USD(R&E)

# Secure Cyber Resilient Engineering (SCRE) Practice

## Update on Standardizing the SCRE Practice

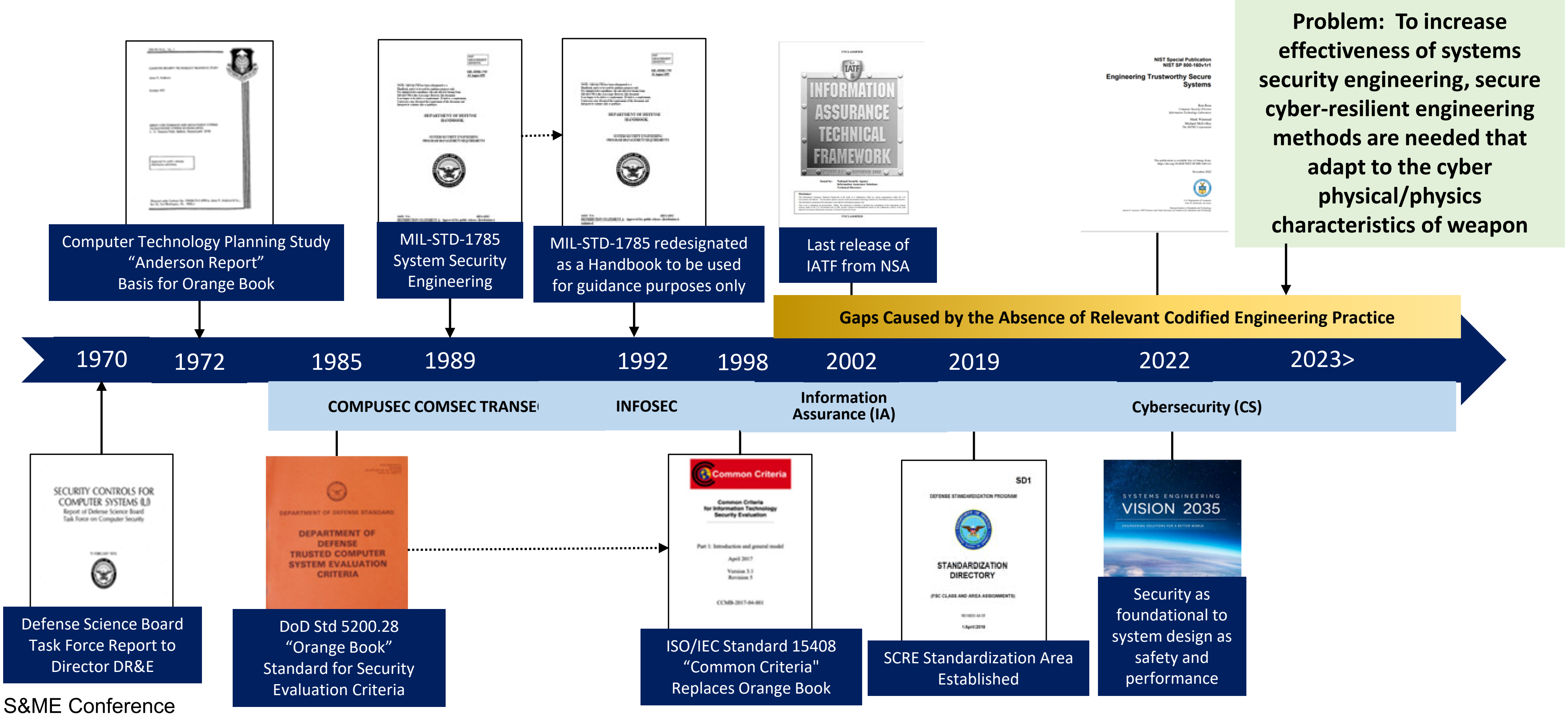
Presented to NDIA Systems and Mission Engineering Conference
Norfolk, Virginia
October 2023

Melinda Reed
Director, System 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

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

# DoD-centric System Security Engineering Timeline



Problem: To increase effectiveness of systems security engineering, secure cyber-resilient engineering methods are needed that adapt to the cyber physical/physics characteristics of weapon

1970
1972
1985
1989
1992
1998
2002
2019
2022
2023>
Gaps Caused by the Absence of Relevant Codified Engineering Practice
COMPUSEC COMSEC TRANSE
INFOSEC
Information Assurance (IA)
Cybersecurity (CS)

Computer Technology Planning Study<br>
"Anderson Report"<br>
Basis for Orange Book

MIL-STD-1785<br>
System Security<br>
Engineering

MIL-STD-1785 redesignated as a Handbook to be used for guidance purposes only

INFORMATION ASSURANCE TECHNICAL FRAMEWORK

Last release of IATF from NSA

NIST Special Publication<br>
NIST SP 800-160v1r1<br>
Engineering Trustworthy Secure Systems

SECURITY CONTROLS FOR COMPUTER SYSTEMS (U)<br>
Report of Defense Science Board Task Force on Computer Security

Defense Science Board Task Force Report to Director DR&E

DEPARTMENT OF DEFENSE STANDARD<br>
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

DoD Std 5200.28<br>
"Orange Book"<br>
Standard for Security Evaluation Criteria

Common Criteria<br>
Common Criteria for Information Technology Security Evaluation<br>
Part 1: Introduction and general model<br>
April 2017<br>
Version 3.1<br>
Revision 5<br>
CCMB-2017-04-001

