USD(R&E)

Secure Cyber Resilient Engineering (SCRE) Practice

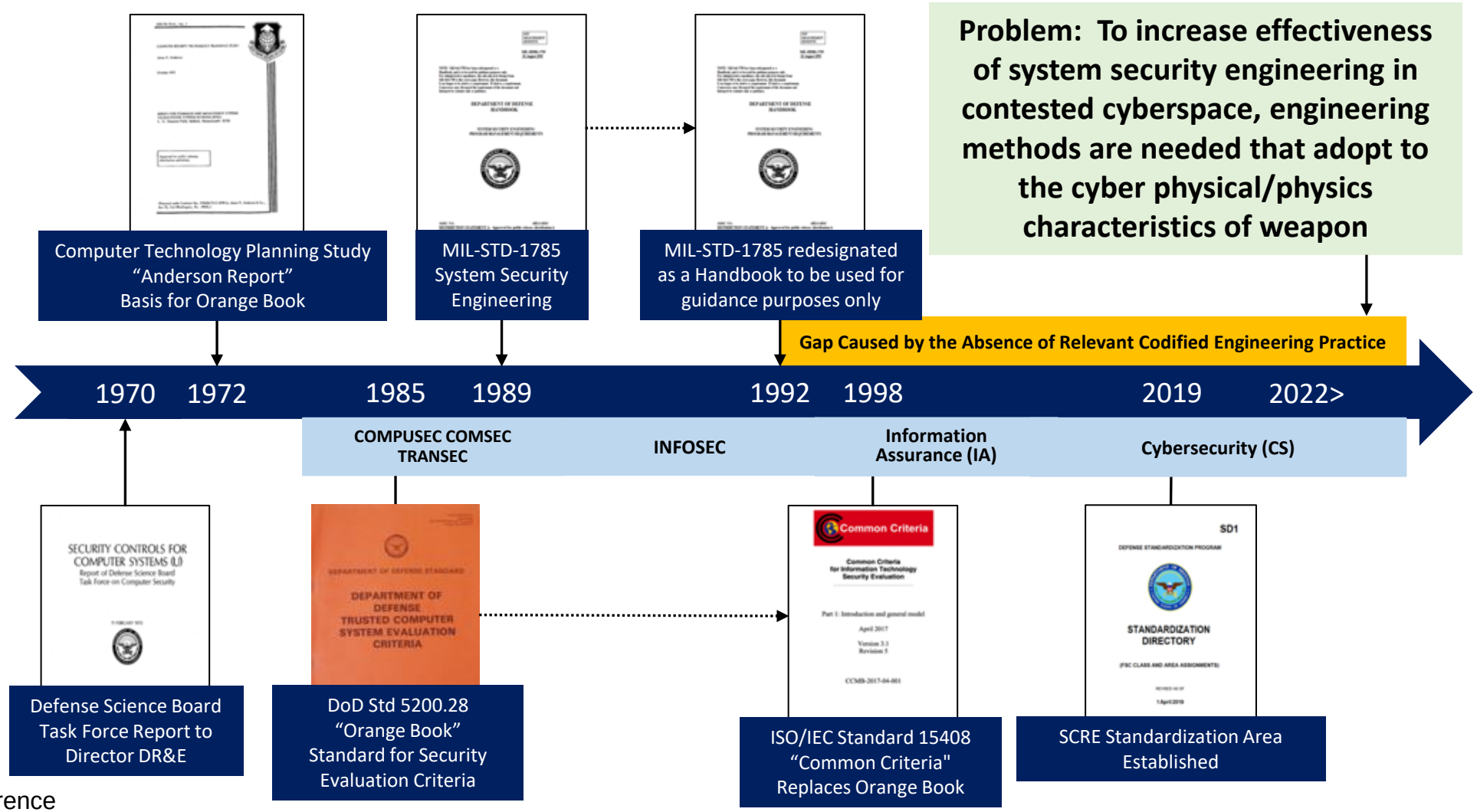
Standardizing the SCRE Practice

Presented to NDIA Systems and Mission Engineering Conference
Orlando, Florida
November 2022

Melinda Reed
Director, Systems Security
Office of Under Secretary of Defense for Research and Engineering
Science and Technology Program Protection

Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation

DoD System Security Engineering Timeline



While Times Have Changed…
The Fundamental Engineering Problem Remains…

How do we know our approach works?

