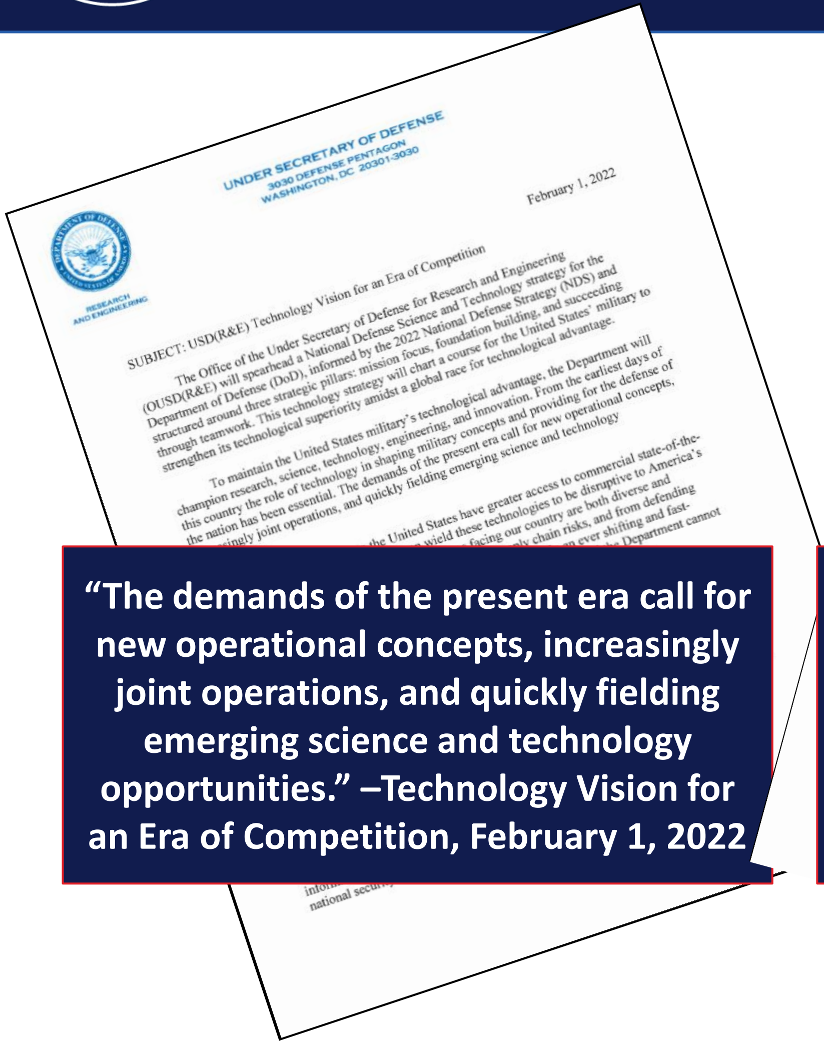
USD(R&E)

Program Protection and Secure Cyber Resilient Engineering Initiatives

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

R&E Mission – Technology Vision in the Era of Competition



UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH AND ENGINEERING

February 1, 2022

SUBJECT: USD(R&E) Technology Vision for an Era of Competition

The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) will spearhead a National Defense Science and Technology strategy for the Department of Defense (DoD), informed by the 2022 National Defense Strategy (NDS) and structured around three strategic pillars: mission focus, foundation building, and succeeding through teamwork. This technology strategy will chart a course for the United States' military to strengthen its technological superiority amidst a global race for technological advantage.

To maintain the United States military's technological advantage, the Department will champion research, science, technology, engineering, and innovation. From the earliest days of this country the role of technology in shaping military concepts and providing for the defense of the nation has been essential. The demands of the present era call for new operational concepts, increasingly joint operations, and quickly fielding emerging science and technology

the United States have greater access to commercial state-of-the-
wield these technologies to be disruptive to America's
facing our country are both diverse and
ply chain risks, and from defending
an ever shifting and fast-
Department cannot

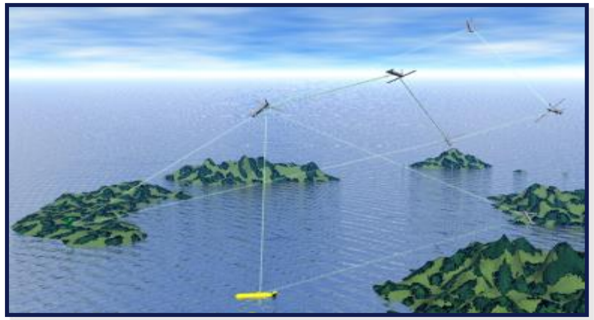
infor
national secu

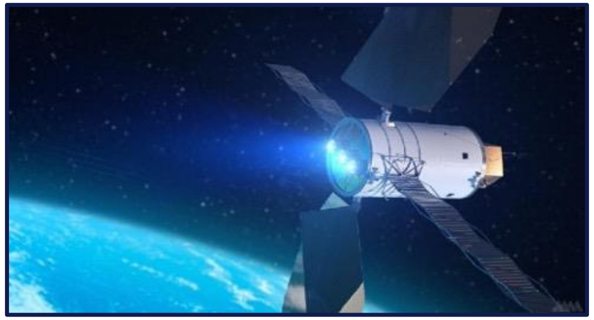
"The demands of the present era call for new operational concepts, increasingly joint operations, and quickly fielding emerging science and technology opportunities." –Technology Vision for an Era of Competition, February 1, 2022

NATIONAL DEFENSE SCIENCE & TECHNOLOGY STRATEGY 2023

UNITED STATES DEPARTMENT OF DEFENSE

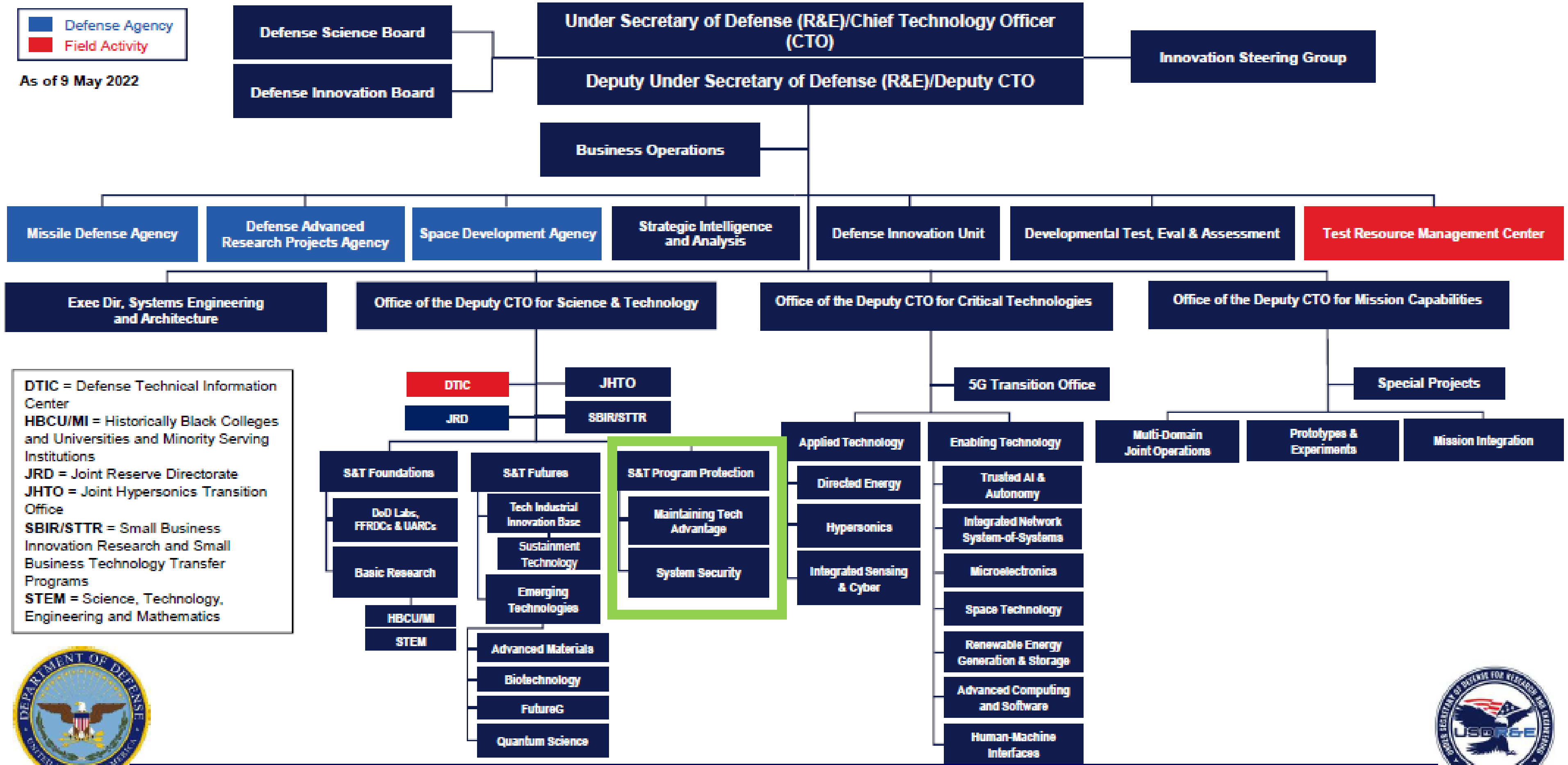
- Focus on the Joint Mission
- Create and field capabilities at speed and scale
- Ensure the foundations for research and development





Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Organization



🟦 Defense Agency
🟥 Field Activity

As of 9 May 2022

Under Secretary of Defense (R&E)/Chief Technology Officer (CTO)

Deputy Under Secretary of Defense (R&E)/Deputy CTO

Defense Science Board

Defense Innovation Board

Innovation Steering Group

Business Operations

Missile Defense Agency

Defense Advanced Research Projects Agency

Space Development Agency

Strategic Intelligence and Analysis

Defense Innovation Unit

Developmental Test, Eval & Assessment

Test Resource Management Center

Exec Dir, Systems Engineering and Architecture

Office of the Deputy CTO for Science & Technology

- DTIC
- JRD
- JHTO
- SBIR/STTR
- S&T Foundations
  - DoD Labs, FFRDCs & UARCs
  - Basic Research
    - HBCU/MI
    - STEM
- S&T Futures
  - Tech Industrial Innovation Base
  - Sustainment Technology
  - Emerging Technologies
    - Advanced Materials
    - Biotechnology
    - FutureG
    - Quantum Science
- S&T Program Protection
  - Maintaining Tech Advantage
  - System Security

