communications with the various cyber operational components, including Cybersecurity Service Providers, component cyber operations forces, Joint Force Headquarters-DoDIN, USCYBERCOM, local defenders, Service-retained cyber forces, and CCMD cyber support (such as Joint Cyberspace Center) are essential to ensuring operations within each system boundary will rapidly access, and digest, cyber threat intelligence. DoD Compliance to Connect capabilities can support this requirement.

3) CSA-10, Actively Manage the System's Configurations to Achieve and Maintain an Operationally Relevant cyber risk posture: One cATO requirement is the adoption and use of a secure software supply chain. The number of components required in modern systems continues to increase rapidly, and underlying software architectures and deployed mission configurations have moved beyond a single binary installed from physical media. These advancements are often invisible to the end-user, where modern software applications are backed by an array of network services that include remote configuration updates, advanced analytics, and AI-powered rulesets that update cyber defense systems automatically. As the Department's operations become increasingly dependent on software, we must ensure that it is created in a protected and controlled environment. In order to prevent human errors, supply chain interdictions, unintended code, or other environmental threats, the adoption of an approved software platform and development pipeline is critical. To achieve a cATO, a system must embrace the DoD Enterprise DevOps strategy that includes cybersecurity and cyber resiliency requirements (DevSecOps), which creates a cultural change that implements the full and open agile collaboration of what have traditionally been separate disciplines. Incorporating development, security, and operations closes gaps and monitors functions that span the maintenance and supply chains. This will also require rapid and recurring information exchange on remediation and mitigation change recommendations between the system's engineers and its assigned defenders. Specifics on the DoD Enterprise DevSecOps strategy are at: <https://dodcio.defense.gov/Library/>

If an AO determines the system has effectively implemented the threshold requirements to achieve and maintain an operationally-relevant real time cybersecurity and cyber resiliency risk posture for a cATO, the AO will notify the component CISO of the intention to move that system to a cATO status. The DoD CISO will review the cATO request and approve it, if the system meets the required criteria. DoD CIO-CS is coordinating and publishing formal guidance for achieving a cATO. As cyber risks change, cATO guidance will be updated with DoD cybersecurity best practices.

Approval of a cATO is not a permanent designation. Systems granted permission to operate under a cATO may have this revoked for reasons, such as poor cybersecurity posture, as identified through continuous monitoring reporting or external assessments; changes in risk tolerance; or a cybersecurity incident resulting from poor adherence to practices.

Making ATOs more relevant to cyber resiliency, and cyber survivability, and less of an administrative burden, will also make it possible for Service and program resources to be used to pursue development of contractually-binding cyber testing threshold requirements, and establish support processes to continually adapt our capabilities to emergent cyber threats.

## 15.0 CSE Vignette

The following is a notional capability requirement that is meant to show how the CSE process can be incorporated into ICD, AoA, and CDD development efforts:

The DoD is taking a more active role in fighting drug cartels in Latin America. To aid USSOUTHCOM intelligence operators on the ground, the DoD requires an off-road vehicle with C4I Surveillance and Reconnaissance capabilities. The vehicle will be used to inconspicuously patrol densely populated urban operational environments and to provide on-board operators with a fully networked platform consisting of the following integrated capabilities:

- Cellular phone surveillance
- Land mobile radio frequency surveillance
- Satellite phone surveillance
- Mobile hot-spot functionality
- Nearby public network analysis (e.g. port scanning, packet analysis, network enumeration, vulnerability scanning, etc.)
- Dynamic street mapping for Google Maps-like functionality to be used by other platforms, and for search and avoidance
- 360 degree cameras for license plate number reconnaissance, facial recognition, and line of sight audio/video monitoring
- Vehicle-to-vehicle (V2V) communication
- Vehicle-to-infrastructure (V2I) communication
- Self-driving functionality
- Automatically zeroize all controlled cryptographic items, classified material, and the entire system if necessary, if the system loses contact with remote command and control segment, and is in immediate danger of crashing, being stolen, or being destroyed

**CSE steps for the requirement sponsor:** The requirement sponsor performed the following steps to determine the Cyber Survivability Risk Category (CSRC) of the system:

**Step 1 – Determine the Mission Type (MT):** The requirement sponsor determined that the proposed system qualifies as having an Operational/Tactical Mission Type 4 (MT 4). Therefore, the system shall require high levels of cybersecurity, survivability, and resiliency. It will be a mission system with Command and Control capabilities, supporting communications systems, and networks.

**Step 2 – Determine the Adversary Threat Tier (ATT):** The requirement sponsor determined that the operational environment of the platform will expose the system to ATT 2, moderate cyber-attack capabilities. They used the DITL to make this determination, located on SIPRNet at:

[https://intellipedia.intellink.sgov.gov/wiki/Defense\\_Intelligence\\_Threat\\_Library](https://intellipedia.intellink.sgov.gov/wiki/Defense_Intelligence_Threat_Library)

They determined that drug cartels use ATT level 2 capabilities to carry out crimes such as credit card cloning, money laundering, and to inform targeted assassinations of informants. They use limited planning and unclear command and control. They have access to hacker forums, and have internal developers. In addition to the general characteristics of ATT 1, ATT 2 adversary characteristics include:

- 1) State and non-state actors
- 2) May be well organized and well-resourced
- 3) Can be determined/persistent
- 4) Capable of discovering new vulnerabilities

**Step 3 – Determine the Cyber Dependence Level (CDL):** The requirement sponsor determined that the system has a CDL of 4 because the Connectivity and Technical Exposure of the system are High and Limited, respectively. The system will have access to GPS, military/commercial SATCOM, and open/commercial internet. Communication systems will be segregated based on classification. The system will have mechanical, electrical/interior communications, and C4I subcomponents. Internal communication protocols will address security through C, I, A. Internal components need to verify validity of all frames. Command, control, positioning, and navigation of the system will be able to be performed remotely and manually. The platform will resemble a recognizable and common make and model, but the adversary will have limited knowledge of the internal components of the platform, due to IC conclusions that the projected adversaries have not conducted intellectual property theft within the defense industrial base for this capability. CDL is not typically known at the ICD stage; this is for illustration only.