ISO/IEC Standard 15408<br>
"Common Criteria"<br>
Replaces Orange Book

SD1<br>
DEFENSE STANDARDIZATION PROGRAM<br>
STANDARDIZATION DIRECTORY<br>
(FSC CLASS AND AREA ASSIGNMENTS)

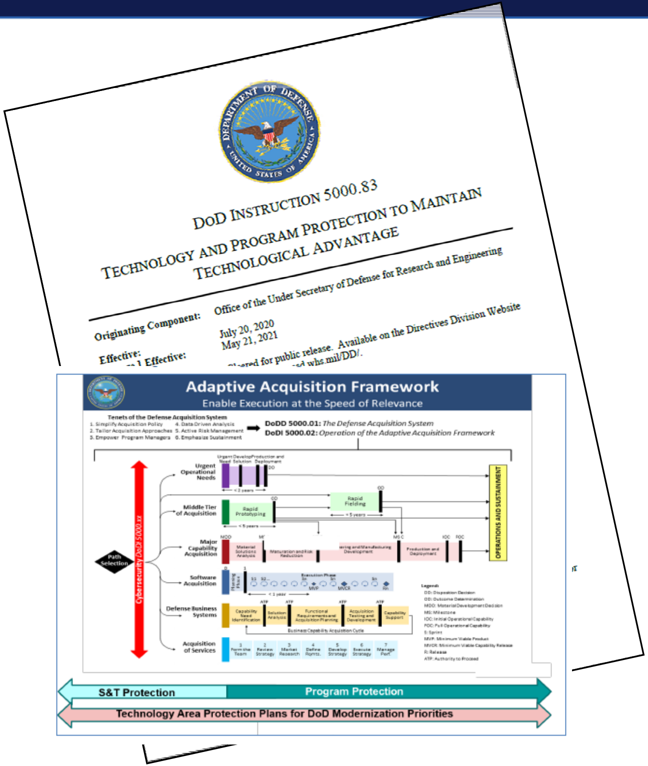
SCRE Standardization Area Established

SYSTEMS ENGINEERING<br>
VISION 2035

Security as foundational to system design as safety and performance

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

# DoDI 5000.83: Technology and Program Protection to Maintain Technological Advantage



DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Originating Component: Office of the Under Secretary of Defense for Research and Engineering

Effective: July 20, 2020

1 Effective: May 21, 2021

leared for public release. Available on the Directives Division Website ed whs.mil/DD/.

Adaptive Acquisition Framework
Enable Execution at the Speed of Relevance
Tenets of the Defense Acquisition System
1. Simplify Acquisition Policy
2. Tailor Acquisition Approaches
3. Empower Program Managers
4. Data Driven Analysis
5. Active Risk Management
6. Emphasize Sustainment
DoDD 5000.01: The Defense Acquisition System
DoDI 5000.02: Operation of the Adaptive Acquisition Framework
Path Selection
Cybersecurity DoDI 5000.xx
Urgent Operational Needs
Urgent Need
Develop Solution
Production and Deployment
DD
< 2 years
Middle Tier of Acquisition
Rapid Prototyping
Rapid Fielding
OD
< 5 years
Major Capability Acquisition
MDD
Material Solutions Analysis
Maturation and Risk Reduction
ering and Manufacturing Development
MS C
Production and Deployment
IOC
FOC
Software Acquisition
Planning Phase
Execution Phase
S1
S2...
Sn
MVP
MVCR
Rn
< 1 year
Defense Business Systems
ATP
Capability Need Identification
Solution Analysis
Functional Requirements and Acquisition Planning
Acquisition Testing and Development
Capability Support
Business Capability Acquisition Cycle
Acquisition of Services
1 Form the Team
2 Review Strategy
3 Market Research
4 Define Rqmts.
5 Develop Strategy
6 Execute Strategy
7 Manage Perf.
OPERATIONS AND SUSTAINMENT
Legend:
DD: Disposition Decision
OD: Outcome Determination
MDD: Material Development Decision
MS: Milestone
IOC: Initial Operational Capability
FOC: Full Operational Capability
S: Sprint
MVP: Minimum Viable Product
MVCR: Minimum Viable Capability Release
R: Release
ATP: Authority to Proceed
S&T Protection
Program Protection
Technology Area Protection Plans for DoD Modernization Priorities

- **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

WORKSHOP REPORT

Cyber Resilient Weapon Systems
Workshop #6

– Preparing the Engineering Workforce
for Cybersecurity Challenges

July 31 – August 2, 2018

Tom McDermott (SERC)
Melinda Reed (OUSD(R&E))
Michael McEvilley (MITRE)