Office of the Deputy CTO for Critical Technologies

- 5G Transition Office
- Applied Technology
  - Directed Energy
  - Hypersonics
  - Integrated Sensing & Cyber
- Enabling Technology
  - Trusted AI & Autonomy
  - Integrated Network System-of-Systems
  - Microelectronics
  - Space Technology
  - Renewable Energy Generation & Storage
  - Advanced Computing and Software
  - Human-Machine Interfaces

Office of the Deputy CTO for Mission Capabilities

- Special Projects
- Multi-Domain Joint Operations
- Prototypes & Experiments
- Mission Integration

DTIC = Defense Technical Information Center
HBCU/MI = Historically Black Colleges and Universities and Minority Serving Institutions
JRD = Joint Reserve Directorate
JHTO = Joint Hypersonics Transition Office
SBIR/STTR = Small Business Innovation Research and Small Business Technology Transfer Programs
STEM = Science, Technology, Engineering and Mathematics

STPP Mission: Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through <u>assured, secure and resilient</u> systems and a healthy viable national security innovation base

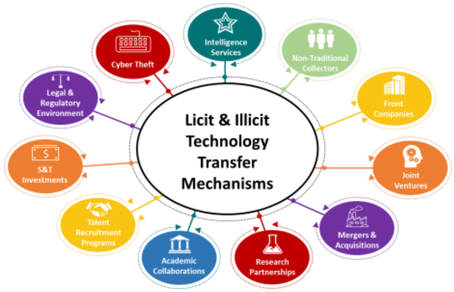
Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

System Security Mission - FY2024

Building Enduring Advantage

U.S. competitors increasingly hold at risk our defense ecosystem - the Department, the defense industrial base, and the landscape of private and academic enterprises that innovate and support the systems on which the Joint Force depends – NDS 2022

- **Adapt policy, guidance and standards to balance Technology and Program Protection that enables accelerated delivery of warfighter capability**
- **Cultivate the System Security, Secure Cyber Resilient Engineering we need**
- **Strengthen Technology and Program Protection methods to ensure technological superiority**
- **Accelerate integration of data, software assurance, and microelectronics trust and assurance efforts through Joint Federated Assurance Center**


Licit & Illicit Technology Transfer Mechanisms

Lead Policy :

DoDI 5000.83, DoDI 5200.44, DoDI 5200.NP, DoDD 5200.47E

Guidance:

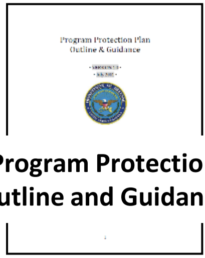
- Program Protection Planning
- Information Communications Technology Supply Chain
- Secure Software Supply Chain
- Controlled Technical Information
- Anti Tamper
- Hardware Assurance
- Microelectronics Assurance Framework
- Software Assurance

Competency:

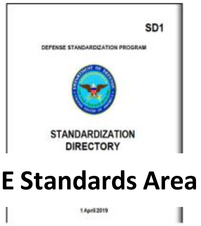
- System Security Engineering
- Secure Cyber Resilient Engineering

Engagements:

- CRWS Workshops
- NDIA SSE Committee

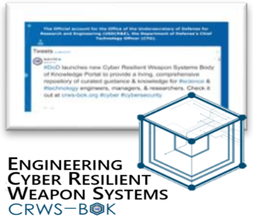


Program Protection Outline and Guidance



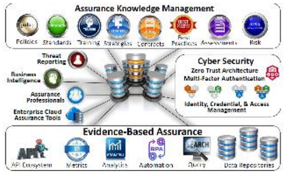
SCRE Standards Area

Standards, Specifications, Handbook, Data Item Descriptions and associated Guidance


The Official account for the Office of the Undersecretary of Defense for Research and Engineering (USD(R&E)), the Department of Defense's Chief Technology Officer (CTO).

Tweets

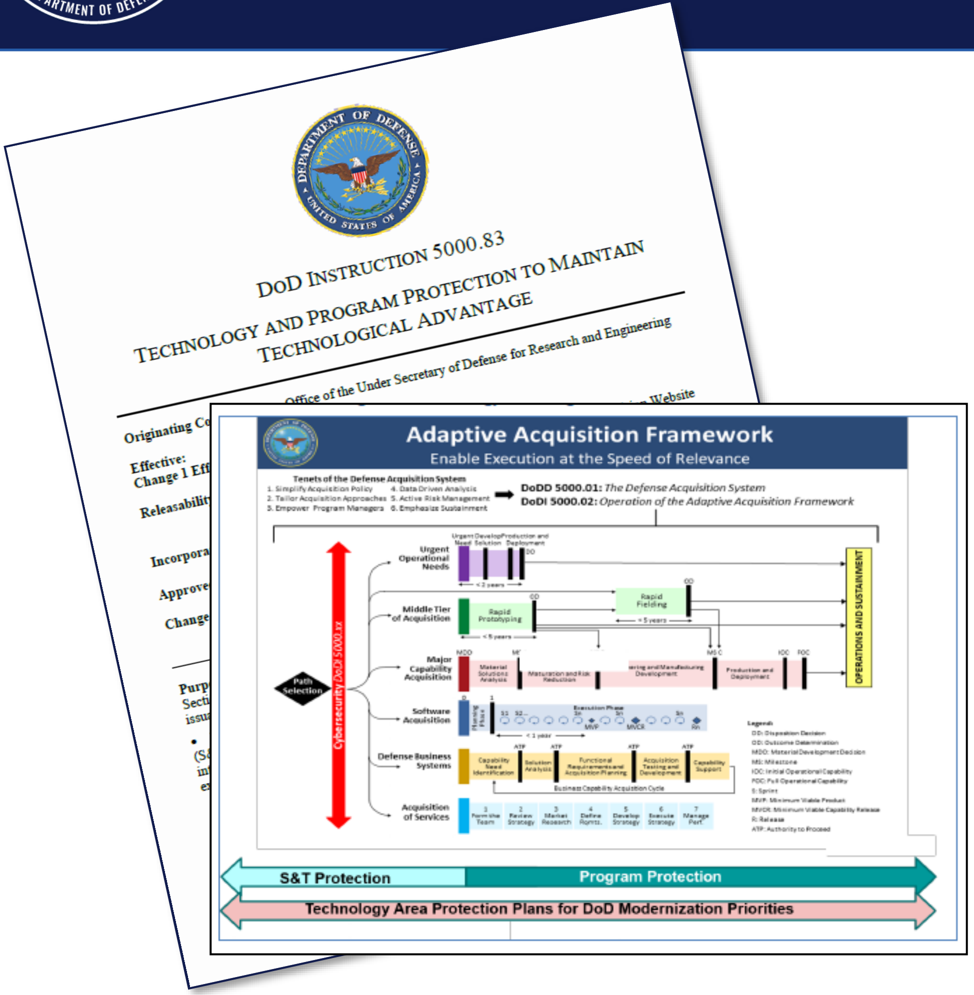
#DoD launches new Cyber Resilient Weapon Systems Body of Knowledge Portal to provide a living, comprehensive repository of curated guidance & knowledge for #science & #technology engineers, managers, & researchers. Check it out at crws-bok.org #cyber #cybersecurity



Joint Federated Assurance Center (JFAC)

Provide the Department the Tools Needed to Build Cost Effective Enduring Advantage Through Resilient Assured, Secure, Innovation, Missions, Systems and Components

DoD Instruction (DoDI) 5000.83: Technology and Program Protection to Maintain Technological Advantage, Jul 2020



DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Office of the Under Secretary of Defense for Research and Engineering

Originating Co

Effective:
Change 1 Eff

Releasabilit

Website

Incorpora

Approve

Change

Purp
Secti
issu

(S
in
ex

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*

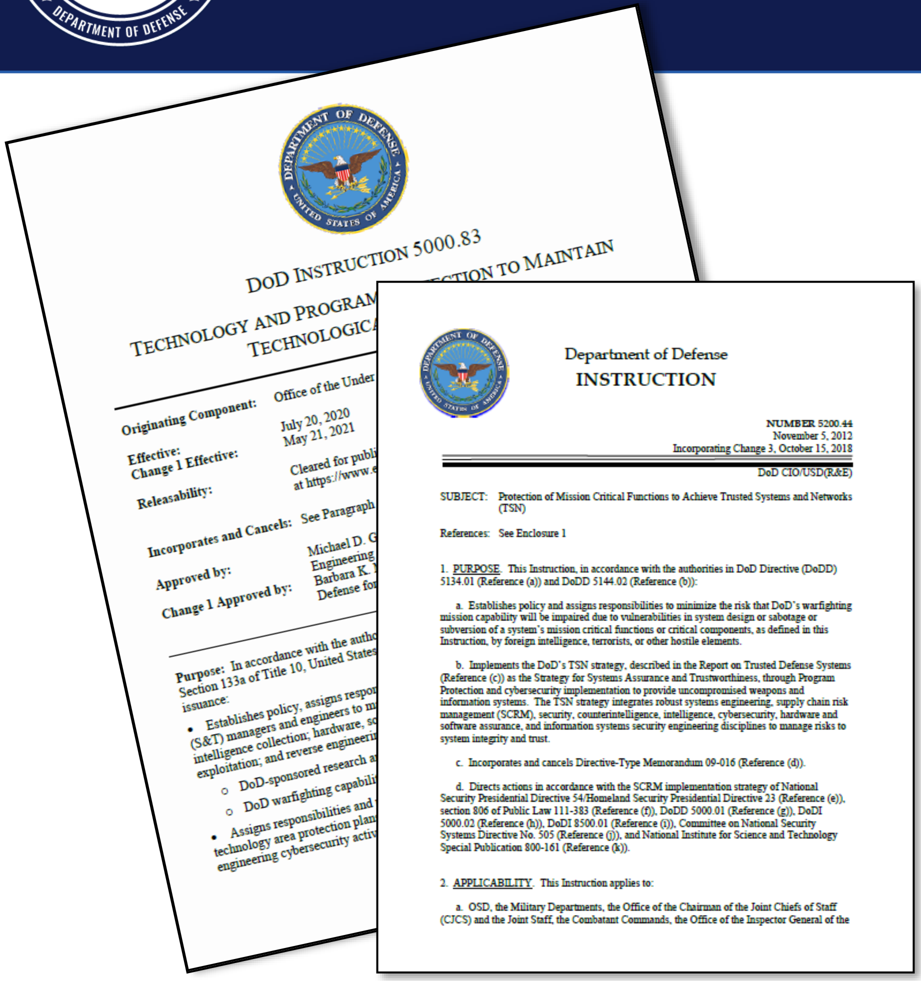
Legend:
DD: Disposition Decision
OD: Outcome Determination
MDD: Material Development Decision
MS: Milestone
IOC: Initial Operational Capability
FOC: Full Operational Capability
S: Sprint
MVP: Minimum Viable Product
MVCR: Minimum Viable Capability Release
R: Release
ATP: Authority to Proceed