**Step 4 – Determine the Impact Level (IL) of system compromise to the mission:** The requirement sponsor determined that if the platform is impacted by cyber compromise, it will have a severe adverse effect to the mission, and an IL of 4. There will be an unacceptable compromise of mission capability or significant mission degradation due to the fact that this platform will be operating in a foreign country and not at war. IL 4 was assigned to the system taking into account the ATT 2 in step 2. Open source intelligence related to credit card cloning, cyber money laundering, and social media stalking was used to subjectively determine that the mission assurance-related cyber threat to the system, posed by the cyber contested environment was not enough to rank the IL at level 5. IL is not typically known at the ICD stage.

**Step 5 – Determine the Cyber Survivability Risk Category (CSRC):** The requirement sponsor determined that the system has an MT of 4, ATT of 2 [CDL of 4, and IL of 4 if AI or ML were being considered for use]; using the High Water Mark method, it was determined that the system is a CSRC 4.

**Include CSRC 4 exemplar language into the ICD and AoA guidance:** After having determined that the system has a CSRC of 4, the requirement sponsor incorporated and tailored the following exemplar language into the ICD and provided it as AoA study guidance:

The system's mission criticality and impact of system compromise requires the capability must survive and operate in an advanced cyber-contested environment (e.g., Russia GRU, APT-28, China APT-41). This level of adversaries uses detailed target technical knowledge to conduct complex, long-term cyber-attack

operations combining multiple intelligence sources to obtain access to high-value networks. After gaining access, they combine well known TTPs to move laterally, evade defenses and collect additional info (e.g., widespread, distributed and anonymized 'brute force' attacks on cloud services). Recognizing this cyber threat will increase and eventually gain access to even greater capabilities, the system must implement best available defensive capabilities and mitigations to prevent/mitigate effects of cyber-events to maintain a minimum functionality to complete the mission, and/or recover/adapt to fight another day, including: implement NSA's Top 10 Cybersecurity Mitigations to ensure Confidentiality, Integrity, & Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; DoD-developed cyber protections, including protections inherited from the operational environment; and as required, specific custom protections to actively manage the system's configuration to achieve and maintain an operationally-relevant cyber risk posture." The following ten Cyber Survivability Attributes (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:

- 1) Prevent cyber-events effects: CSA-01: Control Access; CSA-02: Reduce Cyber Detectability; CSA-03: Secure Transmissions and Communications; CSA-04: Protect Information from Exploitation; CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels; CSA-06: Minimize & Harden Cyber Attack Surfaces.
- 2) Mitigate the effects of cyber-events: CSA-07: Baseline & Monitor Systems and Detect Anomalies; CSA-08: Manage System Performance and Enable Cyberspace Defense.
- 3) Recover from cyber-events: CSA-09: Recover System Capabilities.
- 4) Support adapting to changing threats throughout the system's lifecycle: CSA-10: Actively Manage System's Configurations to Achieve and Maintain an Operationally-relevant cyber risk posture."

**Include CSRC 4 draft exemplar language in the draft CDD:** The requirement sponsor ensured the appropriate CSAs were considered during the ICD and AoA. After the preferred materiel solution was identified, the CSAs used in the AoA were tailored to support the draft CDD.

For a CSRC 4 capability, the requirement sponsor should specify six to nine CSAs: probably three to five Prevent CSAs, one to two Mitigate CSAs, Recover CSA, and Adapt CSA, to ensure a reasoned and risk-managed approach to address the SS KPP requirements.

The following example of a CSA table includes all ten CSAs, which were only slightly tailored for this vignette. A CSRC 4 program would not usually require CSA-02 and CSA-04, and might not require CSA-08. However, because of the varied operational environments this system could be operating in, all ten CSAs could apply to some extent. For illustration purposes, all ten are shown below.