SYSTEMS ENGINEERING RESEARCH CENTER

*"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

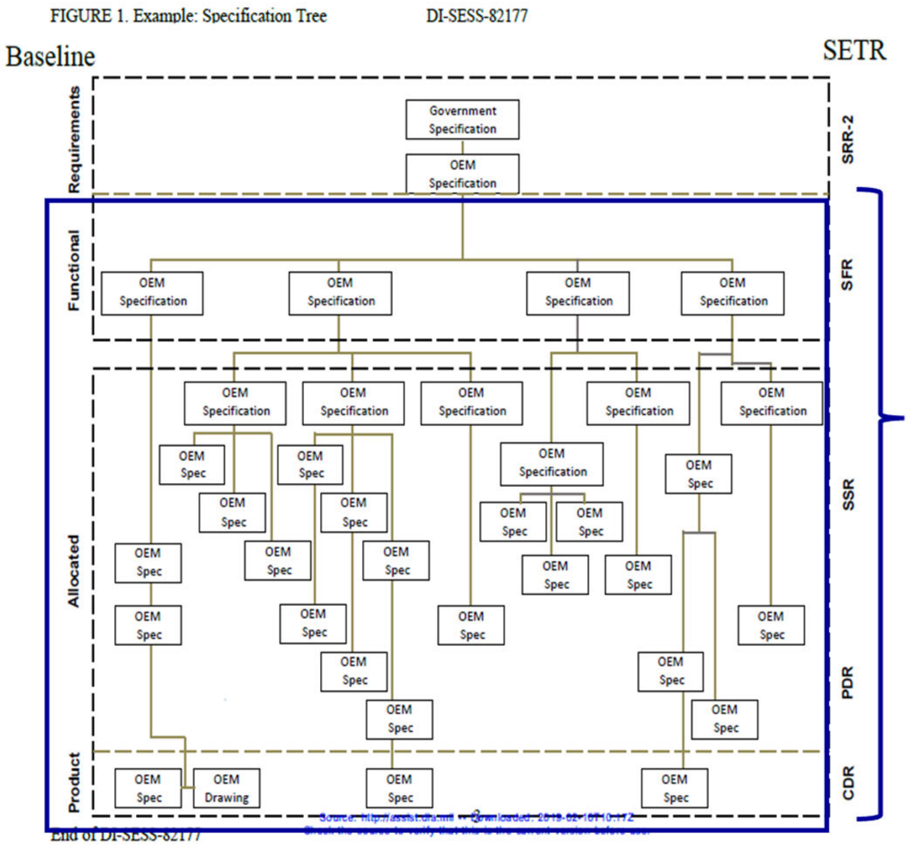


FIGURE 1. Example: Specification Tree DI-SESS-82177

Source: http://assist.dla.mil -- Downloaded: 2019-02-18T10:17Z
Check the source to verify that this is the current version before use.

End of DI-SESS-82177

## 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

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

# Need for A Rising Tide

This Photo by Unknown Author is licensed under CC BY

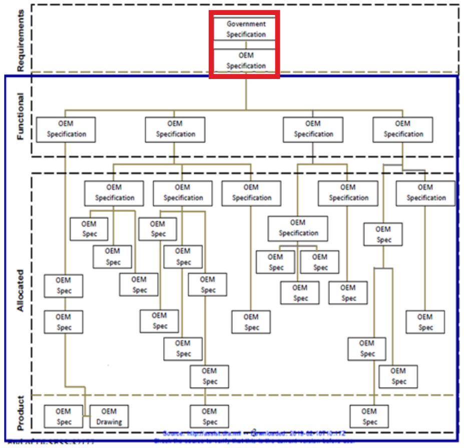
- Industry works across domains, internationally and non-defense
- Workforce development needs are more than DoD
  - Recruitment of workforce by industry partners helped if Knowledge, Skills, and Abilities (KSAs) apply across domains

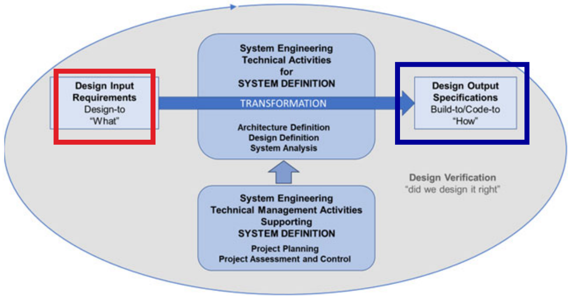
***To build world-class secure and resilient systems, we need to develop a world-class workforce that can engineer inherently safe and secure designs***

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

# SCRE Activities: Engineering Method

## Rooting in International Standards (e.g., ISO/IEC/IEEE 15288:2023) & INCOSE Technical Products




Design Input Requirements
Design-to
"What"