Assessing Performance Across the System Life Cycle

1970's

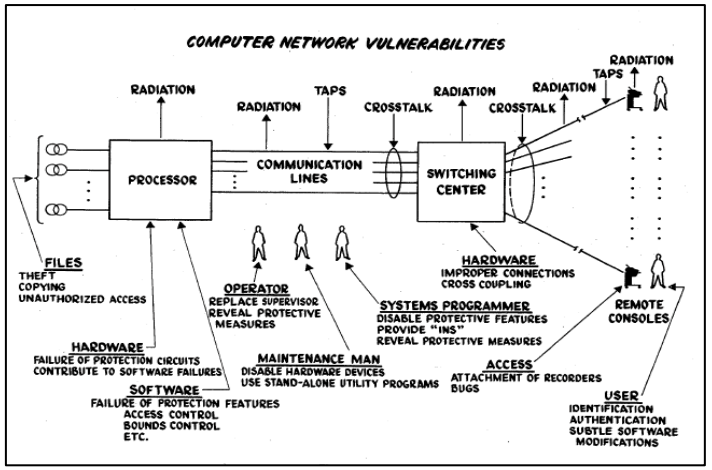


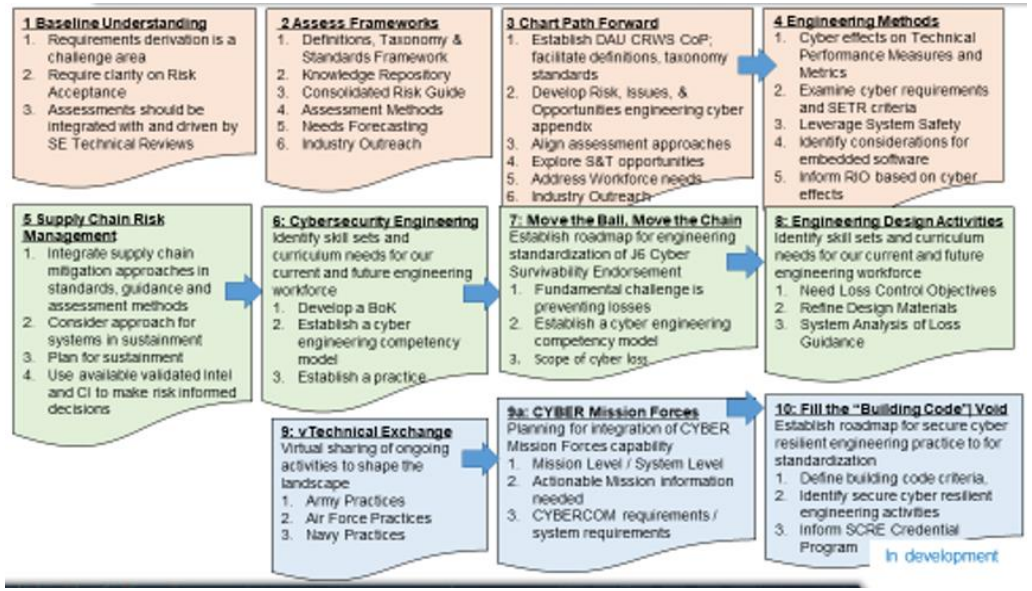
Figure 3 - "Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security", 1970

> 2030's

SCRE Goals

1. Structured standards and methods to evaluate requirements for testability, traceability, and de-confliction
2. Traceable evidence for appropriate decisions at every level of design
3. Cumulative evidence acquired through verification methods conducted by engineering and test organizations
4. Operational Behavior Prediction and Recovery: real time monitoring, just-in-time prediction, and mitigation of undesired decisions and behaviors
5. Reusable assurance arguments based on previous evidence "building blocks"