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
OD
< 5 years
Rapid Fielding
OD
< 5 years
Major Capability Acquisition
MDD
MS
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
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 systems security and cybersecurity technical risks to:**
  - DoD-sponsored research and technology
  - DoD warfighting capabilities
- **Systems security and cybersecurity technical risks include:**
  - Hardware, software, supply chain exploitation
  - Cyber, and cyberspace vulnerabilities
  - Reverse engineering, anti-tamper
  - Controlled Technical Information / data exfiltration
- **Employs SSE and SCRE methods**
- **Introduces S&T protection and Technology Area Protection Plans (TAPPs)**
- **Points to Engineering and Test and Evaluation issuance**
- **Aligns Program Protection Planning and SCRE with acquisition pathways**

Establishes responsibilities for technology and program protection in support of the Adaptive Acquisition Framework; includes considerations to design for security and cyber resiliency

DoDI 5200.44: Trusted Systems and Networks



DoD Instruction 5000.83

Technology and Program ~~~~ection to Maintain

Technologica

Originating Component: Office of the Under

Effective: July 20, 2020

Change 1 Effective: May 21, 2021

Releasability: Cleared for publi
at https://www.e

Incorporates and Cancels: See Paragraph

Approved by: Michael D. G
Engineering

Change 1 Approved by: Barbara K.
Defense for

Purpose: In accordance with the autho
Section 133a of Title 10, United States
issuance:

- Establishes policy, assigns respo
(S&T) managers and engineers to m
intelligence collection; hardware, so
exploitation; and reverse engineeri
  - DoD-sponsored research a
  - DoD warfighting capabili
- Assigns responsibilities and
technology area protection plan
engineering cybersecurity activ

Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012
Incorporating Change 3, October 15, 2018

DoD CIO/USD(R&E)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.02 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and cybersecurity implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoDD 5000.01 (Reference (g)), DoDI 5000.02 (Reference (h)), DoDI 8500.01 (Reference (i)), Committee on National Security Systems Directive No. 505 (Reference (j)), and National Institute for Science and Technology Special Publication 800-161 (Reference (k)).

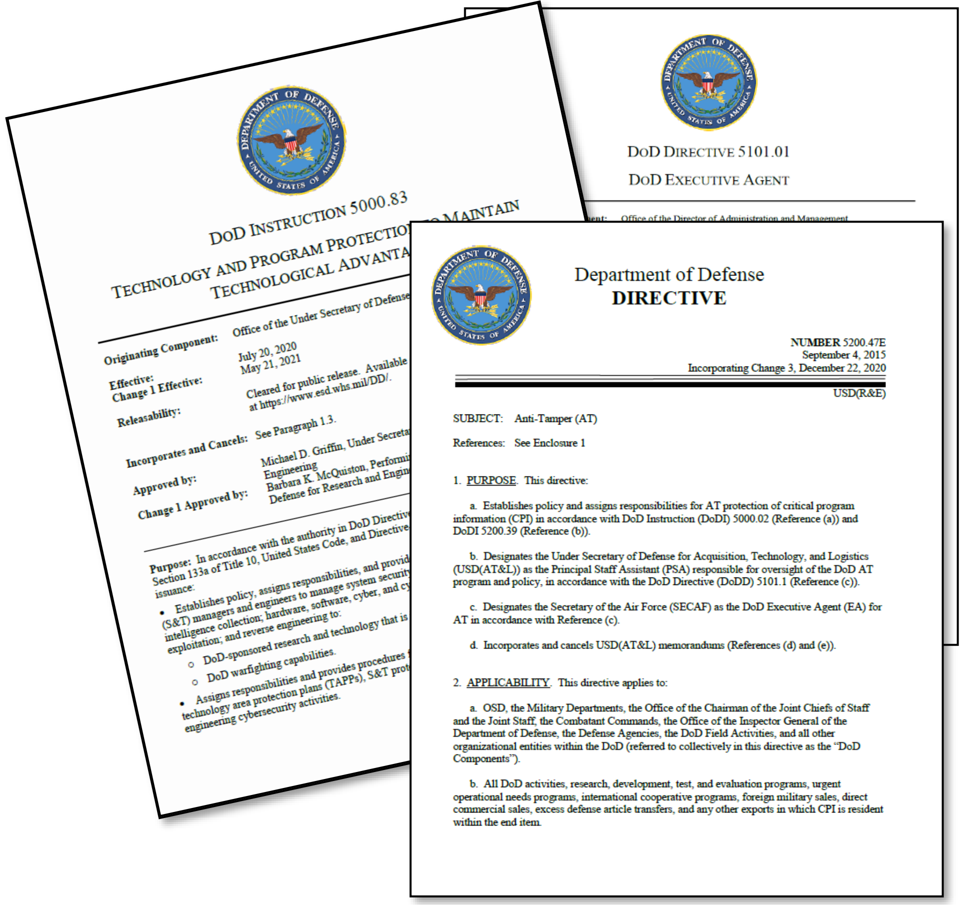
2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the

- **Implements the DoD's Trusted Systems and Networks (TSN) strategy**
- **Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing**
  - Criticality Analysis as the systems engineering process for risk identification
  - Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management
  - Trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)
- **Document Program's implementation and outcomes in Program Protection Plan and relevant cybersecurity plans, as appropriate**

Draft update incorporates procedures to implement information communication technology (ICT) exclusion authorities and use of Trusted Suppliers when available

DoDD 5200.47E: Anti-Tamper



DoD Instruction 5000.83

Technology and Program Protectio… Maintain Technological Advanta…

Originating Component: Office of the Under Secretary of Defense…

Effective: July 20, 2020

Change 1 Effective: May 21, 2021

Releasability: Cleared for public release. Available at https://www.esd.whs.mil/DD/.

Incorporates and Cancels: See Paragraph 1.3.

Approved by: Michael D. Griffin, Under Secreta… Engineering

Change 1 Approved by: Barbara K. McQuiston, Performi… Defense for Research and Engin…

Purpose: In accordance with the authority in DoD Directive… Section 133a of Title 10, United States Code, and Directive… issuance:

- Establishes policy, assigns responsibilities, and provid… (S&T) managers and engineers to manage system security… intelligence collection; hardware, software, cyber, and cy… exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is…
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures… technology area protection plans (TAPPs), S&T prot… engineering cybersecurity activities.

DoD Directive 5101.01

DoD Executive Agent

…ent: Office of the Director of Administration and Management

Department of Defense
DIRECTIVE

NUMBER 5200.47E
September 4, 2015
Incorporating Change 3, December 22, 2020

USD(R&E)

SUBJECT: Anti-Tamper (AT)

References: See Enclosure 1

1. PURPOSE. This directive:

a. Establishes policy and assigns responsibilities for AT protection of critical program information (CPI) in accordance with DoD Instruction (DoDI) 5000.02 (Reference (a)) and DoDI 5200.39 (Reference (b)).

b. Designates the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) as the Principal Staff Assistant (PSA) responsible for oversight of the DoD AT program and policy, in accordance with the DoD Directive (DoDD) 5101.1 (Reference (c)).

c. Designates the Secretary of the Air Force (SECAF) as the DoD Executive Agent (EA) for AT in accordance with Reference (c).

d. Incorporates and cancels USD(AT&L) memorandums (References (d) and (e)).

2. APPLICABILITY. This directive applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this directive as the "DoD Components").

b. All DoD activities, research, development, test, and evaluation programs, urgent operational needs programs, international cooperative programs, foreign military sales, direct commercial sales, excess defense article transfers, and any other exports in which CPI is resident within the end item.

Update required to reassign USD(AT&L) responsibilities to USD(R&E) and USD(A&S)

- **Establishes and Charters the DoD Executive Agent, per DoDD 5101.01**
  - Establishes policy and assigns responsibilities for AT protection of critical program information (CPI) in accordance with DoDI 5000.02 and DoDI 5200.39.
  - Designates the Secretary of the Air Force (SECAF) as the DoD Executive Agent (EA) for AT in accordance with DoDD 5101.1
- **Applicable to:**
  - All DoD activities, research, development, test, and evaluation programs, urgent operational needs programs, international cooperative programs, foreign military sales, direct commercial sales, excess defense article transfers, and any other exports in which CPI is resident within the end item.
- **CPI Identification Working Group:**
  - CPI Capstone and Implementation Plan developed to capture necessary updates to policies, process, tools, guidance, and training to optimize the Department's approach to identification and validation of CPI

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

DoDI 5200.XX: Access to Assured Trusted Microelectronics

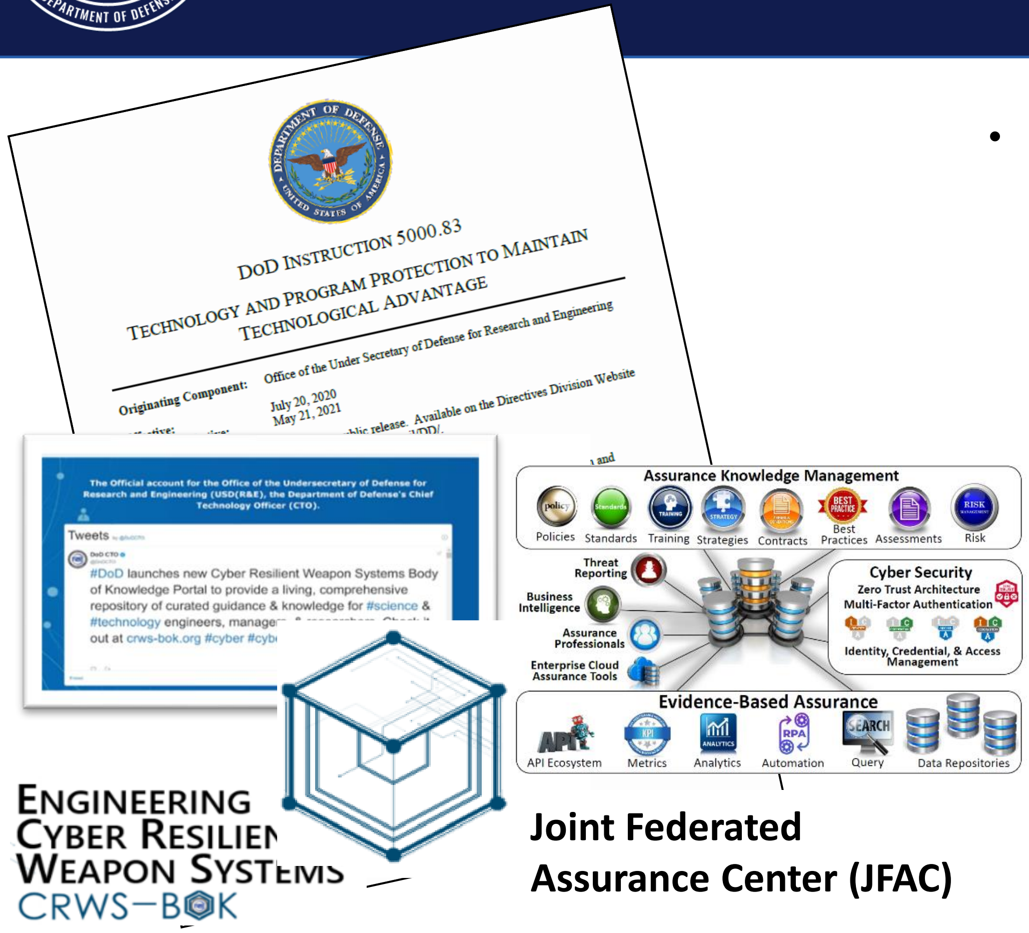
> **"The Department will continue to invest in programs to secure U.S. microelectronics interests; reverse the erosion of domestic innovation and supply; and establish a strong foundation for the next generation of microelectronics technology for DoD applications, while also sustaining current systems."**
>
> Lloyd J. Austin III
>
> *Secretary of Defense*