System Engineering Technical Activities for SYSTEM DEFINITION

TRANSFORMATION

Architecture Definition
Design Definition
System Analysis

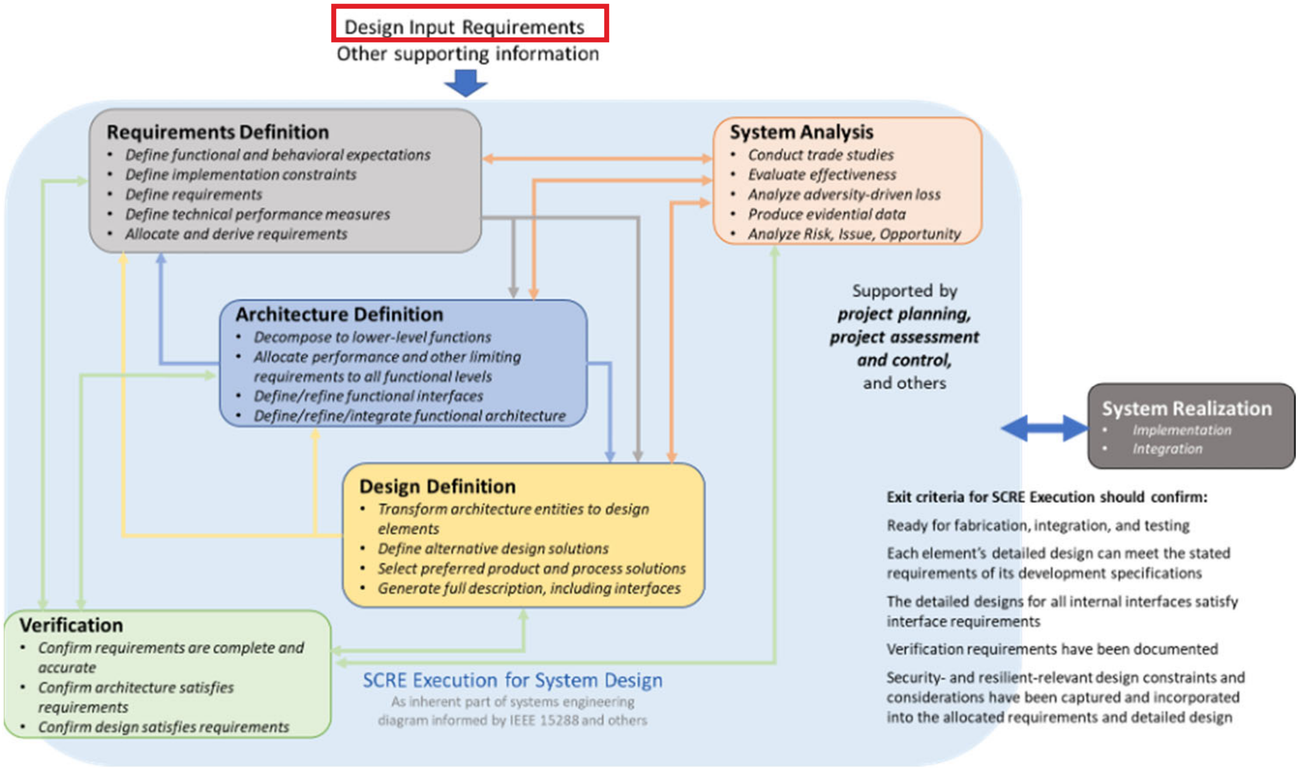
Design Output Specifications
Build-to/Code-to
"How"

System Engineering Technical Management Activities Supporting SYSTEM DEFINITION

Project Planning
Project Assessment and Control

Design Verification
"did we design it right"

Inspired by INCOSE Needs and Requirements Manual (NRM)


Design Input Requirements
Other supporting information

**Requirements Definition**
- *Define functional and behavioral expectations*
- *Define implementation constraints*
- *Define requirements*
- *Define technical performance measures*
- *Allocate and derive requirements*

**System Analysis**
- *Conduct trade studies*
- *Evaluate effectiveness*
- *Analyze adversity-driven loss*
- *Produce evidential data*
- *Analyze Risk, Issue, Opportunity*

**Architecture Definition**
- *Decompose to lower-level functions*
- *Allocate performance and other limiting requirements to all functional levels*
- *Define/refine functional interfaces*
- *Define/refine/integrate functional architecture*

Supported by ***project planning, project assessment and control,*** and others

**System Realization**
- *Implementation*
- *Integration*

**Design Definition**
- *Transform architecture entities to design elements*
- *Define alternative design solutions*
- *Select preferred product and process solutions*
- *Generate full description, including interfaces*

**Verification**
- *Confirm requirements are complete and accurate*
- *Confirm architecture satisfies requirements*
- *Confirm design satisfies requirements*

SCRE Execution for System Design
As inherent part of systems engineering diagram informed by IEEE 15288 and others

**Exit criteria for SCRE Execution should confirm:**

Ready for fabrication, integration, and testing

Each element's detailed design can meet the stated requirements of its development specifications

The detailed designs for all internal interfaces satisfy interface requirements

Verification requirements have been documented

Security- and resilient-relevant design constraints and considerations have been captured and incorporated into the allocated requirements and detailed design

Inspiration – part of ISO/IEC/IEEE 15288:2023's Figure 5

# SCRE: Establishing Discipline and Practice

- **Advance Systems Engineering**
  - Advance SE for contested operational spaces including cyberspace
- **Think Cross-disciplinary**
  - Focus on Loss and Effects to enable
    - 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
    - Synergy across safety, resilience, and security
  - Synergy with System Safety
    - Adopt approaches and methods of system safety
  - System Resilience
    - Characterize resilience as a graph of delivery of capability over time
  - System Security
    - Characterize security as a control function to enforce authorized behaviors and outcomes and to protect against loss and its 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