Implementation: Engineering Cyber Resilient Weapon Systems Workshop

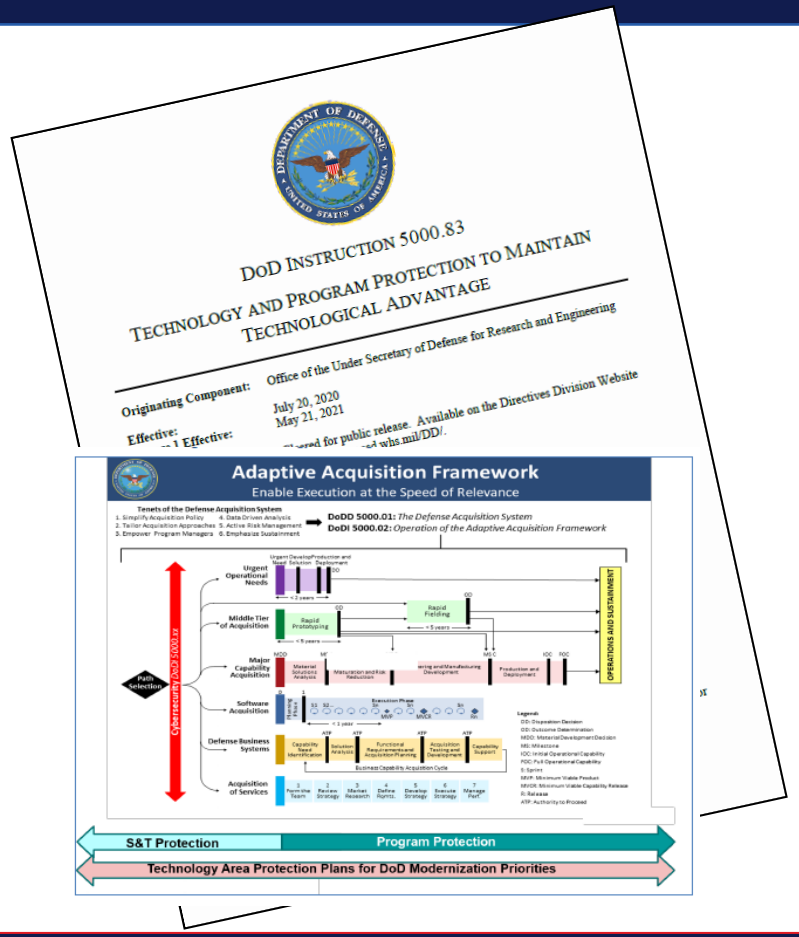


Collaboration Forum with Government, Industry, and Academia that builds upon each workshop to address challenges and lessons learned

March 2017: SCRE Standardization Area
– Defense Standardization Program

- **August 2018: Cyber Resilient Weapon System (CRWS) Workshop Report: Preparing the Engineering Workforce for Cybersecurity Challenges**
- **March 2019: Draft SCRE Competency Model**
- **November 2020: Defense Acquisition University Approved to Establish the SCRE Credential Program**
- **June 2021: CRWS Body of Knowledge Deployment**

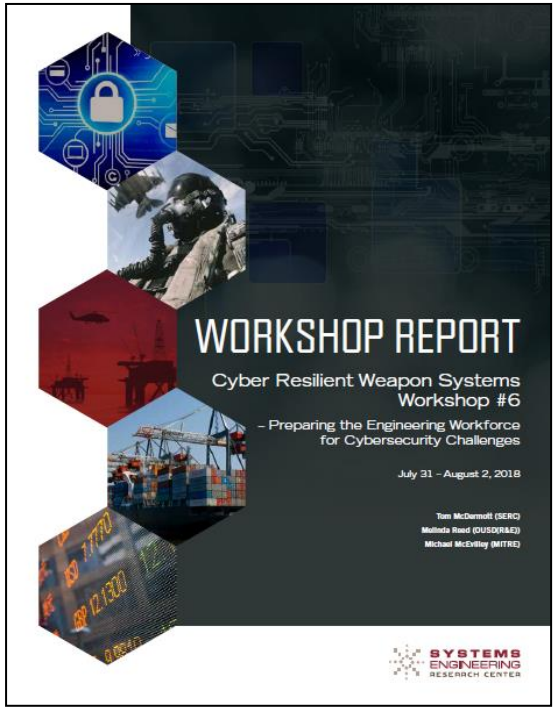
DoDI 5000.83: Technology and Program Protection to Maintain Technological Advantage



- **Establishes responsibilities and procedures for *S&T managers and engineers* to manage system security and cybersecurity technical risks to:**
  - DoD-sponsored research and technology
  - DoD warfighting capabilities
- **System security and cybersecurity technical risks include:**
  - Hardware, software, supply chain exploitation
  - Cyber and cyberspace vulnerabilities
  - Reverse engineering, anti-tamper
  - Controlled technical information / data exfiltration
- **Introduces S&T protection and Technology Area Protection Plans**
- **Points to engineering and test and evaluation issuance**
- **Aligns Program protection planning with acquisition pathways**

Design for security and cyber resiliency includes allocation of requirements to the system architecture and design and assess the design for vulnerabilities