- **Status: DoDI 5200.XX completed informal coordination**
  - Incorporating feedback prior to initiating DoD Issuance Formal Coordination process
- **Codify FY2017 NDAA Section 231(d) Access to Assured Trusted Microelectronics and FY2021 NDAA Section 276 Section 231(d) as amended by 276(3)**
  - (d) Not later than September 30, 2019, the Secretary of Defense shall issue a directive for the Department of Defense describing how Department of Defense entities may access assured and trusted microelectronics supply chains for Department of Defense systems.
- **Informed by NDAA FY 2023 Report 117-130; Air Force Independent Review of USD (R&E) Microelectronics Quantifiable Assurance Effort**

Scheduled to Complete April 2024

Distribution Statement A: Approved for public release. DOPSR case #24-T-0022 applies. Distribution is unlimited.

Design for Security and Cyber Resiliency



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

July 20, 2020
May 21, 2021

…blic release. Available on the Directives Division Website …/DD/.

The Official account for the Office of the Undersecretary of Defense for Research and Engineering (USD(R&E), the Department of Defense's Chief Technology Officer (CTO).

Tweets

DoD CTO

#DoD launches new Cyber Resilient Weapon Systems Body of Knowledge Portal to provide a living, comprehensive repository of curated guidance & knowledge for #science & #technology engineers, manage… out at crws-bok.org #cyber #cyb…

ENGINEERING CYBER RESILIEN… WEAPON SYSTEMS
CRWS–BOK

Joint Federated Assurance Center (JFAC)

- **Allocate cybersecurity and related system security requirements to the system architecture and design and assess the design for vulnerabilities. The system architecture and design will address, at a minimum, how the system:**

  (a) Manages access to, and use of, the system and system resources.

  (b) Is structured to protect and preserve system functions or resources, such as through segmentation, separation, isolation, or partitioning.

  (c) Maintains priority system functions under adverse conditions.

  (d) Is configured to minimize exposure of vulnerabilities that could impact the mission, including through application of techniques, such as:

  1. Design choice.
  2. Component choice.

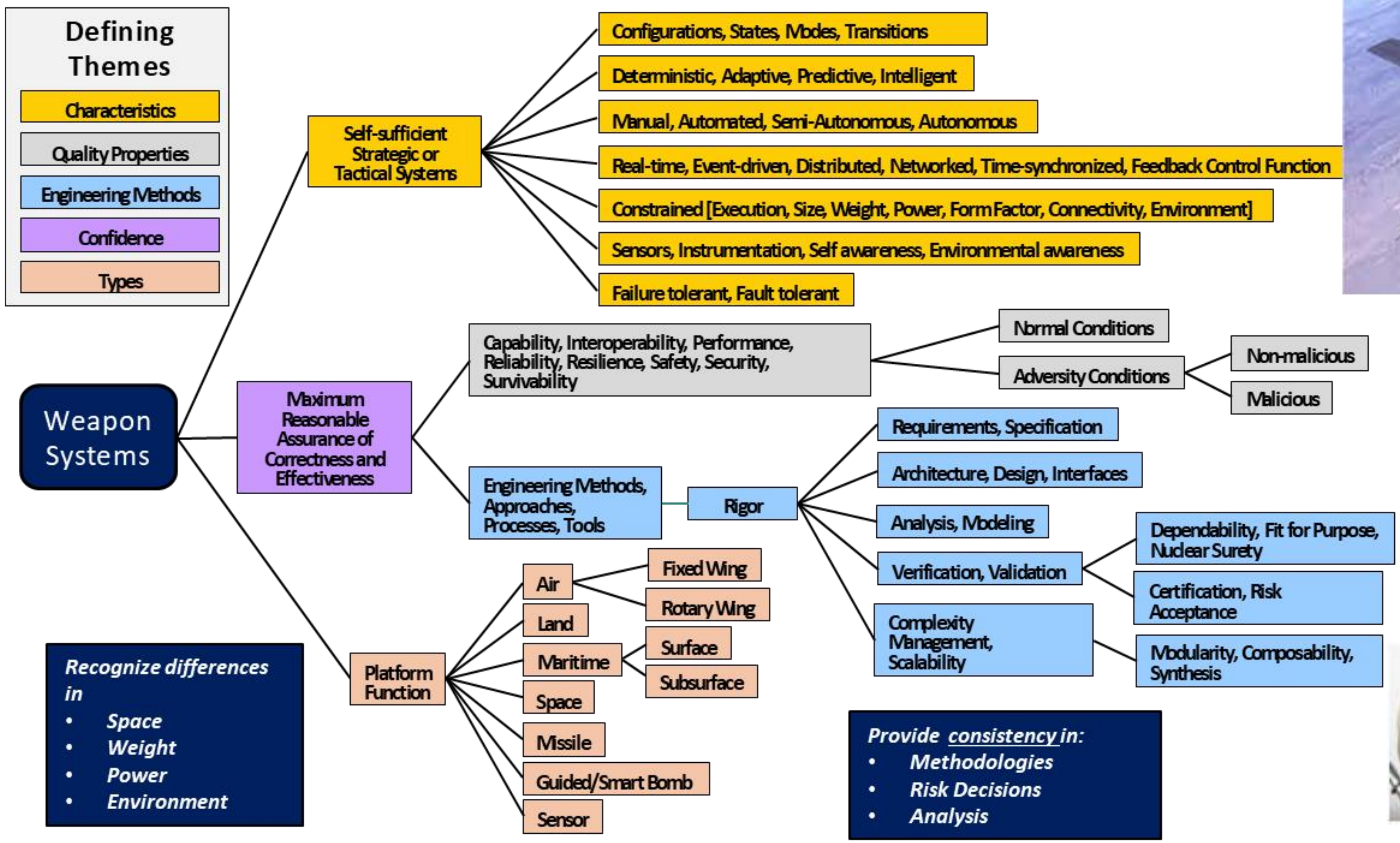
  (e) Monitors, detects, and responds to security anomalies.

  (f) Interfaces with the DoD Information Network or other external services.

Includes Allocation of Requirements for System Architecture and Design

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Design for Security and Cyber Resiliency



Defining Themes
- Characteristics
- Quality Properties
- Engineering Methods
- Confidence
- Types

Weapon Systems
- Self-sufficient Strategic or Tactical Systems
  - Configurations, States, Modes, Transitions
  - Deterministic, Adaptive, Predictive, Intelligent
  - Manual, Automated, Semi-Autonomous, Autonomous
  - Real-time, Event-driven, Distributed, Networked, Time-synchronized, Feedback Control Function
  - Constrained [Execution, Size, Weight, Power, Form Factor, Connectivity, Environment]
  - Sensors, Instrumentation, Self awareness, Environmental awareness
  - Failure tolerant, Fault tolerant
- Maximum Reasonable Assurance of Correctness and Effectiveness
  - Capability, Interoperability, Performance, Reliability, Resilience, Safety, Security, Survivability
    - Normal Conditions
    - Adversity Conditions
      - Non-malicious
      - Malicious
  - Engineering Methods, Approaches, Processes, Tools
    - Rigor
      - Requirements, Specification
      - Architecture, Design, Interfaces
      - Analysis, Modeling
      - Verification, Validation
        - Dependability, Fit for Purpose, Nuclear Surety
        - Certification, Risk Acceptance
      - Complexity Management, Scalability
        - Modularity, Composability, Synthesis
- Platform Function
  - Air
    - Fixed Wing
    - Rotary Wing
  - Land
  - Maritime
    - Surface
    - Subsurface
  - Space
  - Missile
  - Guided/Smart Bomb
  - Sensor