# SCRE: Standardization Framework

**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**

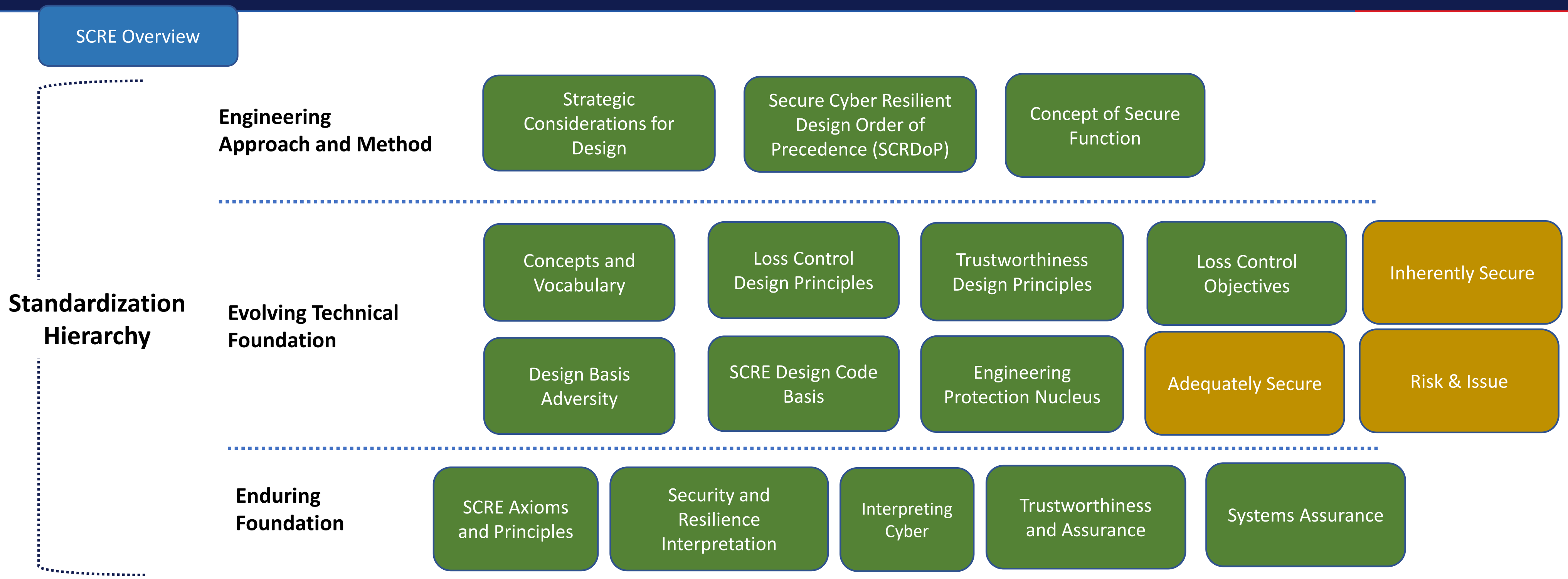
Core ideas, concepts, philosophy, and interpretations that persist and are not likely to undergo significant change or evolution over time

# SCRE: Technical Whitepapers

🟩 Released DoD Distro A

🟦 In revision (previously released D)

🟨 Currently DoD Distro D



🟦 SCRE Overview

**Standardization Hierarchy**

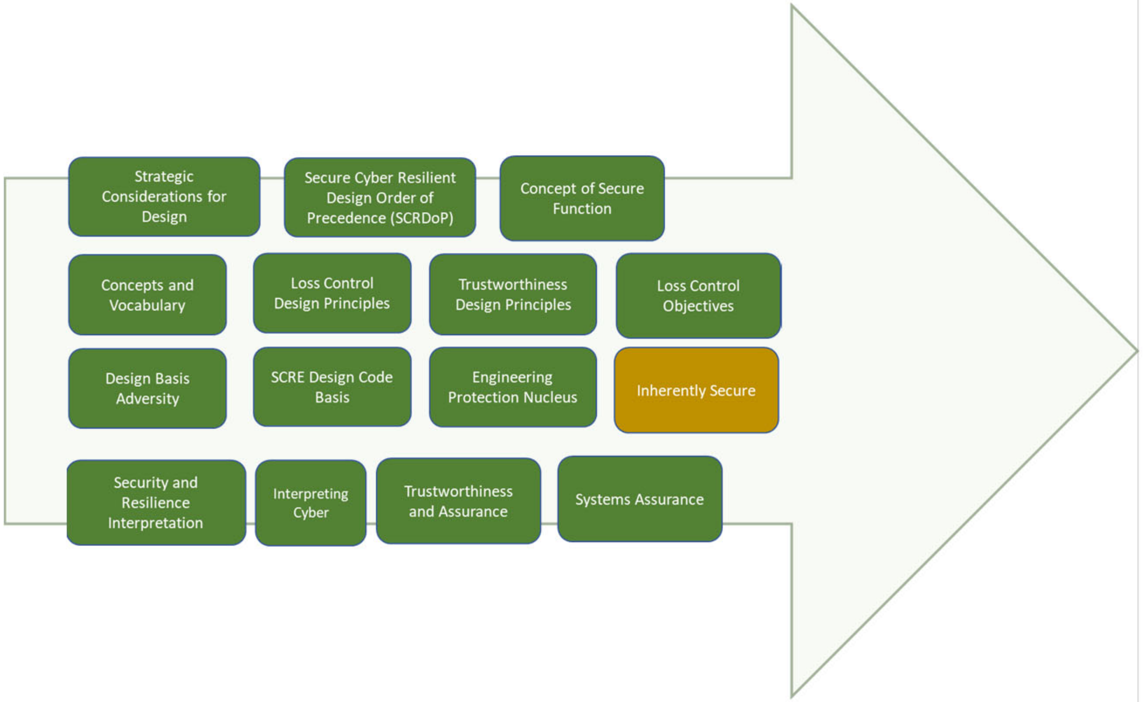
**Engineering Approach and Method**
- 🟩 Strategic Considerations for Design
- 🟩 Secure Cyber Resilient Design Order of Precedence (SCRDoP)
- 🟩 Concept of Secure Function