SCRE: Design for Security and Cyber Resilience

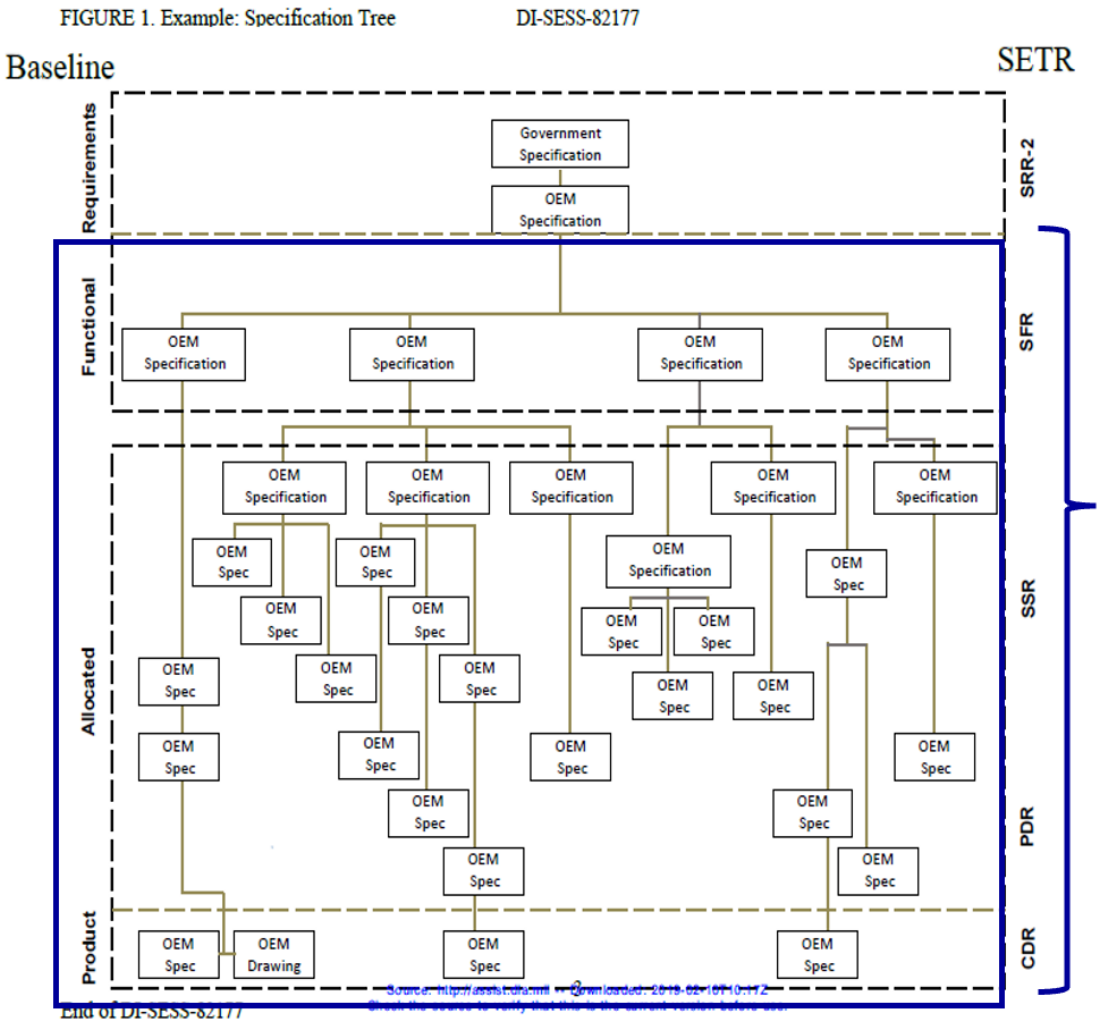


"Gap: Engineering domain knowledge, methods, and tools have not yet fully addressed the effect cyberspace has on for designing and evaluating safe and secure achievement of capability performance measures" – CRWS 6 Workshop Report

- **Develop application specific interpretation guides and use these to drive education and training outcomes**
- **Increase consistency and repeatability of engineering approaches, methods, tools, and outcomes; improve efficiency and effectiveness of safe and secure engineering practice**
- **Improve communication of requirements, methods, and tools, across government, industry, academia, and military operations and sustainment stakeholders**

A secure and cyber resilient system is one that can deliver required capability in a secure manner under the presence of adverse conditions

