Operationalizing Cyber Survivability Through Requirements Decomposition: A Marine Corps Case Study

Ms. Kathleen Coen
kathleen.coen@usmc.mil / kathleen.coen@nps.edu

May 2026

Cyber Survivability

Cyber Security

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.

PREVENTION

Source: CNSS No. 4009, here

Cyber Resilience

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.

RESPONSE

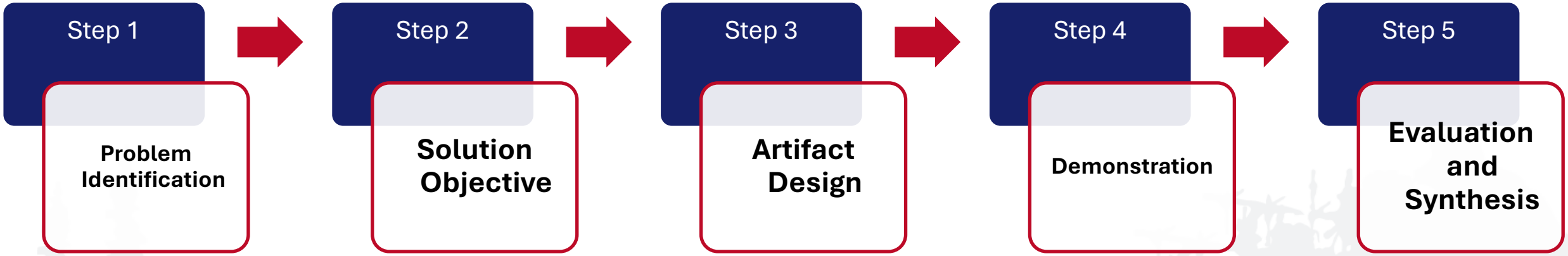
Source: CNSS No. 4009, here

Cyber Survivability

CSAs

SS KPP Pillars	Cyber Survivability Attributes (CSAs)
Prevent	CSA-01: Control Access
	CSA-02: Reduce Cyber Detectability
	CSA-03: Protect Data in Transit
	CSA-04: Protect Data at Rest
	CSA-05: Protect Critical Functions
	CSA-06: Minimize and Harden Attack Surfaces
Mitigate	CSA-07: Baseline and Monitor Systems to Detect Anomalies
	CSA-08: Enable Cyber Defense
Recover	CSA-09: Recover Capabilities
Adapt	CSA-10: Sustain an Operationally Relevant Cyber Survivability Risk Posture (CSRP)

Design Science Research

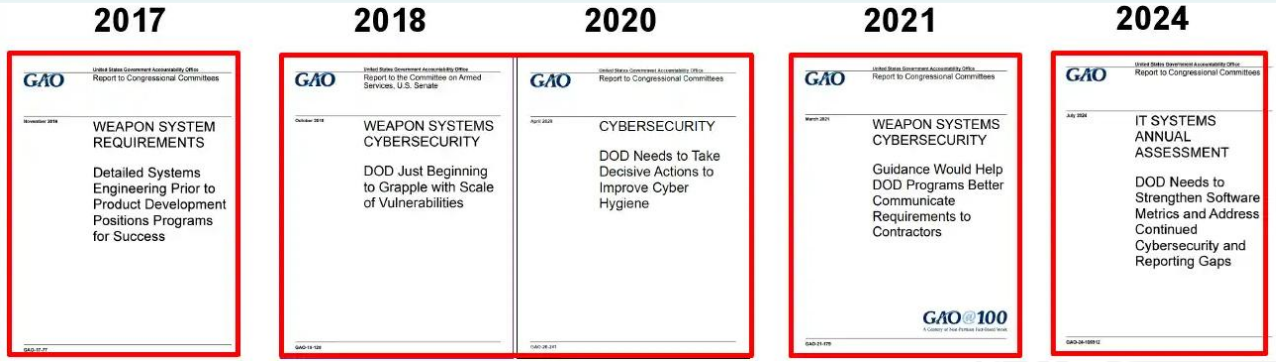


DSR Seminal Work, Hevner et al., 2004 (MISQ): here

Step 1: Problem Identification

Government Accountability Office

GAO reports found that omitting cyber performance specifications leads to costly, ineffective “bolt-on” protections post-fielding. Incorporating “built-in” measures early is vastly cheaper and more effective.



MCTSSA’s Perspective

As part of our cyber assessment planning process, the MCTSSA Cyber Branch reviews system CDDs, SRDs, and RTMs across acquisition systems.