**Evolving Technical Foundation**
- 🟩 Concepts and Vocabulary
- 🟩 Loss Control Design Principles
- 🟩 Trustworthiness Design Principles
- 🟩 Loss Control Objectives
- 🟨 Inherently Secure
- 🟩 Design Basis Adversity
- 🟩 SCRE Design Code Basis
- 🟩 Engineering Protection Nucleus
- 🟨 Adequately Secure
- 🟨 Risk & Issue

**Enduring Foundation**
- 🟩 SCRE Axioms and Principles
- 🟩 Security and Resilience Interpretation
- 🟩 Interpreting Cyber
- 🟩 Trustworthiness and Assurance
- 🟩 Systems Assurance

***Provides basis for consensus building***

# Pulling it together - Guidance



Strategic Considerations for Design

Secure Cyber Resilient Design Order of Precedence (SCRDoP)

Concept of Secure Function

Concepts and Vocabulary

Loss Control Design Principles

Trustworthiness Design Principles

Loss Control Objectives

Design Basis Adversity

SCRE Design Code Basis

Engineering Protection Nucleus

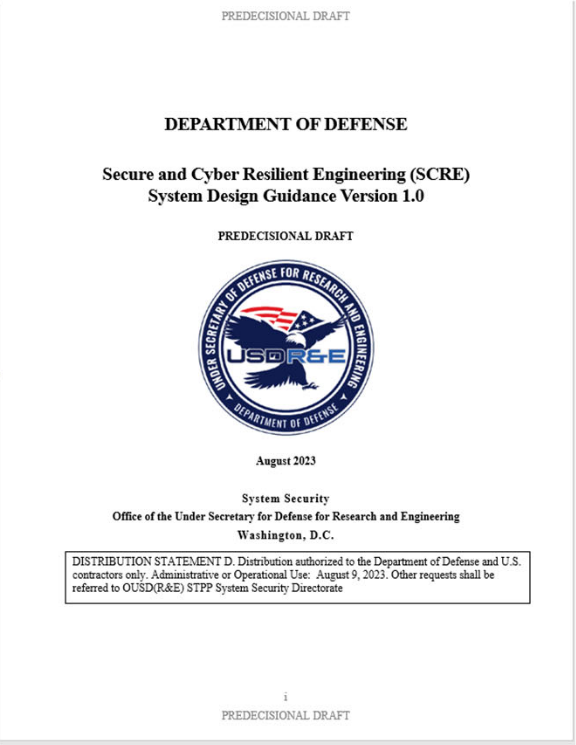
Inherently Secure

Security and Resilience Interpretation

Interpreting Cyber

Trustworthiness and Assurance

Systems Assurance



PREDECISIONAL DRAFT

**DEPARTMENT OF DEFENSE**

**Secure and Cyber Resilient Engineering (SCRE)**
**System Design Guidance Version 1.0**

**PREDECISIONAL DRAFT**

**August 2023**

**System Security**
**Office of the Under Secretary for Defense for Research and Engineering**
**Washington, D.C.**

DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. contractors only. Administrative or Operational Use: August 9, 2023. Other requests shall be referred to OUSD(R&E) STPP System Security Directorate

i

PREDECISIONAL DRAFT

***Separate Presentation on the Design Guidance at this Conference***

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

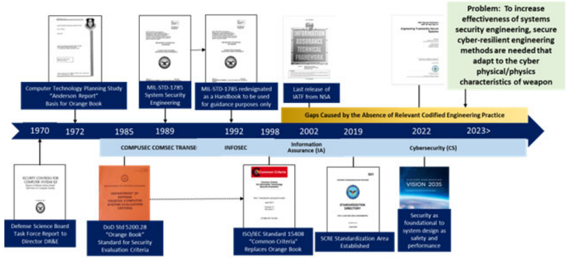
# Cyber Resilient Weapon Systems Workshop #12
# Industry Perspectives

- **Plenary Topics include**
  - **Design Code Basis and Role of System Analysis**
  - **MIL-HBK 516 Recommendations and Challenges**
  - **Digital Engineering Topics**
  - **Foundational Skills**
- **Breakouts include**
  - **Training and Education**
  - **Digital Engineering for SCRE**
  - **Airworthiness and Security Standardization**

# Advancing the Systems Engineering Practice is Teamwork

CRWS Workshops, NDIA Systems Security Engineering Working Group, INCOSE, Gov't partners, and other community engagements