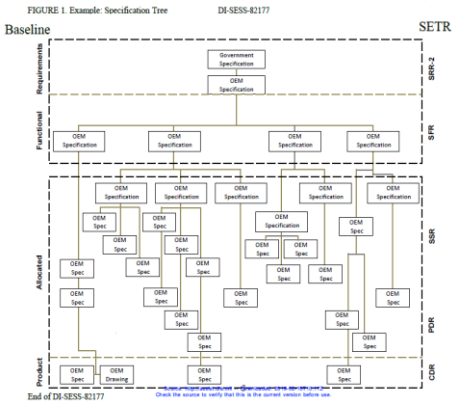
Approach to Codify the SCRE Practice



DoDI 5000.83 Expectations

- **Requirements**
  - Derive and include cybersecurity, security, and other system requirements into system performance specifications
  - Incorporate the derived requirements, design characteristics, and verification methods in the technical baseline and system requirements traceability verification matrix
  - Maintain bi-directional traceability among requirements throughout the system lifecycle
- **Design**
  - Allocate cybersecurity and related system security requirements to the system architecture and design
  - Manages access to, and use of, the system and system resources
  - Has a structure sufficient to protect and preserve system functions or resources
  - Maintains priority system functions under adverse conditions
  - Is configurable to minimize exposure of vulnerabilities that could adversely impact system function, intended operational use driven, and mission objectives.
  - Monitors, detects, and responds to security anomalies
  - Interfaces with supporting systems and external networks and external services
- **Analysis**
  - Assess the design for vulnerabilities

SCRE Activities: Engineering Method



Requirements Analysis
- Analyze capability and adversity driven by mission, operations, sustainment, and environments
- Identify functional requirements
- Define/refine performance and design constraint requirements

System Analysis
- Trade studies
- Effectiveness analysis
- Adversity-driven loss analysis
- Risk, issue, and opportunity analysis

Requirements Loop

Functional Analysis/Allocation
- Decompose to lower-level functions
- Allocate performance and other limiting requirements to all functional levels
- Define/refine functional interfaces
- Define/refine/integrate functional architecture

Design Loop

Verify

Synthesis
- Transform architecture (functional to physical)
- Define alternative system concepts, configuration items, and system elements
- Select preferred product and process solutions
- Define/refine physical interfaces

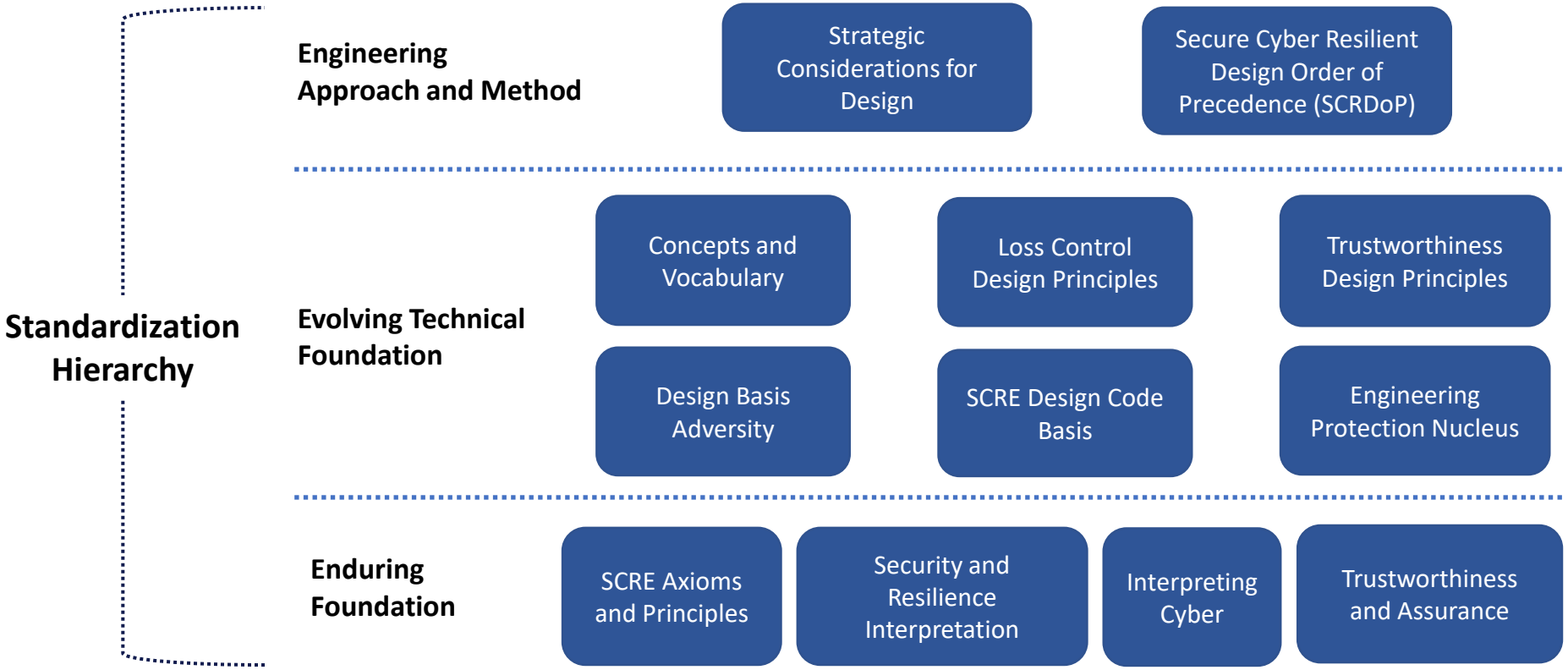
SCRE: Establishing Disciplines and Practices