Table 3: Vignette CDD Table

| <p><b>(U) Table 5.1 - Cyber Survivability Attributes Threshold and Objective Requirements</b></p> <p><b>(Listing CSRC and CSAs specific to a capability would be U//CUI at a minimum)</b></p> |   |
|---|---|
| <p>CSRC Rationale</p>   | <p><b>(U) CSRC Rationale:</b> The system’s Cyber Survivability Risk Category (CSRC) level 4 was determined by assessing its Mission Type (MT) of 4, Adversary Threat Tier (ATT) of 2, Cyber Dependency Level (CDL) of 4 and Impact Level (IL) of system compromise of 4.</p> <p><b>(U) CSRC 4 Summary:</b> The system’s mission criticality and impact of system compromise requires the capability must survive and operate in an advanced cyber-contested environment (e.g., Russia GRU, APT-28, China APT-41). This level of adversaries uses detailed target technical knowledge to conduct complex, long-term cyber-attack operations combining multiple intelligence sources to obtain access to high-value networks. After gaining access, they combine well known TTPs to move laterally, evade defenses and collect additional info (e.g., widespread, distributed and anonymized ‘brute force’ attacks on cloud services). Recognizing this cyber threat will increase and eventually gain access to even greater capabilities, the system must implement best available defensive capabilities and mitigations to prevent/mitigate effects of cyber-events to maintain a minimum functionality to complete the mission, and recover/adapt to fight another day, including: implement NSA’s Top 10 Cybersecurity Mitigations to ensure Confidentiality, Integrity, &amp; Availability for trusted internal and external information flows; defense in depth architecture, with no single points of failure; DoD-developed cyber protections, including protections inherited from the operational environment; and as required, specific custom protections to actively manage the system’s configuration to achieve and maintain an operationally-relevant cyber risk posture. Due to safety and liability concerns inherent with the self-driving requirement, as well as to maintain control of the sensitive on-board materials, the system will maintain constant contact with operators and local cyber defenders.”</p> |
| <p>CSRC Summary</p>   | <p><b>(U) System Survivability Critical CSAs:</b> The following subset of the 10 CSAs in the table below have been determined to be critical for <i>(capability’s name)</i> cyber survivability, and should drive development of RFP and source selection criteria. These CSAs have been tailored to define the capability’s threshold requirements, with CSA-10 enabling adaptive incremental improvements for countering advances in adversary capabilities and newly identified vulnerabilities to maintain an operationally-relevant cyber risk posture:</p> <p>[Unless otherwise stated, CSAs are threshold performance requirements to prevent, mitigate, recover from and adapt to cyber-events. The CSAs are sufficiently detailed to be support creation of measureable and testable requirements, but not so detailed as to limit the ability of system security engineers to meet indirect and implied requirements for other system functionality. With modification, these CSAs also lend themselves to be used as source selection criteria.]</p>   |

| Cyber Survivability Attribute   | Developmental Threshold   | Objective  |
|---|---|------------|
| Prevent<br><b>CSA-01 – Control Access</b>   | (U) “System shall only allow identified, authenticated, and authorized persons and non-person entities (including all assigned cyber defenders and their tools) access or interconnection to system or sub-system elements. The capability shall enforce a validation mechanism to protect the C, I, A of system resources (e.g., memory, files, interfaces, logical networks). The system shall employ anti-tamper measures that include features for protection of critical system components, information technologies, and maintenance of technology/program protection. Physical access to the system shall also be controlled.” | <b>T=O</b> |
| Prevent<br><b>CSA-02 – Reduce System’s Cyber Detectability</b>  | (U) “System survivability requires signaling and communications (both wired and wireless) implemented by the system shall minimize the ability of an adversary to monitor and/or target system and/or supported DoD weapon systems through its emanations.”   | <b>T=O</b> |
| Prevent<br><b>CSA-03 – Secure Transmissions and Communications</b>  | (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.”   | <b>T=O</b> |
| Prevent<br><b>CSA-04 – Protect System’s Information from Exploitation</b>                                   | (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).”  | <b>T=O</b> |
| Prevent<br><b>CSA-05 – Partition and Ensure Critical Functions at Mission Completion Performance Levels</b> | (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.”   | <b>T=O</b> |
| Prevent<br><b>CSA-06 – Minimize and Harden Attack Surfaces</b>  | (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.”   | <b>T=O</b> |

|                       |  |  |            |
|-----------------------|--|--|------------|
| Mitigate              | <b>CSA-07 – Baseline &amp; Monitor Systems and Detect Anomalies</b>  | (U) “System shall implement and maintain a cyber survivability configuration baseline for its GOTS/COTS HW, SW, FW and open source modules, by version number to ensure an operationally acceptable cyber risk posture 24/7 (note: drives CDRLs). System shall monitor, detect and report system health status and anomalies indicative of cyber events, based on its current adversary cyber threat intelligence, CONOPS and Mission Relevant Terrain in Cyberspace (MRT-C). Applicable report detail shall be provided to users, system operators and assigned cyber defenders (e.g., system shall report anomalies such as configuration changes, cyber-related event indicators, slowed processing, or loss of functionality within T = (# of seconds/minutes) [specified by sponsor]).”   | <b>T=O</b> |
| Mitigate              | <b>CSA-08 – Manage System Performance and Enable Cyberspace Defense</b>  | (U) “If anomalies are detected and/or cyber-events degrade system capability, the system shall be sufficiently resilient to mitigate cyber-related event effects through orderly, structured and prioritized system responses, in order to ensure minimum mission functionality requirements [system functionality threshold specified by sponsor] to complete the current mission or return for recovery. The system shall enable assigned cyber defenders to impose effects on adversaries to counter their operations and objectives. Alternatively, the mission commander shall be able to selectively disconnect/disable subsystems that are not critical as well as isolate the system from integrated platform systems and/or Department of Defense Information Network (DoDIN).”   | <b>T=O</b> |
| Recover               | <b>CSA-09 – Recover System Capabilities</b>  | (U) “After a cyber-event, the system shall be capable of being restored to full functionality from a trusted source; at a minimum, restore partial-to-full mission capability, between mission cycles or within 24 hours, to fight another day. System recovery shall prioritize cyber operational resiliency functions.”  | <b>T=O</b> |
| Adapt - All 3 Pillars | <b>CSA-10 – Actively Manage System’s Configurations to Achieve and Maintain an Operationally-Relevant Cyber Risk Posture</b> | (U) “Throughout a system’s lifecycle and within one standard mission cycle of xx hours [specified by sponsor] of identification of a drop in cyber risk posture below its commensurate CSRC level, the system shall have a configuration management process, supported by automated capabilities and technology refresh options, to achieve and continuously maintain an objectively assessed and operationally-relevant risk posture. The process shall include inputs from operators, defenders and intel analysts to continuously assess changes in adversary threat, and include a machine readable Bill of Materials (BOM) of the system’s GOTS/COTS HW, SW, FW and open source modules for a supply chain risk assessment prior to each milestone decision and supported release. The process shall determine the sufficiency of system cyber survivability, and support a DevOps framework to prioritize vulnerability mitigation and remediation in the system and connected infrastructure with greatest mission risks.” (note: drives CDRLs) | <b>T=O</b> |

(U) Table 5.1 Cyber Survivability Attributes Threshold and Objective Requirements

Note that the CSA exemplar content shown above will not apply to every system. It is meant to provide the reader with an example of how to use the cyber survivability content described throughout this guide to develop measurable and testable performance requirements. The CSAs described throughout this guide and referenced in this table are concepts that requirement sponsors should consider during ICD, AoA, and CDD development efforts in order to describe capabilities that are needed to help the system survive in a cyber-contested environment.