Whitepapers, Design Guidance, and future draft guides and other products


Problem: To increase effectiveness of systems security engineering, secure cyber-resilient engineering methods are needed that adapt to the cyber physical/physics characteristics of weapon
Computer Technology Planning Study "Anderson Report" Basis for Orange Book
MIL-STD-1785 System Security Engineering
MIL-STD-1785 redesignated as a Handbook to be used for guidance purposes only
Last release of IATF from NSA
Gaps Caused by the Absence of Relevant Codified Engineering Practice
1970
1972
1985
1989
1992
1998
2002
2019
2022
2023>
COMPUSEC COMSEC TRANSE
INFOSEC
Information Assurance (IA)
Cybersecurity (CS)
Defense Science Board Task Force Report to Director DR&E
DoD Std 5200.28 "Orange Book" Standard for Security Evaluation Criteria
ISO/IEC Standard 15408 "Common Criteria" Replaces Orange Book
SCRE Standardization Area Established
VISION 2035
Security as foundational to system design as safety and performance

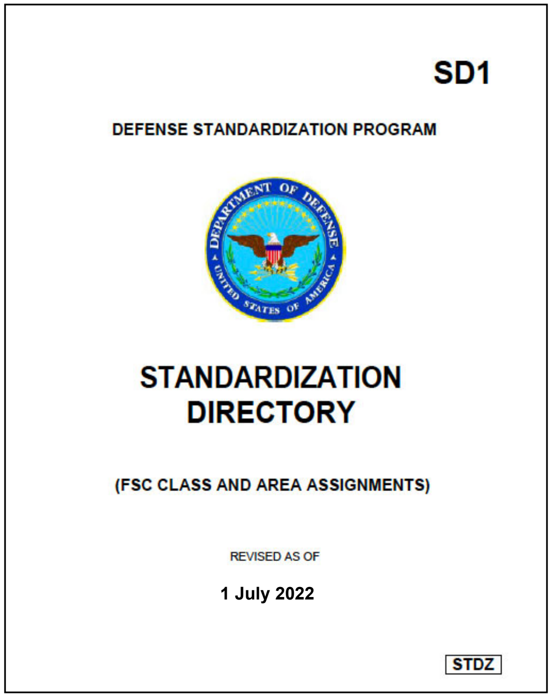
Other societies, Academic Partners, etc.

Conference Papers, Journal Articles, Tutorials, Presentations

All informing future

Guidebooks
Military Specifications
Military Handbooks
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

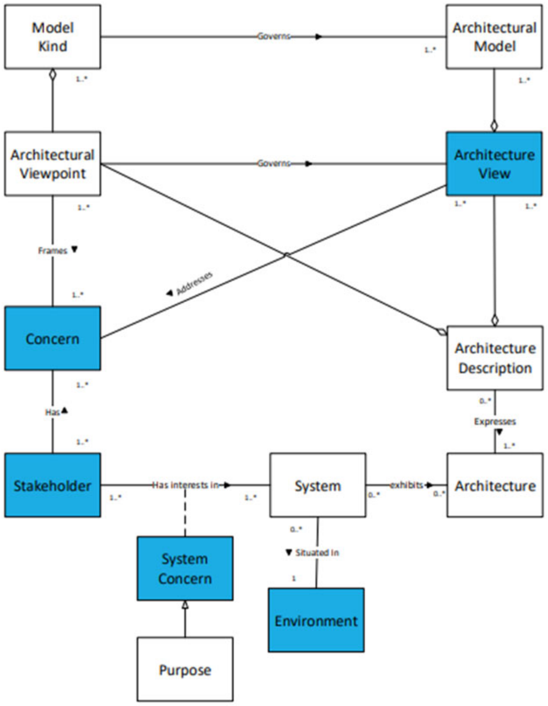
- Covers the ***integration of life cycle security and protection considerations*** in the requirements, design, test, demonstration, operations, maintenance, sustainment, and disposal of military systems that operate in physical and cyberspace operational domains

- 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

- **Continue to leverage *and influence* INCOSE Products related to SCRE**
- **Continue to utilize workshops to inform SCRE standardization efforts**
- **Explore additionally opportunities to engage in Security in Future of Systems Engineering activities**
- **Will make accessible, additional SCRE whitepapers, guidance, and implementation guidelines when ready**



From *Recommendation for System Analysis in Support of Secure Architecture in Acquisition* (April 2022).
By the Architecture Analysis Working Group of the Cybersecurity Technical Advisory Group (CITAG)