- **Synergy with System Safety**
  - Adopt approaches and methods of system safety to establish secure cyber resilient engineering
- **System Resilience**
  - Characterize resilience as a graph of delivery of capability over time
  - Develop concept of resilience scenario and patterns expressing resilience in system requirements
- **System Security**
  - Characterize security as a control function to enforce authorized behaviors and outcomes and to protect against loss
  - Develop patterns expressing security in system requirements
- **Loss-Driven Protection Control**
  - Loss is the basis for security activities and judgments
  - Protection needs exercise control to prevent the occurrence of loss and to limit the extent of loss effects
- **Assured Trustworthy Secure Design**
  - Identify idealized design foundations and principles for security
  - Define multidisciplinary-influenced principles that underlie assured trustworthy secure system design
- **Assurance, Confidence, Risk**
  - Assurance: Justified confidence that a claim has been or will be achieved [IEEE 15026]
  - Insufficient confidence translates to risk
    - DoD MIL-STD 882E “Level of Rigor”
    - NASA System Safety “Assurance Deficit”
  - Differentiate
    - Known, insufficiently known, and unknown scenarios that contribute to risk
    - Risk and issue for security/cybersecurity
- **Software Contribution to Risk**
  - Uncertainty about composed software emergent behaviors and side-effects drives risk

SCRE: Standardization Approach

Engineering Approach and Method	Descriptive statement of engineering process, activities, and tasks
Evolving Technical Foundation	The basis of a standard and associated guidance: terms, principles, concepts, etc., that will evolve as appropriate as the practice evolves in response to advances in technology, capability, methods, tools, and the understanding of adversity and how to control adversity and its effects
Enduring Principled Foundation	Core ideas, concepts, philosophy, and interpretations that persist and are not likely to undergo significant change or evolution over time

SCRE: Technical Whitepapers



Provides basis for consensus building

Peer Review Through Engineering CRWS Workshops

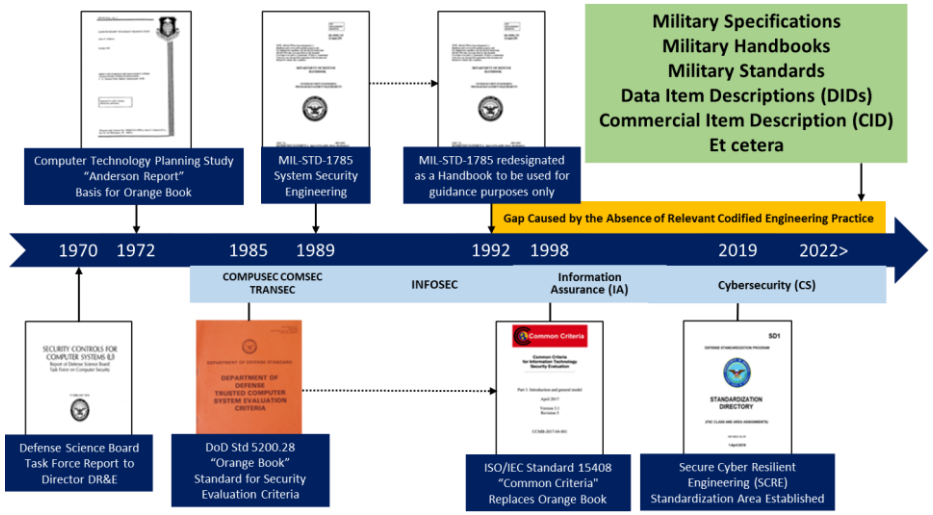
- **Design Code Criteria**
  - Assess, validate, alter the strawman criteria provided
- **Derivation and decomposition of protection requirements**
  - Identify the activities and tasks
- **Assured trustworthy design**
  - Identify the activities and tasks
- **SCRE Analyses**
  - Assess, validate, alter the strawman guidance provided

Advancing the Practice

CRWS Workshops, NDIA Systems Security Engineering Working Group, and other community engagements