Recognize differences in
- *Space*
- *Weight*
- *Power*
- *Environment*

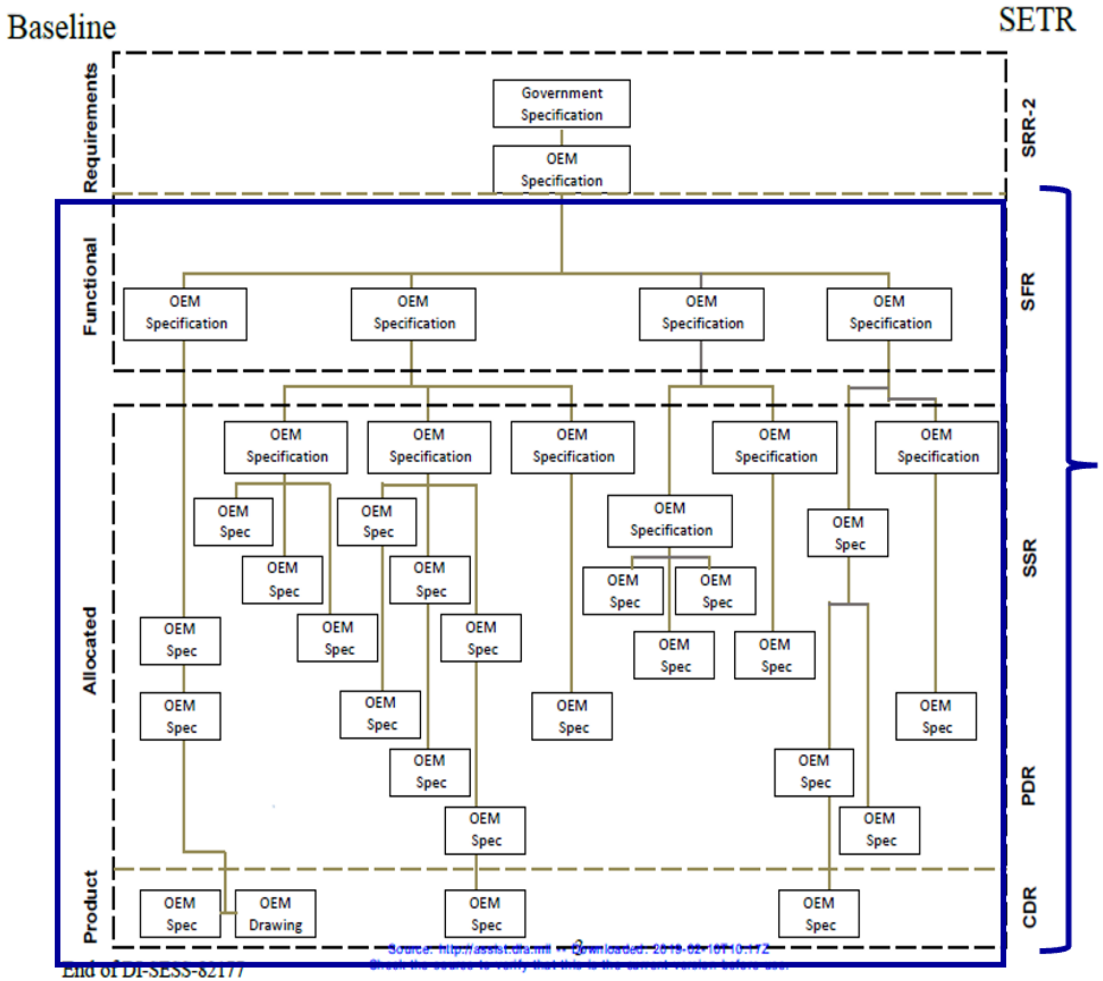
Provide consistency in:
- *Methodologies*
- *Risk Decisions*
- *Analysis*

Includes Allocation of Requirements in System Architecture and Design

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Consider Physics Based Constraints

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



Source: http://assist.dla.mil -- Downloaded: 2019-02-10T10:17Z
Check the source to verify that this is the current version before use.

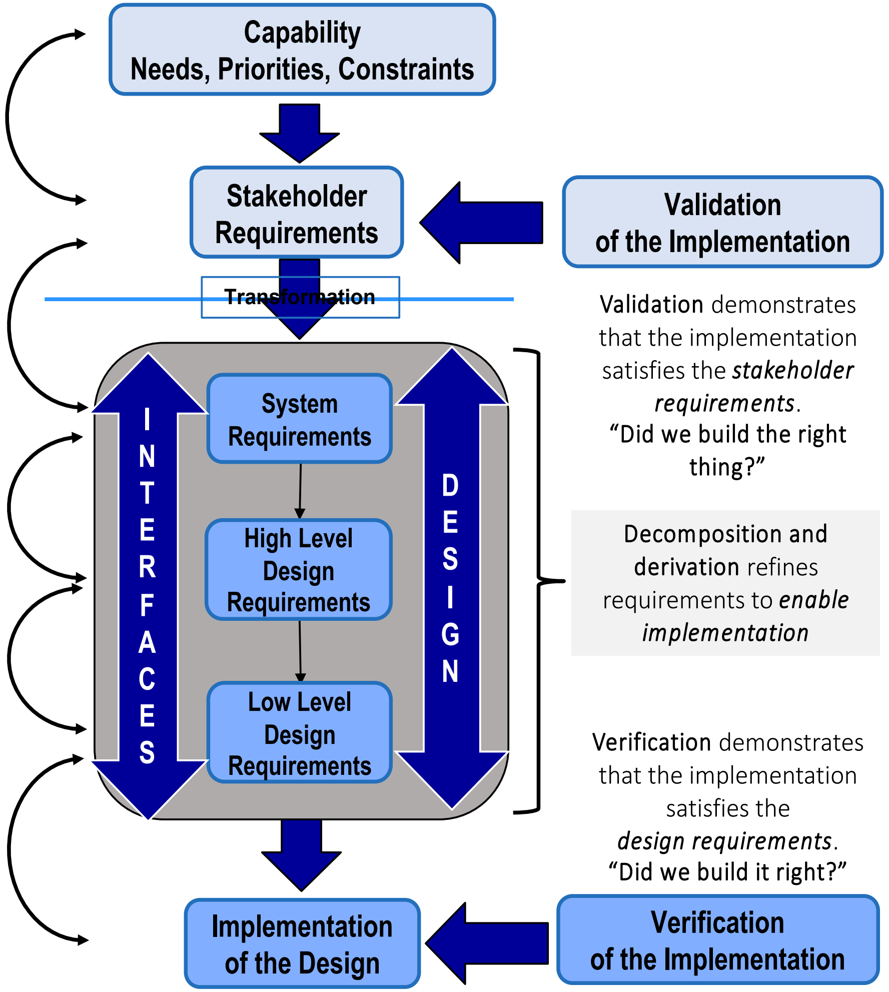
End of DI-SESS-82177

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

Consider Technical Implementation of Cybersecurity Requirements

Engineering Requirements



Capability
Needs, Priorities, Constraints

Stakeholder Requirements

Validation of the Implementation

Transformation

System Requirements

High Level Design Requirements

Low Level Design Requirements

INTERFACES

DESIGN

Validation demonstrates that the implementation satisfies the *stakeholder requirements*.
"Did we build the right thing?"

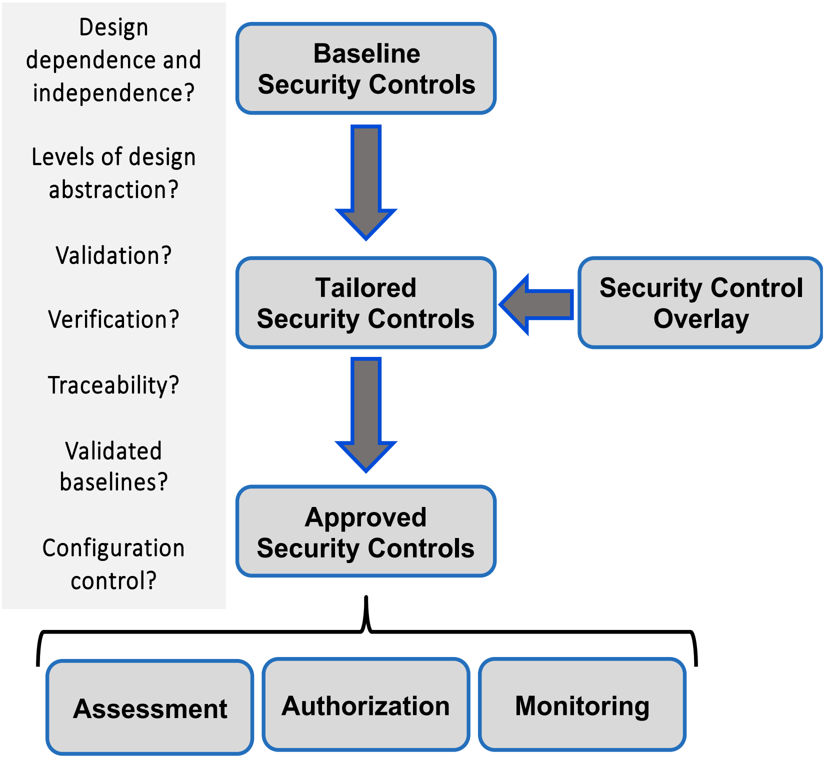
Decomposition and derivation refines requirements to *enable implementation*

Verification demonstrates that the implementation satisfies the *design requirements*.
"Did we build it right?"

Implementation of the Design

Verification of the Implementation

Security Controls



Design dependence and independence?

Levels of design abstraction?

Validation?

Verification?

Traceability?

Validated baselines?

Configuration control?

Baseline Security Controls

Tailored Security Controls

Security Control Overlay

Approved Security Controls

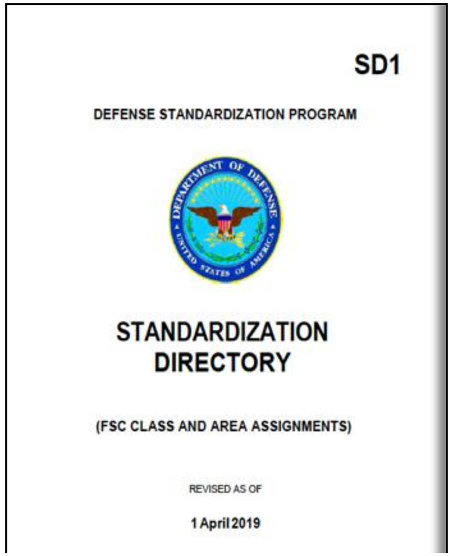
Assessment

Authorization

Monitoring

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Engineering Design Standards



SD1

DEFENSE STANDARDIZATION PROGRAM

STANDARDIZATION DIRECTORY

(FSC CLASS AND AREA ASSIGNMENTS)

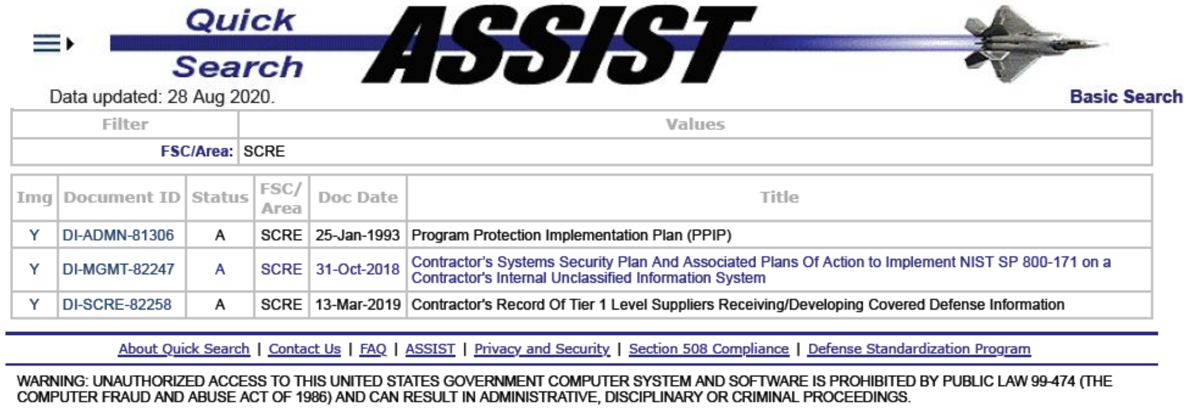
REVISED AS OF

1 April 2019

Standards, Specifications, Handbook, Data Item Descriptions and associated Guidance

Driving Transformation: Consistent, Repeatable Implementation

- **Secure Cyber Resilient Engineering (SCRE) Standardization Area**
  - 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.