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

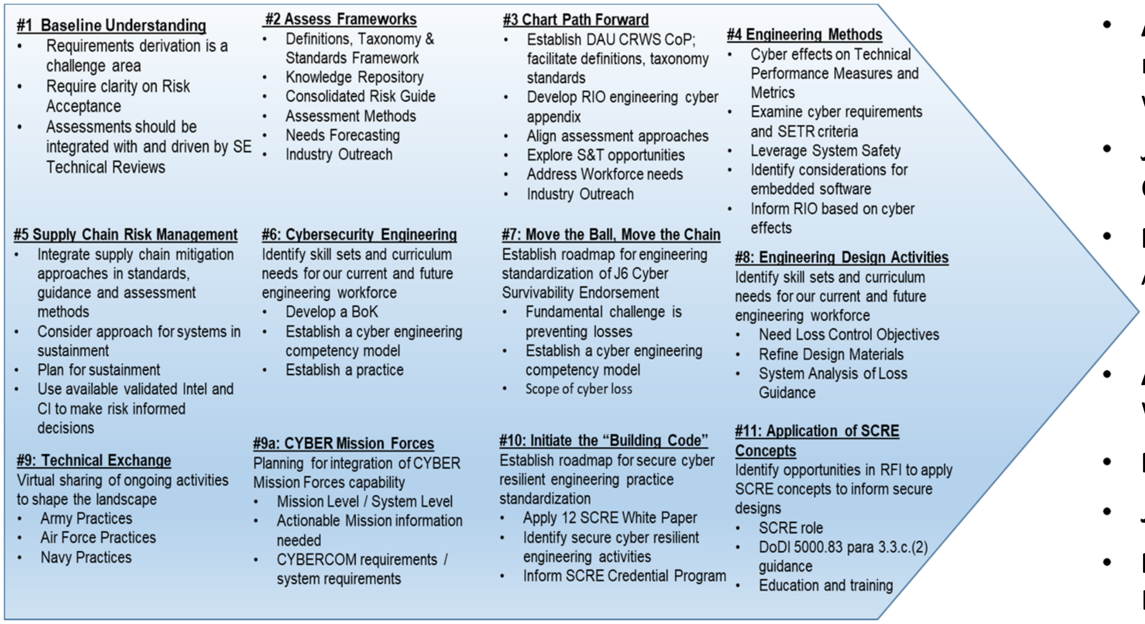
# Questions?

***Melinda Reed*** ***melinda.k.reed.civ@mail.mil***

***Mark Winstead*** ***mwinstead@mitre.org***

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

# Engineering Cyber Resilient Weapon Systems Workshop Series



**#1 Baseline Understanding**
- Requirements derivation is a challenge area
- Require clarity on Risk Acceptance
- Assessments should be integrated with and driven by SE Technical Reviews

**#2 Assess Frameworks**
- Definitions, Taxonomy & Standards Framework
- Knowledge Repository
- Consolidated Risk Guide
- Assessment Methods
- Needs Forecasting
- Industry Outreach

**#3 Chart Path Forward**
- Establish DAU CRWS CoP; facilitate definitions, taxonomy standards
- Develop RIO engineering cyber appendix
- Align assessment approaches
- Explore S&T opportunities
- Address Workforce needs
- Industry Outreach

**#4 Engineering Methods**
- Cyber effects on Technical Performance Measures and Metrics
- Examine cyber requirements and SETR criteria
- Leverage System Safety
- Identify considerations for embedded software
- Inform RIO based on cyber effects

**#5 Supply Chain Risk Management**
- Integrate supply chain mitigation approaches in standards, guidance and assessment methods
- Consider approach for systems in sustainment
- Plan for sustainment
- Use available validated Intel and CI to make risk informed decisions

**#6: Cybersecurity Engineering**
Identify skill sets and curriculum needs for our current and future engineering workforce
- Develop a BoK
- Establish a cyber engineering competency model
- Establish a practice

**#7: Move the Ball, Move the Chain**
Establish roadmap for engineering standardization of J6 Cyber Survivability Endorsement
- Fundamental challenge is preventing losses
- Establish a cyber engineering competency model
- Scope of cyber loss

**#8: Engineering Design Activities**
Identify skill sets and curriculum needs for our current and future engineering workforce
- Need Loss Control Objectives
- Refine Design Materials
- System Analysis of Loss Guidance

**#9: Technical Exchange**
Virtual sharing of ongoing activities to shape the landscape
- Army Practices
- Air Force Practices
- Navy Practices

**#9a: CYBER Mission Forces**
Planning for integration of CYBER Mission Forces capability
- Mission Level / System Level
- Actionable Mission information needed
- CYBERCOM requirements / system requirements

**#10: Initiate the "Building Code"**
Establish roadmap for secure cyber resilient engineering practice standardization
- Apply 12 SCRE White Paper
- Identify secure cyber resilient engineering activities
- Inform SCRE Credential Program

**#11: Application of SCRE Concepts**
Identify opportunities in RFI to apply SCRE concepts to inform secure designs
- SCRE role
- DoDI 5000.83 para 3.3.c.(2) guidance
- Education and training

**" It is true you can build a [securer] system by building [secure] parts. However, you can't build a truly [secure] system without having [secure] parts interacting with each other in a [secure] manner" …**

*John A. Thomas in introduction article to INCOSE Insight Vol 16 Issue 2 July 2013 Special Issue on SSE*

- **August 2016:** Established CRWS Workshop identify engineering methods, standards and grow the workforce to engineer cyber resilient weapon systems
- **January 2017**: Issued DTM 17-001/DoDI 5000.02 Enclosure 14 – Cybersecurity in the Defense Acquisition System
- **March 2017:** Secure Cyber Resilient Engineering (SCRE) Standardization Area
  - – Defense Standardization Program
- **August 2018:** CRWS Workshop Report: Preparing the Engineering Workforce for Cybersecurity Challenges
- **March 2019:** Draft SCRE Competency Model
- **July 2020:** Issued DoDI 5000.83; codified SCRE in policy
- **November 2020:** Defense Acquisition University (DAU) Approved to Establish the SCRE Credential Program
- **June 2021:** CRWS Book of Knowledge Deployment
- **August 2022:** 12 Secure Cyber Resilient Engineering Design Code White Papers
- **November 2022:** NIST adopted efforts in NIST SP 800-160 volume 1

**Collab with Govt, industry, and academia stakeholders to address recurring challenges**