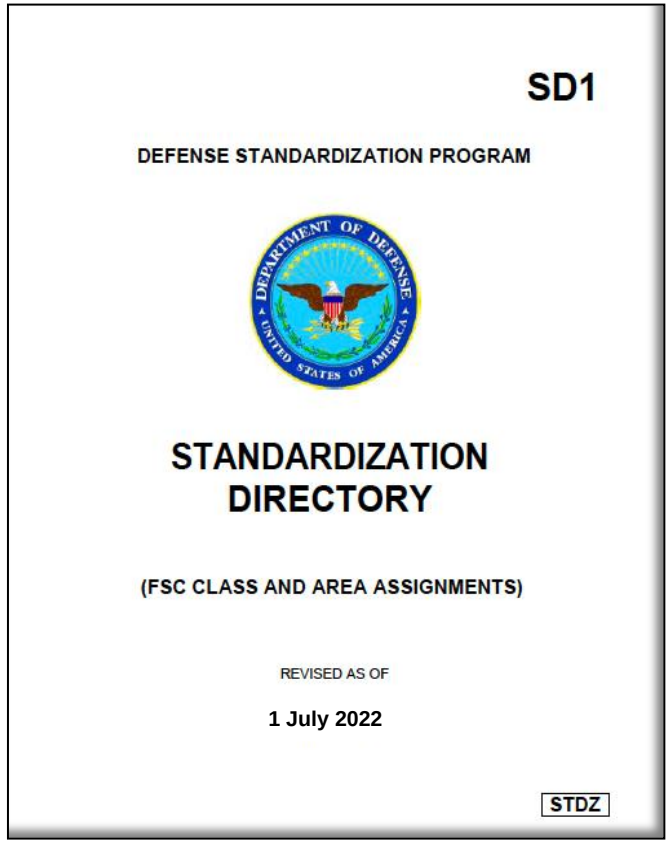
Inform future

Whitepapers and (future) draft guides and other products



Guidebooks
Military Specifications
Military Handbooks
Military Standards
Data Item Descriptions (DIDs)
etc.

SCRE Standardization Area


SD1

DEFENSE STANDARDIZATION PROGRAM

STANDARDIZATION DIRECTORY

(FSC CLASS AND AREA ASSIGNMENTS)

REVISED AS OF

1 July 2022

STDZ

SCRE Area Category

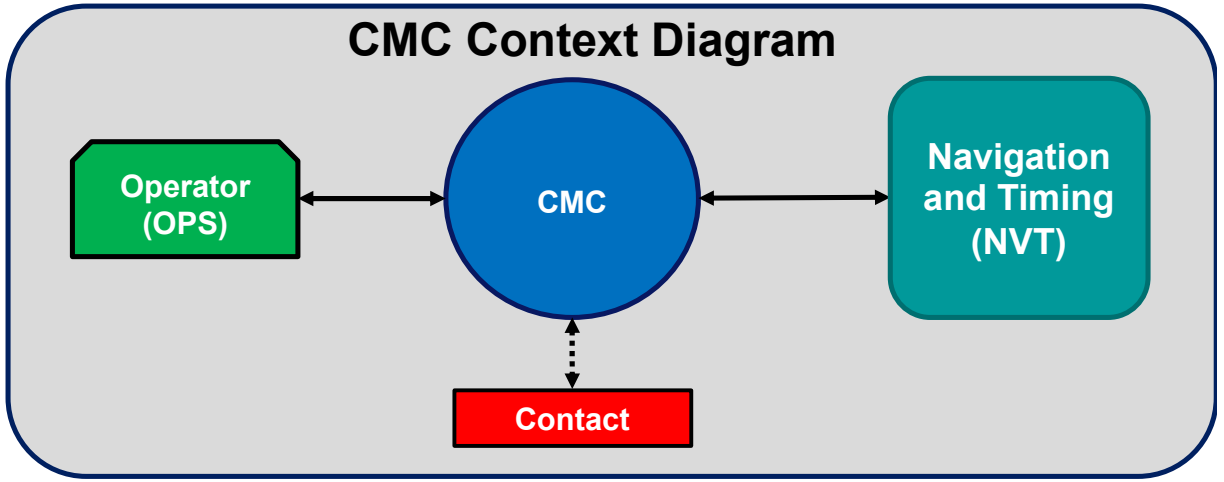
- Covers the ***integration of life cycle security and protection considerations*** in the requirements, design, test, demonstration, operations, maintenance, sustainment, and disposal of military systems that operate in physical and cyberspace operational domains

- Specifically encompasses the standards, specifications, methods, practices, techniques, and data requirements ***for the security aspects of systems engineering*** activities executed and artifacts produced, with explicit consideration of malicious and non-malicious adversity