Quick Search ASSIST

Data updated: 28 Aug 2020.

Basic Search

Filter	Values
FSC/Area:	SCRE

Img	Document ID	Status	FSC/ Area	Doc Date	Title
Y	DI-ADMN-81306	A	SCRE	25-Jan-1993	Program Protection Implementation Plan (PPIP)
Y	DI-MGMT-82247	A	SCRE	31-Oct-2018	Contractor's Systems Security Plan And Associated Plans Of Action to Implement NIST SP 800-171 on a Contractor's Internal Unclassified Information System
Y	DI-SCRE-82258	A	SCRE	13-Mar-2019	Contractor's Record Of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information

About Quick Search | Contact Us | FAQ | ASSIST | Privacy and Security | Section 508 Compliance | Defense Standardization Program

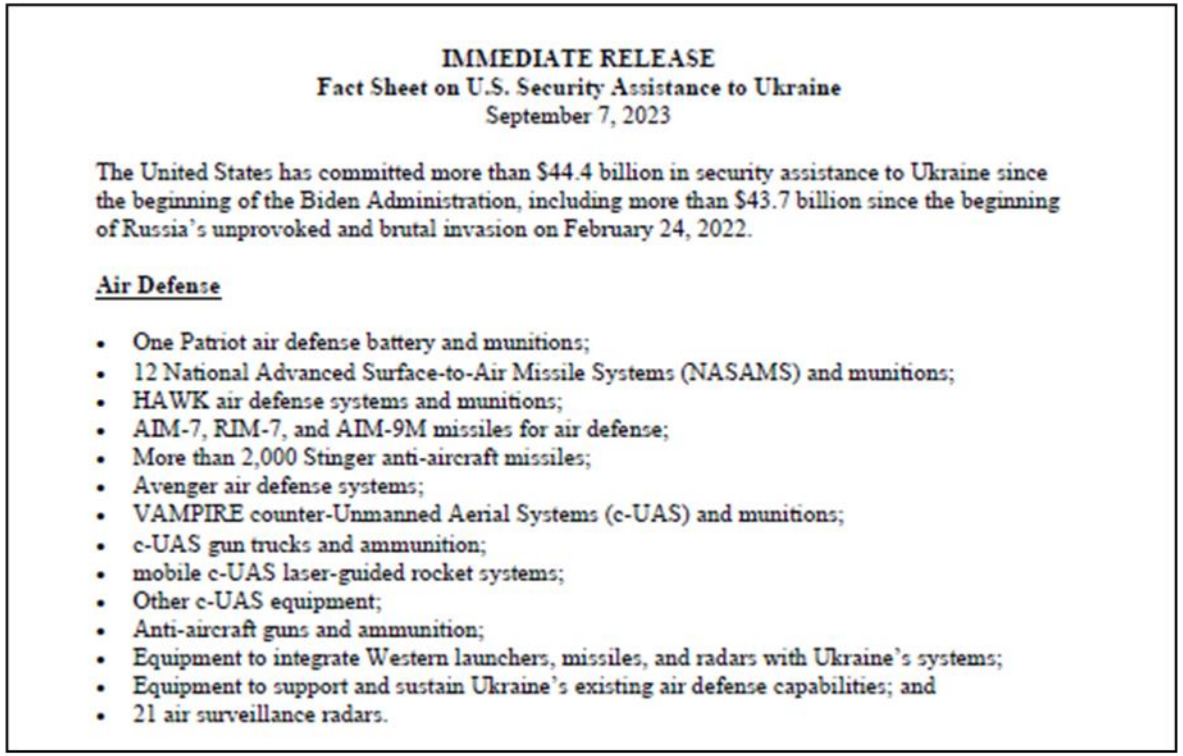
WARNING: UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474 (THE COMPUTER FRAUD AND ABUSE ACT OF 1986) AND CAN RESULT IN ADMINISTRATIVE, DISCIPLINARY OR CRIMINAL PROCEEDINGS.

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Design Standard Considerations

Trilateral Australia-UK-US Partnership on Nuclear-Powered Submarines

On March 13, 2023, AUKUS partners announced an optimal pathway to produce a nuclear-powered submarine capability in Australia at the earliest point while ensuring all three partners maintain the highest non-proliferation standards.



IMMEDIATE RELEASE
Fact Sheet on U.S. Security Assistance to Ukraine
September 7, 2023

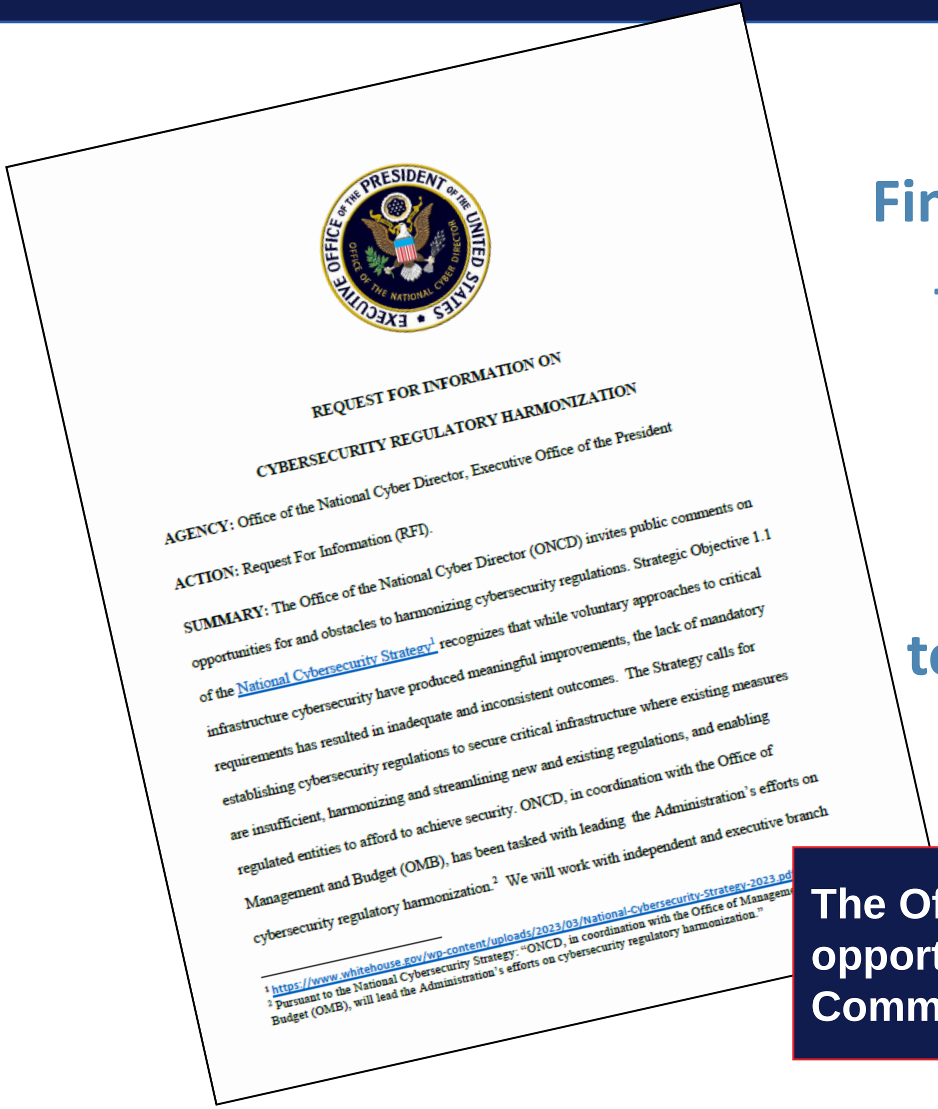
The United States has committed more than $44.4 billion in security assistance to Ukraine since the beginning of the Biden Administration, including more than $43.7 billion since the beginning of Russia's unprovoked and brutal invasion on February 24, 2022.

Air Defense

- One Patriot air defense battery and munitions;
- 12 National Advanced Surface-to-Air Missile Systems (NASAMS) and munitions;
- HAWK air defense systems and munitions;
- AIM-7, RIM-7, and AIM-9M missiles for air defense;
- More than 2,000 Stinger anti-aircraft missiles;
- Avenger air defense systems;
- VAMPIRE counter-Unmanned Aerial Systems (c-UAS) and munitions;
- c-UAS gun trucks and ammunition;
- mobile c-UAS laser-guided rocket systems;
- Other c-UAS equipment;
- Anti-aircraft guns and ammunition;
- Equipment to integrate Western launchers, missiles, and radars with Ukraine's systems;
- Equipment to support and sustain Ukraine's existing air defense capabilities; and
- 21 air surveillance radars.

National Defense Strategy: Anchoring our strategy in Allies and Partners

Contract Considerations



REQUEST FOR INFORMATION ON

CYBERSECURITY REGULATORY HARMONIZATION

AGENCY: Office of the National Cyber Director, Executive Office of the President

ACTION: Request For Information (RFI).

SUMMARY: The Office of the National Cyber Director (ONCD) invites public comments on opportunities for and obstacles to harmonizing cybersecurity regulations. Strategic Objective 1.1 of the National Cybersecurity Strategy[1] recognizes that while voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes. The Strategy calls for establishing cybersecurity regulations to secure critical infrastructure where existing measures are insufficient, harmonizing and streamlining new and existing regulations, and enabling regulated entities to afford to achieve security. ONCD, in coordination with the Office of Management and Budget (OMB), has been tasked with leading the Administration's efforts on cybersecurity regulatory harmonization.[2] We will work with independent and executive branch

[1] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pd

[2] Pursuant to the National Cybersecurity Strategy: "ONCD, in coordination with the Office of Manageme Budget (OMB), will lead the Administration's efforts on cybersecurity regulatory harmonization."