Findings

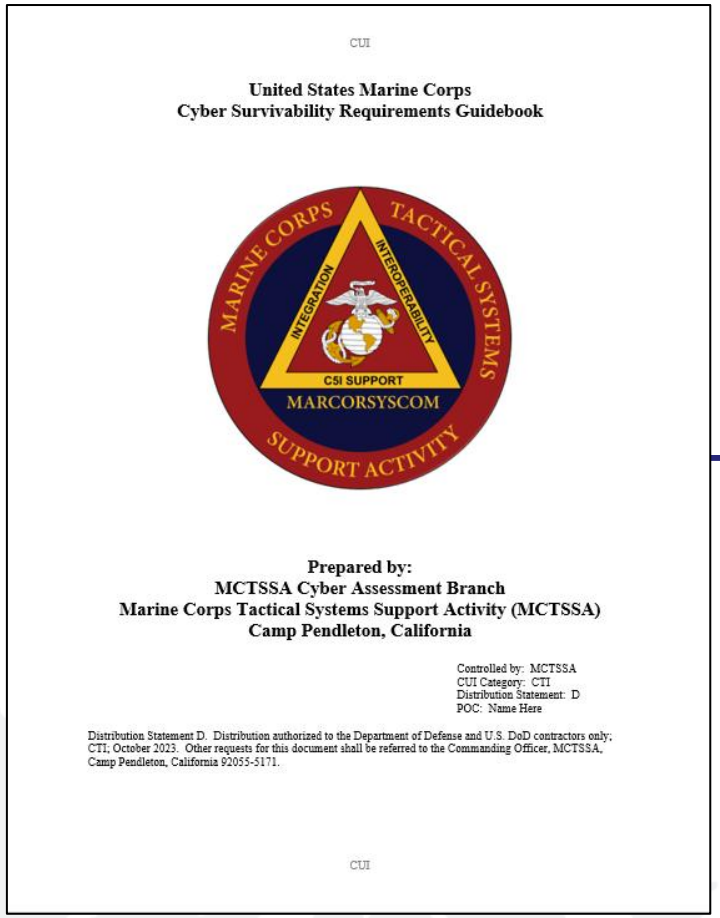
While high-level CSAs were named in policy, they were explicitly not decomposed into measurable, testable sub-system requirements.

Step 2: Solution Objective

To successfully operationalize survivability, the final artifact must:

1. Facilitate the decomposition of CSAs into measurable, system-level performance specifications
2. Align derived requirements with NIST SP 800-53 controls, the backbone of the DoW's RMF
3. Provide associated verification methods and plans to support developmental and operational cyber T&E
4. Support said evaluation of implementation effectiveness by providing defined metrics
5. Integrate with existing DoW acquisition and engineering processes without introducing additional procedural burden

Step 3: Artifact Design



CUI

United States Marine Corps
Cyber Survivability Requirements Guidebook

Prepared by:
MCTSSA Cyber Assessment Branch
Marine Corps Tactical Systems Support Activity (MCTSSA)
Camp Pendleton, California

Controlled by: MCTSSA
CUI Category: CTI
Distribution Statement: D
POC: Name Here

Distribution Statement D. Distribution authorized to the Department of Defense and U.S. DoD contractors only; CTI; October 2023. Other requests for this document shall be referred to the Commanding Officer, MCTSSA, Camp Pendleton, California 92055-5171.

CUI

- CSA Summary
- Performance Specifications
- Verification Methods and Plans
- Metrics
- NIST SP 800-53 Controls

Step 4: Demonstration

- The guidebook was tested on a USMC Program of Record, a vehicle platform
  - Using the Middle Tier Acquisition (MTA) pathway
- The system has a Cyber Survivability Risk Category (CSRC) of 3 (out of 5)
  - Based on the system's Mission Type, Adversary Threat Tier, Cyber Dependence Level, and Impact Level
  - With a CSRC of 3, the system only had to select 5-7 CSAs
- The system selected 7 of the 10 CSAs

Step 5: Evaluation

90% of the platform's cyber performance specifications were directly taken and tailored from the USMC Guidebook

~8 verification methods were mapped to each performance specification on average, establish robust test coverage density

82% Of utilized verification methods were directly taken and tailored from the USMC guidebook

Questions?

Ms. Kathleen Coen
kathleen.coen@usmc.mil
kathleen.coen@nps.edu

Acronyms

- CDD = Capability Development Document
- CSA = Cyber Survivability Attribute
- CSRC = Cyber Survivability Risk Category
- DoW = Department of War
- DSR = Design Science Research
- GAO = Government Accountability Office
- MCTSSA = Marine Corps Tactical Systems Support Activity
- MTA = Middle Tier Acquisition
- NPS = Naval Postgraduate School
- RFI = Request for Information
- RFP = Request for Proposal
- RMF = Risk Management Framework
- RTM = Requirements Traceability Matrix
- SRD = System Requirements Document
- SS KPP = System Survivability Key Performance Parameter
- T&E = Test and Evaluation
- USMC = United States Marine Corps