Defense Standardization Program Standards Area for SCRE Engineering Technologies, Disciplines, and Practices

Next Steps

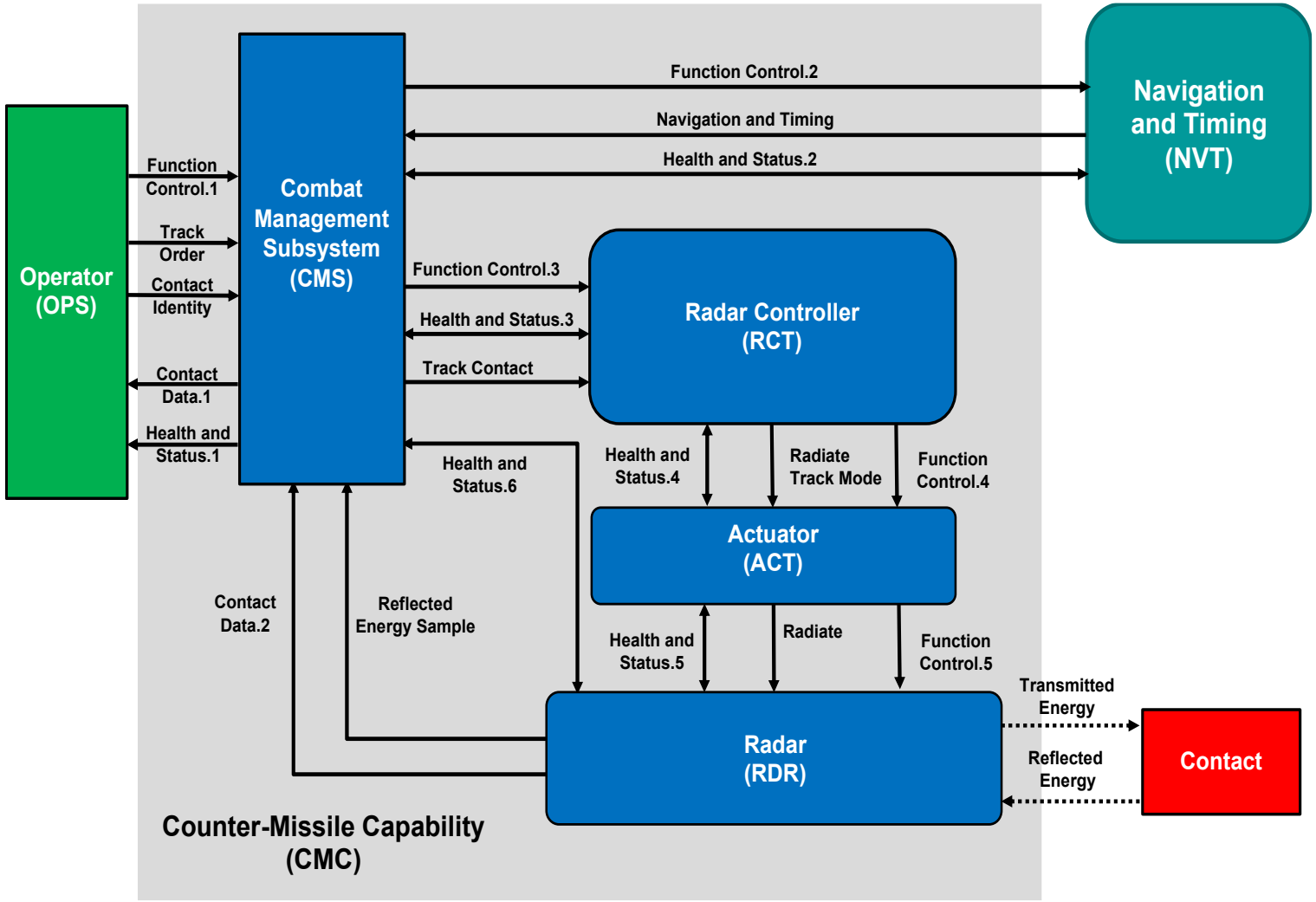
- **Analysis of CRWS 10 outcomes**
- **Continued work with the Cybersecurity Industry Technical Advisory Group (CITAG)**
- **Additional CRWS Workshops**
- **Release of whitepapers for adoption to CRWS BoK**



Engineering Cyber Resilient Weapon System Workshop Notional Use Case: Counter-Missile Capability

Questions?

Notional Use Case



Engineering Cyber Resilient Weapon System (CRWS) Workshop Notional Use Case: Counter-Missile Capability