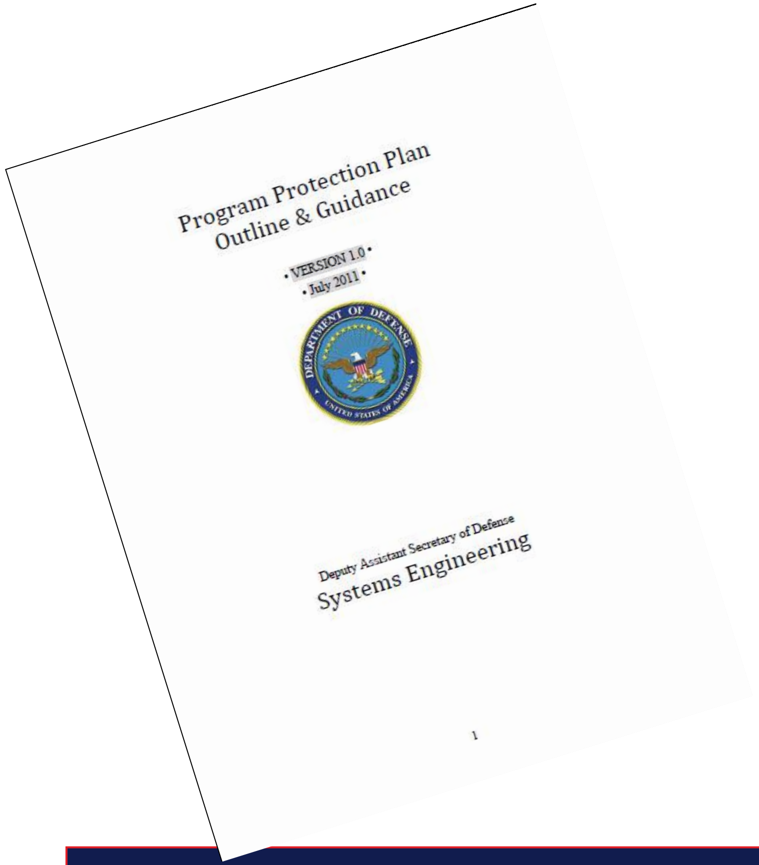
Find an effective balance between supply chain health – represented by the scope and capability of the DIB – and the implementation of the necessary cybersecurity and related supply chain regulatory requirements

to protect the asymmetric advantages generated by the DIB's innovation and technologic capabilities

The Office of the National Cyber Director (ONCD) invites public comments on opportunities for and obstacles to harmonizing cybersecurity regulations Comments must be received in writing by 5 p.m. EDT October 31, 2023.

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Managing Program Protection Risks



Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

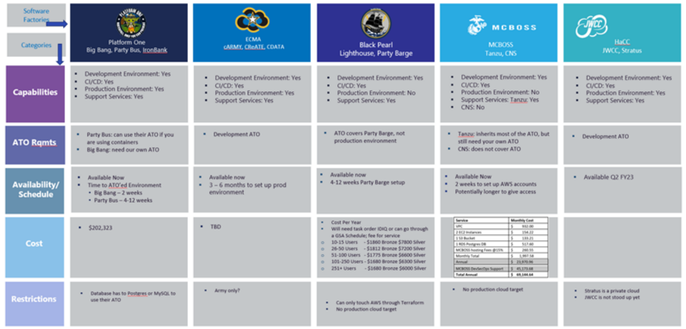
1

- **Program Protection Plan update in process, includes:**
  - Updates signatory from USD(AT&L) to USD(R&E) for ACAT 1D programs
    - Delegates responsibility to DoD Component heads for all other acquisition
  - Allows for tailoring to the Adaptive Acquisition Framework
  - Proposed Software Assurance Tables include development frameworks, services, and reuse practices
  - Clarifies Government and industry responsibilities

Informed by 4 Tabletop Exercises conducted with Army, Navy, Air Force and Missile Defense Agency

Joint Federated Assurance Center

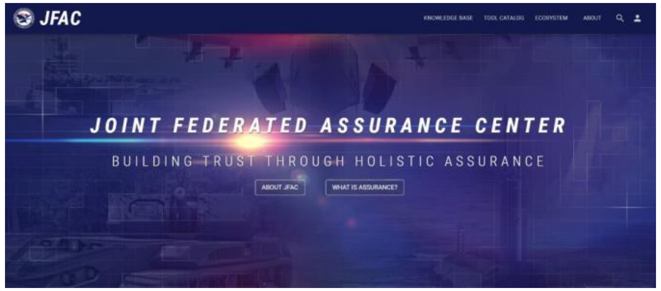
Joint Federated Assurance Center – Coordination Support Center (JFAC-CSC)



Software Factories → Categories ↓	Platform One Big Bang, Party Bus, IronBank	ECMA cARMY, CReATE, CDATA	Black Pearl Lighthouse, Party Barge	MCBOSS Tanzu, CNS	HaCC JWCC, Stratus
Capabilities	• Development Environment: Yes • CI/CD: Yes • Production Environment: Yes • Support Services: Yes	• Development Environment: Yes • CI/CD: Yes • Production Environment: Yes • Support Services: Yes	• Development Environment: Yes • CI/CD: Yes • Production Environment: No • Support Services: Yes	• Development Environment: Yes • CI/CD: Yes • Production Environment: No • Support Services: Tanzu: Yes • CNS: No	• Development Environment: Yes • CI/CD: Yes • Production Environment: Yes • Support Services: Yes
ATO Rqmts	• Party Bus: can use their ATO if you are using containers • Big Bang: need our own ATO	• Development ATO	• ATO covers Party Barge, not production environment	• Tanzu: inherits most of the ATO, but still need your own ATO • CNS: does not cover ATO	• Development ATO
Availability/ Schedule	• Available Now • Time to ATO'ed Environment • Big Bang – 2 weeks • Party Bus – 4-12 weeks	• Available now • 3 – 6 months to set up prod environment	• Available now • 4-12 weeks Party Barge setup	• Available Now • 2 weeks to set up AWS accounts • Potentially longer to give access	• Available Q2 FY23
Cost	• $202,323	• TBD	• Cost Per Year • Will need task order IDIQ or can go through a GSA Schedule; fee for service ○ 10-15 Users - $1860 Bronze $7800 Silver ○ 26-50 Users - $1812 Bronze $7200 Silver ○ 51-100 Users - $1775 Bronze $6600 Silver ○ 101-250 Users - $1680 Bronze $6300 Silver ○ 251+ Users - $1680 Bronze $6000 Silver	see below	
Restrictions	• Database has to Postgres or MySQL to use their ATO	• Army only?	• Can only touch AWS through Terraform • No production cloud target	• No production cloud target	• Stratus is a private cloud • JWCC is not stood up yet

Service	Monthly Cost
VPC	$ 932.00
2 EC2 Instances	$ 154.22
1 S3 Bucket	$ 133.21
1 RDS Postgres DB	$ 517.60
MCBOSS hosting Fees @15%	$ 260.55
Monthly Total	$ 1,997.58
Annual	$ 23,970.96
MCBOSS DevSecOps Support	$ 45,173.68
Total Annual	$ 69,144.64

JFAC Digital Infrastructure: DoD Cloud Broker Analysis of Alternatives


JFAC
KNOWLEDGE BASE
TOOL CATALOG
ECOSYSTEM
ABOUT
JOINT FEDERATED ASSURANCE CENTER
BUILDING TRUST THROUGH HOLISTIC ASSURANCE
ABOUT JFAC
WHAT IS ASSURANCE?

JFAC Portal Modernization

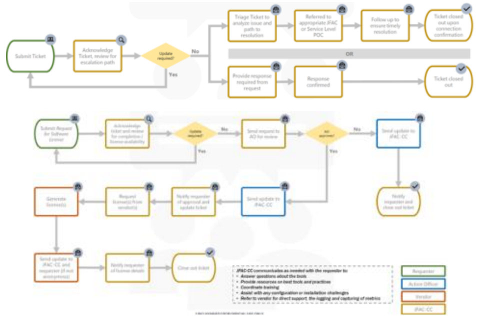
SYNOPSYS BLACKDUCK
Software Composition Analysis

SYNOPSYS Code Dx
Assurance Data Correlation

PARASOFT
Automated API Testing

GRAMMATECH CODESONAR
Static Application Security Testing

Enterprise License Dissemination


Submit Ticket
Acknowledge Ticket, review for escalation path
Update required?
No
Yes
Triage Ticket to analyze issue and path to resolution
Referred to appropriate JFAC or Service Level POC
Follow up to ensure timely resolution
Ticket closed out upon connection confirmation
OR
Provide response required from request
Response confirmed
Ticket closed out
Submit Request for Software License
Acknowledge ticket and review for completion / license availability
Update required?
No
Yes
Send request to AO for review
AO approve?
No
Yes
Send update to JFAC-CC
Notify requester and close out ticket
Send update to JFAC-CC
Notify requester of approval and update ticket
Request license(s) from vendor(s)
Generate license(s)
Send update to JFAC-CC and requester (if not anonymous)
Notify requester of license details
Close out ticket
JFAC-CC communicates as needed with the requester to:
Answer questions about the tools
Provide resources on best tools and practices
Coordinate training
Assist with any configuration or installation challenges
Refer to vendor for direct support, the logging and capturing of metrics
Requester
Action Officer
Vendor
JFAC-CC

JFAC Ticketing Process

Joint Federated Assurance Center - Software Assurance

Modern Cloud-Hosted

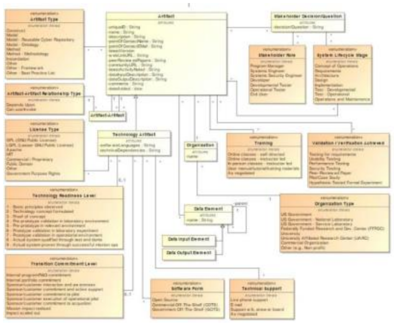
CLOUD ONE FAST SECURE STREAMLINED

NSERC

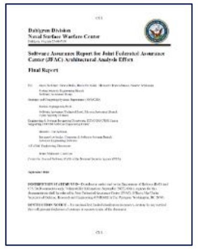
Legacy On-Premise

NAVSEA WARFARE CENTERS DAHLGREN

JFAC Portal Infrastructure



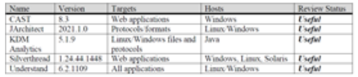
DEVCOM GROUND VEHICLE SYSTEMS CENTER



Dahlgren Division
Naval Surface Warfare Center

Software Assurance Report for Joint Federated Assurance Center (JFAC) Architectural Analysis Effort