## 16.0 Joint Staff Gatekeeping

The Joint Staff Gatekeepers are part of the J8 organization. The gatekeepers work in coordination with the document Sponsor and the Protection FCB to ensure any exceptions or variances meet the needs of the validation authority, while allowing for appropriate flexibility in the capability requirements process. The Joint Staff Gatekeepers work with the Protection FCB to provide synchronized responses to capability requirement documents using the staffing process found in Appendix C to Enclosure A of the 2021 JCIDS Manual. The Chair of the Protection FCB provides endorsement of the SS KPP to the Gatekeepers in accordance with Annex C to Appendix G to Enclosure B of the JCIDS Manual.

The Joint Staff J6 cyber survivability analysts review the draft capability requirement document from the requirement sponsor, and use the assessment criteria shown below to determine whether the capability sufficiently considered cyber survivability. The analysts will use these assessment criteria to assess JROC Interest and JCB Interest capabilities attempting to attain a Cyber Survivability Endorsement as part of the System Survivability KPP Endorsement (for CDDs). The Protection FCB is not authorized to provide this SS KPP endorsement to Joint Information capabilities.

1. Did the document include a determination of its CSRC using the available CSRC factors?
2. Did the document include a CSRC-defined Cyber Survivability cyber threat and countermeasures requirement summary statement?
3. Did the document's Threat Summary include the cyber Adversary Threat Tier?
4. Did the AoA guidance include a CSRC-defined cyber survivability requirement and threat statement, and the requirement to consider the resource and mission risk implications of each alternative's ability to meet the intent of the CSAs?
5. Did the CDD include a tailored subset of the ten CSAs identified as critical to system survivability in the expected operational environment?
6. How will the system prevent the impact of cyber-events on C, I, A? These attributes include:
  - Controlling access
  - Reducing system's cyber detectability
  - Securing transmissions and communications
  - Protecting system's information from exploitation
  - Partitioning and ensuring critical functions are at mission completion performance levels
  - Minimizing, hardening and baselining attack surfaces
7. How will the system mitigate the effects of cyber-events to complete the mission? These attributes include:
  - Baselining the system and monitoring to detect anomalies
  - Managing system performance if degraded by cyber-events
8. How will the system recover from cyber-events to fight another day? These attributes include recovering system capabilities to complete the mission or to return to base.
9. How will the system adapt to new threats? How are the mission risks from future threats to be identified, and how will GOTS/COTS HW, SW, FW and open source modules countermeasures be developed and deployed? How are patch updates and engineering change proposals incorporated

into system releases and configuration management processes, into the lifecycle sustainment plan, and during operations and maintenance in the operational environment, to ensure that the system remains secure, survivable, and mission capable?

## 17.0 Annotated References

- **Cyber Survivability Portal:**
  - <https://intelshare.intelink.gov/sites/cybersurvivability/> (NIPRNet)
  - <https://intelshare.intelink.sgov.gov/sites/cybersurvivability/> (SIPRNet)
- **Committee on National Security Systems Instruction (CNSSI) 1253** – This Instruction states that the potential impact levels determined for C, I, A are retained, meaning there are 27 possible three-value combinations for National Security Information (NSI) or National Security Systems (NSS), as opposed to the three possible single-value categorizations obtained using the guidelines in FIPS 200. Retaining the discrete impact levels for each of the three security objectives is done to provide a better granularity in allocating security controls to baselines and should thereby reduce the need for subsequent tailoring of controls. The definition for what constitutes a Low, Moderate, or High C, I, A potential impact level for NSI or NSS is included in Chapter 2, Section 2.1.
  - **Confidentiality** – “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” [44 U.S.C., Sec. 3542]. A loss of confidentiality is the unauthorized disclosure of information.
  - **Integrity** – “Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity...” [44 U.S.C., Sec. 3542]. A loss of integrity is the unauthorized modification or destruction of information.
  - **Availability** – “Ensuring timely and reliable access to and use of information...” [44 U.S.C., Sec. 3542]. A loss of availability is the disruption of access to or use of information or an information system.

More information is at: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

- **National Security Directive 42 (NSD-42)** – Assigns the National Security Agency (NSA) as the National Manager for cryptographic components/systems utilized to protect National Security Systems (NSS).
- **National Security Memorandum 8 (NSM-8)** - NSM-8 sets forth requirements for National Security Systems (NSS) that are equivalent to or exceed the cybersecurity requirements for Federal Information Systems set forth within Executive Order 14028 and establishes methods to secure exceptions for circumstances necessitated by unique mission needs.
- **Chairman of the Joint Chiefs of Staff Instruction 6510.02E (CJCSI 6510.02E)**, Cryptographic Modernization and Planning – Directs customers’ current and future planning.
- **Defense Acquisition Guidebook, Chapter 9** – Program Protection; see DoDI 5000.83 [to be replaced by the “DoD Technology and Program Protection (T&PP) Guidebook” later in 2022; the information shown below will be updated with the T&PP Guidebook info when it is made available]:
  - Section 9-3.1.3.1 describes the criticality analysis (CA) of a program to focus attention and resources on the system capabilities, mission critical functions, and critical components that

matter most. Mission critical functions are those functions of the system that, if corrupted or disabled, would likely lead to mission failure or degradation. Mission critical components are primarily the elements of the system (hardware, software, or firmware) that implement mission critical functions. It can include components that perform defensive functions that protect critical components and components that have unobstructed access to critical components. Criticality analysis includes the following iterative steps:

- Identify and group the mission capabilities the system will perform
- Identify the system's mission critical functions based on mission capabilities and assign criticality levels to those functions
- Map the mission critical functions to the system architecture and identify the defined system components (hardware, software, and firmware) that implement those functions (i.e. components that are critical to the mission effectiveness of the system or an interfaced network)
- Allocate criticality levels to those components that have been defined
- Identify suppliers of critical components
- The identified functions and components are assigned levels of criticality commensurate with the consequence of their failure on the system's ability to perform its mission. Protection Failure Criticality Levels are:
  - Level I – Total Mission Failure: Failure results in total compromise of mission capability
  - Level II – Significant/Unacceptable Degradation: Failure that results in unacceptable compromise of mission capability or significant mission degradation
  - Level III – Partial/Acceptable: Failure that results in partial compromise of mission capability or partial mission degradation
  - Level IV – Negligible: Failure that results in little or no compromise of mission capability
- Section 9-3.1.3.2, Trusted Systems and Networks (TSN) Threat Analysis – All-source intelligence is available to the PM to understand threats to the system and threats posed by specific suppliers. Multiple sources of intelligence can be used to feed into this analysis.
- A source for supplier threat information is the DIA SCRM Threat Analysis Center (DIA SCRM TAC). DoD has designated the DIA to be the DoD enterprise focal point for threat assessments needed by the PM to inform and assess supplier risks.
- DIA supplier threat assessments provide threat characterization of the identified suppliers to inform risk-mitigation activities. The PM and the engineering team should use these threat assessments to assist in developing appropriate mitigations for supply chain risks. TAC requests should be submitted for all Level I and Level II critical functions and components as identified by a criticality analysis, and a list of suppliers of critical components should be created. TAC requests may be submitted as soon as sources of critical functions and components are identified.
- **DoDI 5000.83 – Technology and Program Protection to Maintain Technological Advantage:** Establishes the policy to employ risk-based measures to protect systems and technologies from adversarial exploitation and compromise.



- **DoDI 8500.01 – Cybersecurity:** Establishes a DoD cybersecurity program to protect and defend DoD information and IT. DoDI 8500.01 replaced “Information Assurance” with “Cybersecurity”. The instruction establishes policy to focus all DoD IT efforts on risk management, operational resiliency, integration and interoperability, and cyberspace defense. By defining operational resiliency separately from risk management, the instruction establishes the implied requirement for all DoD programs to be resilient in a mission context as opposed to a system context. The instruction requires cybersecurity DT and OT to evaluate resiliency.
- **DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT:** Establishes associated cybersecurity policy, and assigns responsibilities for executing and maintaining the RMF. The RMF manages the life-cycle cybersecurity risk to DoD IT. The cybersecurity requirements for DoD IT will be managed through the RMF consistent with the principles established in NIST SP 800-37. All DoD IS and Platform IT systems must be categorized in accordance with CNSSI 1253, implement a corresponding set of security controls from NIST SP 800-53, and use assessment procedures from NIST SP 800-53A and DoD-specific assignment values, overlays, implementation guidance, and assessment procedures found on the RMF Knowledge Service (KS).
- **Risk Management Framework Knowledge Service (KS):** The online, web-based resource (<https://rmfks.osd.mil>) that provides guidance and tools for implementing and executing the RMF. It is the authoritative source for RMF guidance and the repository for DoD RMF policy. It provides access to security control baselines, overlays, individual security controls, and security control implementation guidance and assessment procedures. It will also provide greater granularity on the CSAs, and Cyber Survivability strength of implementation via CSE Implementation Guide volumes II and III.
- **DoD CISO Continuous Authorization to Operate (cATO) Memo:** Signed in February 2022, this memo is intended to provide “specific guidance on the necessary steps to allow systems to operate under a cATO state”. While limited to the continuous monitoring (COMMON) of a system’s applicable RMF controls by the system owner, it reinforces and supports adaptive maintenance of a cyber posture, which could then support a system’s cyber survivability efforts. See section 14.0; the memo is available in the Shared Documents section of the CSE SharePoint
- **NIST Cybersecurity Framework White Paper:** directed by Executive Order (EO) 13636, based on existing standards, guidelines, and practices – For reducing cybersecurity risks to critical infrastructure. Additional information is at: <https://www.nist.gov/cyberframework/>
- **NIST SP 800-37 Rev. 2 – RMF for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy:** provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>
- **NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations:** NIST SP 800-53 represents an initiative to update the security controls catalog

content, and guidance for selecting and specifying security controls for federal information systems and organizations. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

- **NIST SP 800-160 Volume 2 Revision 1 – Developing Cyber-Resilient Systems: A Systems Security Engineering Approach:** NIST SP 800-160, Volume 2 focuses on cyber resiliency engineering—an emerging specialty systems engineering discipline applied in conjunction with systems security engineering and resiliency engineering to develop survivable, trustworthy secure systems. It is aligned closely to, and provides significant synergy with, CSEIG version 3. <https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final>
- **DIA Directive 5000.200** – Intelligence Threat Support for Major Defense Acquisition Programs (19 June 2018): URL available on SIPRNet Cyber Survivability Portal
- **DoDI O-5240.24 Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA):** available on NIPRNet Cyber Survivability Portal.
- **Defense Intelligence Analysis Program, User’s Guide** (January 2016); URL available on SIPRNet Cyber Survivability Portal.
- **Intelligence Support to the Adaptive Acquisition Framework (ISTAAF) Guidebook**, OUSD (A&S), September 2021.
- **SSE Cybersecurity and Cyber Resiliency System and Lower Level Specification Requirements (Excel workbook)** – contains a top-level worksheet for system-level requirements, as well as multiple worksheets for the lower-level system requirements intended for engineers experienced in DoD acquisitions. SEs and SSEs will be able to derive the appropriate requirements to put in the System Requirements Document and/or System Specification using the Functional Thread Analysis, top-level architecture, System Survivability KPP’s CSAs, along with the requirements in the “Sys Req” tab of the worksheet. This is available in the CSE documents library section of the NIPRNet SharePoint site.

## 18.0 Acronyms

|           |   |
|-----------|---|
| AFRL      | Air Force Research Laboratory                               |
| AI        | Artificial Intelligence                                     |
| AO        | Authorizing Official  |
| AoA       | Analysis of Alternatives                                    |
| APT       | Advanced Persistent Threat                                  |
| ATO       | Authorization to Operate                                    |
| ATT       | Adversary Threat Tier                                       |
| C, I, A   | Confidentiality, Integrity and Availability                 |
| C4I       | Command, Control, Communication, Computers and Intelligence |
| C4ISR     | C4I Surveillance and Reconnaissance                         |
| CBA       | Capability Based Assessment                                 |
| CAC       | Common Access Card  |
| cATO      | Continuous Authorization to Operate                         |
| CCMD      | Combatant Command   |
| CDD       | Capability Development Document                             |
| CDL       | Cyber Dependency Level                                      |
| CDRL      | Contract Deliverable Requirements List                      |
| CI        | Critical Infrastructure                                     |
| CIO       | Chief Information Officer                                   |
| CIP       | Critical Intelligence Parameter                             |
| CISA      | Cybersecurity and Infrastructure Security Agency            |
| CMMC      | Cybersecurity Maturity Model Certification                  |
| CNSSI     | Committee on National Security Systems Instruction          |
| ConMon    | Continuous Monitoring                                       |
| CONOPS    | Concept of Operations                                       |
| CORA-P    | Cyberspace Operational Resilience Assessment – Platform     |
| COTS      | Commercial Off The Shelf                                    |
| CS        | Control System  |
| CSA       | Cyber Survivability Attribute                               |
| CSE       | Cyber Survivability Endorsement                             |
| CSRC      | Cyber Survivability Risk Category                           |
| CSRP      | Cyber Survivability Risk Posture                            |
| CTM       | Cyber Threat Module   |
| CTT       | Cyber Table-Top   |
| CTTX      | Cyber Table-Top exercise                                    |
| CUI       | Critical Unclassified Information                           |
| DCRA      | Deep Cyber Resiliency Assessment [OUSD(A&S)]                |
| DevOps    | Development Operations                                      |
| DevSecOps | Development, Security, Operations                           |

UNCLASSIFIED

|         |   |
|---------|---|
| DFARS   | Defense Federal Acquisition Regulation Supplement     |
| DIA     | Defense Intelligence Agency                           |
| DIB     | Defense Industrial Base                               |
| DITL    | Defense Intelligence Threat Library                   |
| DoD     | Department of Defense                                 |
| DoD CIO | Department of Defense - Chief Information Officer     |
| DoDI    | Department of Defense Instruction                     |
| DoDIN   | Department of Defense Information Network             |
| DOJ     | Department of Justice                                 |
| DOT&E   | Director, Operational Test & Evaluation               |
| FCB     | Functional Capability Board                           |
| FIPS    | Federal Information Processing Standards              |
| FOC     | Full Operational Capability                           |
| FW      | Firmware  |
| GAO     | Government Accountability Office                      |
| GOTS    | Government Off The Shelf                              |
| GPS     | Global Positioning System                             |
| HW      | Hardware  |
| HWM     | High Water Mark                                       |
| IC      | Intelligence Community                                |
| ICD     | Initial Capabilities Document                         |
| IG      | Implementation Guide                                  |
| IL      | Impact Level  |
| IMD     | Intelligence Mission Data                             |
| IOC     | Initial Operational Capability                        |
| IS-CDD  | Information Systems – Capability Development Document |
| IS-ICD  | Information Systems – Initial Capabilities Document   |
| JCB     | Joint Capabilities Board                              |
| JP      | Joint Publication                                     |
| JCIDS   | Joint Capabilities Integration and Development System |
| JROC    | Joint Requirements Oversight Council                  |
| JWICS   | Joint Worldwide Intelligence Communication System     |
| KM/DS   | Knowledge Management and Decision Support             |
| KPP     | Key Performance Parameter                             |
| KS      | Knowledge Service                                     |
| LCSP    | Life Cycle Sustainment Plan                           |
| LMDP    | Lifecycle Mission Data Plan                           |
| MA      | Mission Assurance                                     |
| MBCRA   | Mission-Based Cyber Risk Assessment                   |
| MDA     | Milestone Decision Authority                          |

|            |   |
|------------|---|
| MDD        | Materiel Development Decision                                       |
| ML         | Machine Learning  |
| MS         | Milestone   |
| MT         | Mission Type  |
| NDAA       | National Defense Authorization Act                                  |
| NIST       | National Institute of Standards and Technology                      |
| NIPRNet    | Non-Classified Internet Protocol Router Network                     |
| NSA        | National Security Agency  |
| NSS        | National Security Systems   |
| NSI        | National Security Information                                       |
| OMS/MP     | Operational Mode Summary/Mission Profile                            |
| OPLAN      | Operational Plan  |
| OT         | Operational Technology  |
| OT&E       | Operational Test and Evaluation                                     |
| OUSD (A&S) | Office of the Undersecretary of Defense (Acquisition & Sustainment) |
| OUSD (I)   | Office of the Undersecretary of Defense (Intelligence & Security)   |
| OUSD (P)   | Office of the Undersecretary of Defense (Policy)                    |
| OUSD (R&E) | Office of the Undersecretary of Defense (Research & Engineering)    |
| PM         | Program Manager   |
| PMO        | Program Management Office   |
| PPP        | Program Protection Plan   |
| PPS        | Ports, Protocols and Services                                       |
| RFI        | Request for Information   |
| RFP        | Request for Proposal  |
| RMF        | Risk Management Framework   |
| ROM        | Rough Order of Magnitude  |
| SAP        | Special Access Program  |
| SATCOM     | Satellite Communications  |
| SCRM       | Supply Chain Risk Management  |
| SE         | Systems Engineering   |
| SSE        | Systems Security Engineering  |
| SEP        | Systems Engineering Plan  |
| SIPRNet    | Secret Internet Protocol Router Network                             |
| SoS        | System of Systems   |
| SOW        | Statement of Work   |
| SP         | Special Publication   |
| SS         | System Survivability  |
| SW         | Software  |
| STIG       | Security Technical Implementation Guide                             |
| T&PP       | Technology and Program Protection                                   |

|         |   |
|---------|---|
| TAC     | Threat Assessment Center                          |
| TEMP    | Test and Evaluation Master Plan                   |
| TSN     | Trusted Systems and Networks                      |
| TTP     | Tactics, Techniques, and Procedures               |
| US-CERT | United States – Computer Emergency Readiness Team |
| V2V     | Vehicle to Vehicle                                |
| V2I     | Vehicle to Infrastructure                         |
| VOLT    | Validated Online Lifecycle Threat (report)        |
| WBS     | Work Breakdown Structure                          |
| WiFi    | Wireless Fidelity                                 |
| WS      | Weapon System                                     |

## 19.0 Glossary

### **Advanced Persistent Threat**

An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:

- pursues its objectives repeatedly over an extended period of time,
- adapts to defenders' efforts to resist it, and
- is determined to maintain the level of interaction needed to execute its objectives.

Reference: NIST SP 800-39

### **Adversary**

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities; a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged.

Reference: CNSSI 4009, JP 3-0

### **Cooperative Vulnerability and Penetration Assessment**

The process to characterize the cybersecurity and operational resilience of a system in an operation context and provide reconnaissance of the system in support of the adversarial assessment.

Reference: DoD Cybersecurity Test and Evaluation Guidebook Version 2.0, Change 1

### **Cooperative Vulnerability Identification**

The process to identify known cybersecurity vulnerabilities in hardware, software, interfaces, operations, and architecture; to assess the mission risk associated with those vulnerabilities; and to determine appropriate mitigations or countermeasures to reduce the risk.

Reference: DoD Cybersecurity Test and Evaluation Guidebook Version 2.0, Change 1

### **Critical Infrastructure**

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Reference: Section 1016(e) of the USA PATRIOT ACT of 2001 (42 U.S.C. 5195c(e))

### **Cyber-event**

Any actual unauthorized, accidental or unlawful access, use, exfiltration, theft, disablement, destruction, loss, alteration, disclosure, transmission of any IT assets owned or used by or on behalf of either party or

any member of its group, or any information or data (including any personally identifiable information) stored therein or transmitted thereby.

### **Cyber Resiliency**

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. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. Reference: NIST SP 800-160 Vol 2 revision 1

### **Cyber Survivability**

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.

Reference: JCIDS Manual [Oct 2021], Section 2.5.1.4, Annex C to Appendix G to Enclosure B

[NOTE: This JCIDS Manual definition for Cyber Survivability will be clarified in the next update to include the intent of two other definitional statements. Those references can be found on page 7 of Appendix A to Enclosure B and page 6 of Annex A to Appendix B to Enclosure B, and both state “Cyber Survivability Considerations (cybersecurity and cyber resiliency)”.]

### **Cyber Survivability Attributes (CSAs)**

Created to address System Survivability Key Performance Parameter pillars (Prevent, Mitigate, Recover, and Adapt), CSAs are a holistic set of cybersecurity and cyber resiliency requirements that support, and go beyond, the Risk Management Framework technical controls. They help provide resource sponsors an understanding of the resource and mission risk implications to prevent pursuit/acquisition of capabilities so flawed that it would not be cost effective to mitigate known vulnerabilities to an operationally relevant level. A system's Cyber Survivability Risk Category drives the number of CSAs to be considered, tailored and implemented in a capability's design.

Reference: JCIDS Manual [Oct 2021], Section 2.5.1.4.2, Annex C to Appendix G to Enclosure B

### **Cyber Survivability Risk Category (CSRC)**

The threat methodology employed by a cyber review broadly accounts for mission type, cyber dependency level of the system, adversary threat tier, and impact level of system loss or compromise, in determining a CSRC that identifies appropriate strength of CSA implementation levels.

Reference: JCIDS Manual [Oct 2021], Section 2.5.2.1 Annex C, Appendix B, Enclosure B

### **Cyber Survivability Risk Posture (CSRP)**

A measurable and repeatable methodology to assess a capability's survivability readiness through analysis of cybersecurity and cyber resiliency vulnerabilities, threats, risks, mitigations, and anticipated threat updates to prioritize addressing vulnerabilities with the greatest mission risk and indicate the resulting risk posture. Reference: JCIDS Manual, Section 2.5.1.4.2.4



**Cybersecurity**

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Reference: National Security Presidential Directive-54/Homeland Security Presidential Directive-23

**Cybersecurity Maturity Model Certification**

The Cybersecurity Maturity Model Certification (CMMC) is a framework that measures a contractor’s cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see <https://www.acq.osd.mil/cmmc/index.html>).

Reference: Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7021

**Cyberspace**

A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Reference: JP 3-12; DoD Dictionary of Military and Associated Terms

**Cyberspace attack (“Cyber attack” in CNSSI 4009)**

Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires.

Reference: JP 3-12, CNSSI 4009

**Defense Industrial Base**

The worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

Reference: <https://www.cisa.gov/defense-industrial-base-sector>

**Defined Process**

A managed process that is tailored from the organization’s set of standard processes according to the organization’s tailoring guidelines; has a maintained process description; and contributes work products, measures, and other process improvement information to organizational process assets.

Reference: US-CERT Resilience Management Model v1.2

**Enterprise**

An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition; program management; financial management (e.g., budgets); human resources; security; information systems; information and mission management.  
Reference: CNSSI 4009

**Enterprise Architecture**

A strategic information asset base that defines the mission, the information necessary to perform the mission, the technologies necessary for performing the mission, and the transitional process for implementing new technologies in response to changing mission needs. The enterprise architecture includes a baseline architecture, target architecture, and sequencing plan.  
Reference: CNSSI 4009

**Event**

Any observable occurrence in a network or system.  
Reference: CNSSI 4009, NIST SP 800-61 rev. 2

**Environment**

The physical and logical surroundings in which a system processes, stores, and transmits information.  
Reference: NIST SP 800-53 Rev 5 (adapted)

**Incident**

An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.  
Reference: CNSSI 4009

**Information System**

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.  
Reference: Title 44 U.S.C. §3502, NIST SP 800-171 Rev 2

**Interoperability**

The ability of systems, units or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces, and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. This includes information exchanges, systems, processes, procedures, organizations, and missions over the lifecycle and must be balanced with cybersecurity.  
Reference: DoDI 5000.87

**Malicious Cyber Activity**

Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communication systems, networks, physical or virtual infrastructure controlled by computers of information systems, or information resident thereon.

Reference: CNSSI 4009

**Mission Assurance (MA)**

A process to protect or ensure the continued function and resiliency of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions.

Reference: DoDD 3020.40 change 1, JP 3-26

**Mission Critical Functionality**

Any system function, the compromise of which would degrade the effectiveness of that system in achieving the core mission for which it was designed.

Reference: CNSSI 4009

**Mitigation**

Act of reducing risk by taking some other action generally outside the domain of the influenced system, which cannot be remediated.

Reference DoDI 8531.01 (15 Sep 2020)

**National Security System**

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which—

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions;

Or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Reference: US Code (2014) Title 44-Chap 35, Subchapter II, Section 3552 and CNSSI 4009

**Operational Resilience**

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.

Reference: CNSSI 4009, NIST SP 800-160 Vol 2 (Rev 1), and DoDI 8500.01.

**Operational Technology**

Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Reference: DOE O 205.1C Change 1, Department of Energy Cybersecurity Program

**Recovery**

Recovery is executing system contingency plan activities to restore organizational missions/business functions.

Reference: CNSSI 4009

**Requirements: Threshold versus Objective**

Stakeholders have a need for a system to meet certain performance criteria. The Threshold value is the minimum acceptable value for a given parameter, whereas the objective value is what a stakeholder would really like to have the system achieve.

**Remediation**

Actions taken to eliminate an identified risk. Reference DoDI 8531.01 (15 Sep 2020)

**Resiliency**

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resiliency includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Reference: Presidential Policy Directive (PPD) 21

**Risk**

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Reference: CNSSI 4009

**Risk Tolerance**

Levels and types of risk that are acceptable.

Reference: CNSSI 4009

**Secure/Security**

To reduce the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions

despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Reference: PPD 21, CNSSI 4009

### **Supply Chain**

A linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

Reference: CNSSI 4009

### **Supply Chain Attack**

An incident where an adversary exploits vulnerabilities in the product or service supply network of the intended target.

Reference: CNSSI 4009

### **Supply Chain Risk Management**

A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

Reference: CNSSD 505, CNSSI 4009, DoDI 5200.44, DFARS Clause 252.239-7018

### **Survivability**

A property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance; e.g., nuclear burst. For a given application, survivability must be qualified by specifying the range of conditions over which the entity will survive, the minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration.

Reference: Federal Standard 1037C (in support of MIL-STD-188)

### **Sustain**

Maintain in a desired operational state.

Reference: US-CERT RMM v1.2

### **System of Systems**

A set or arrangement that results when independent and useful systems are integrated into a larger system that delivers unique capabilities. System of Systems may deliver capabilities by combining multiple

collaborative and independent-yet-interacting systems. The mix of systems may include existing, partially developed and yet-to-be designed independent systems.

Reference: DAU Glossary, 2022

**Threat**

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Reference: NIST SP 800-30 Rev 1, CNSSI 4009

**Threat Intelligence**

Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Reference: NIST SP 800-150

**Validation**

The review and approval of JCIDS documents by a designated validation authority. The JROC is the ultimate validation authority for capability requirements unless otherwise delegated to a subordinate board or to a designated validation authority in a Service, CCMD, or another DoD Component.

Reference: CJCSI 5123.01

**Vulnerability**

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Reference: NIST SP 800-30 Rev 1

**Vulnerability Assessment**

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Reference: CNSSI 4009