Final Report

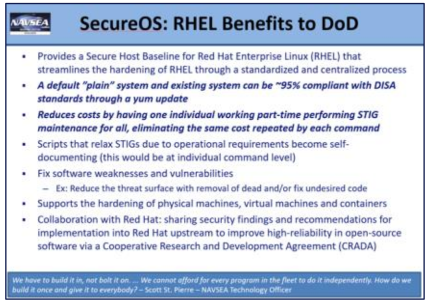


Name	Version	Targets	Hosts	Review Status
CAST	8.3	Web applications	Windows	*Useful*
JArchitect	2021.1.0	Protocols/formats	Linux/Windows	*Useful*
KDM Analytics	5.1.9	Linux/Windows files and protocols	Java	*Useful*
Silverthread	1.24.44.1448	Web applications	Windows, Linux, Solaris	*Useful*
Understand	6.2.1109	All applications	Linux/Windows	*Useful*

NAVSEA WARFARE CENTERS DAHLGREN

Architectural Analysis: 5 Tools Assessed

Red Hat Enterprise Linux



SecureOS: RHEL Benefits to DoD

- Provides a Secure Host Baseline for Red Hat Enterprise Linux (RHEL) that streamlines the hardening of RHEL through a standardized and centralized process
- ***A default "plain" system and existing system can be ~95% compliant with DISA standards through a yum update***
- ***Reduces costs by having one individual working part-time performing STIG maintenance for all, eliminating the same cost repeated by each command***
- Scripts that relax STIGs due to operational requirements become self-documenting (this would be at individual command level)
- Fix software weaknesses and vulnerabilities
  - Ex: Reduce the threat surface with removal of dead and/or fix undesired code
- Supports the hardening of physical machines, virtual machines and containers
- Collaboration with Red Hat: sharing security findings and recommendations for implementation into Red Hat upstream to improve high-reliability in open-source software via a Cooperative Research and Development Agreement (CRADA)

We have to build it in, not bolt it on. ... We cannot afford for every program in the fleet to do it independently. How do we build it once and give it to everybody? – Scott St. Pierre – NAVSEA Technology Officer

NAVSEA WARFARE CENTERS DAHLGREN

Securing Operating System Software

Source Code Scanning and Analysis

Vulnerability Result Fusion

Collaborative

Standardized Reporting

GOTS Developed and Owned

TACTICAL NETWORK PROTECTION Software Assurance Toolset

NAVSEA WARFARE CENTERS DAHLGREN

DEVCOM CSISR CENTER

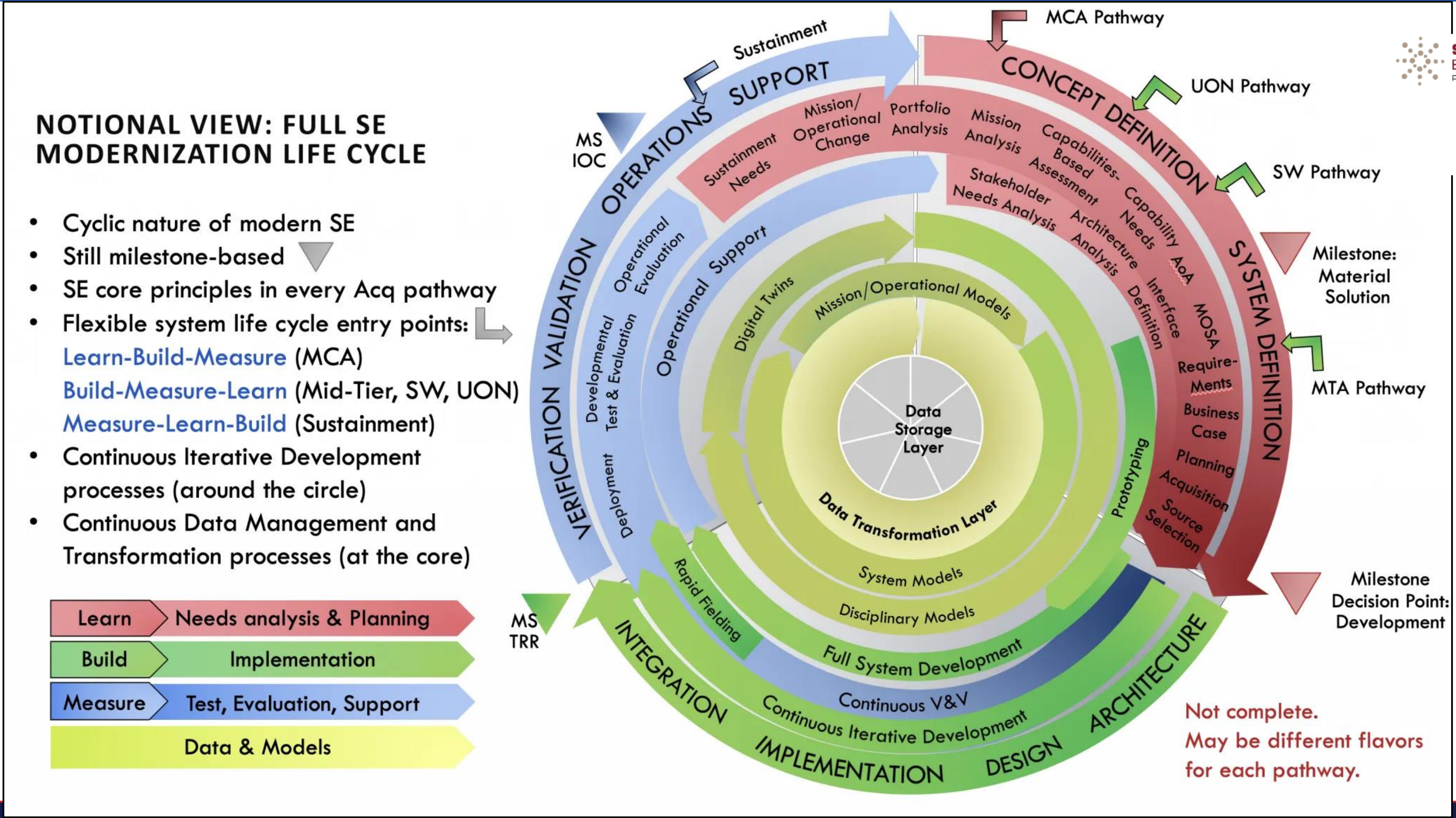
DEVCOM AVIATION & MISSILE CENTER

Joint Software Assurance Tool (J-SwAT)

NDIA S&ME Conference
Oct 16-19, 2023

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Digital Transformation Opportunities



NOTIONAL VIEW: FULL SE MODERNIZATION LIFE CYCLE

- Cyclic nature of modern SE
- Still milestone-based ▽
- SE core principles in every Acq pathway
- Flexible system life cycle entry points:
  Learn-Build-Measure (MCA)
  Build-Measure-Learn (Mid-Tier, SW, UON)
  Measure-Learn-Build (Sustainment)
- Continuous Iterative Development processes (around the circle)
- Continuous Data Management and Transformation processes (at the core)

Learn	Needs analysis & Planning
Build	Implementation
Measure	Test, Evaluation, Support
	Data & Models

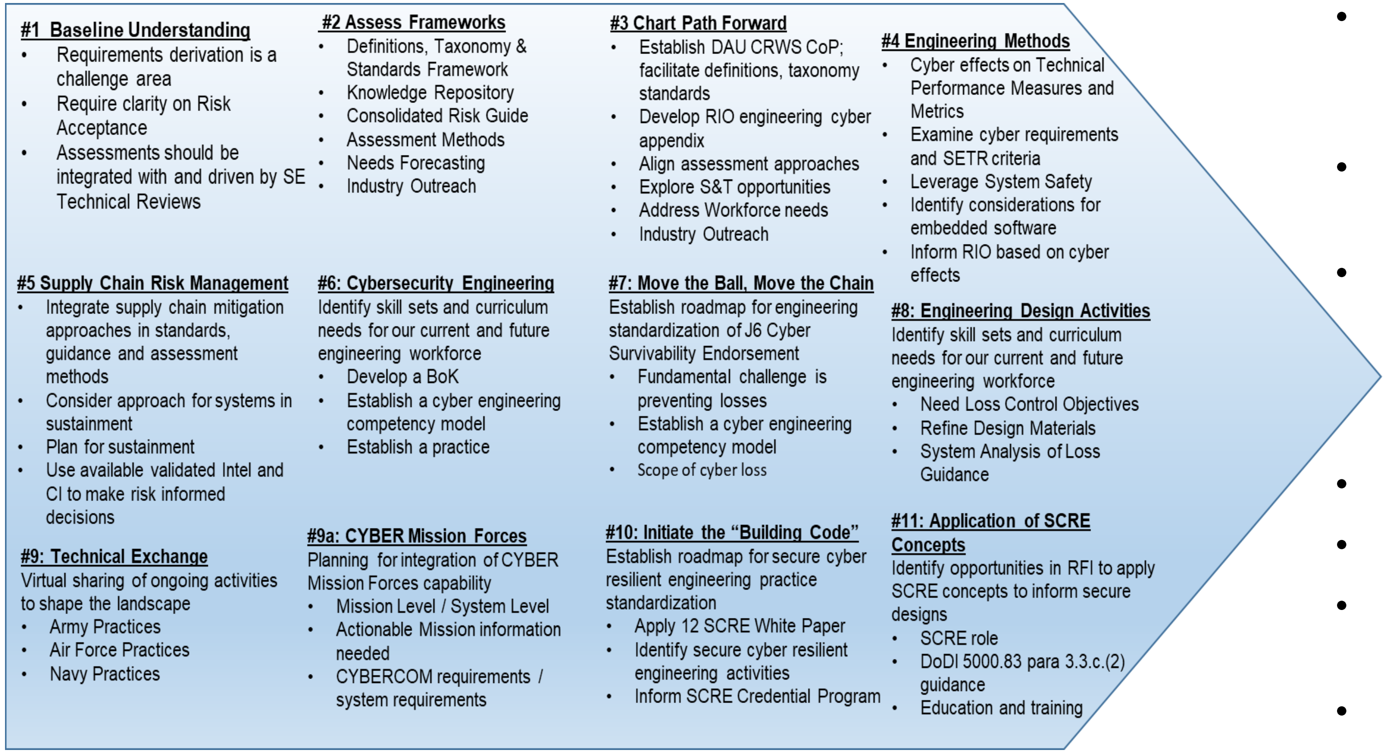
Not complete.
May be different flavors for each pathway.

Modernizing Systems Engineering For Digital Transformation

Leverage System Engineering and Architecture Digital Transformation Initiative

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 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
- **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
- **September 2023**: CRWS #12 Industry Perspectives

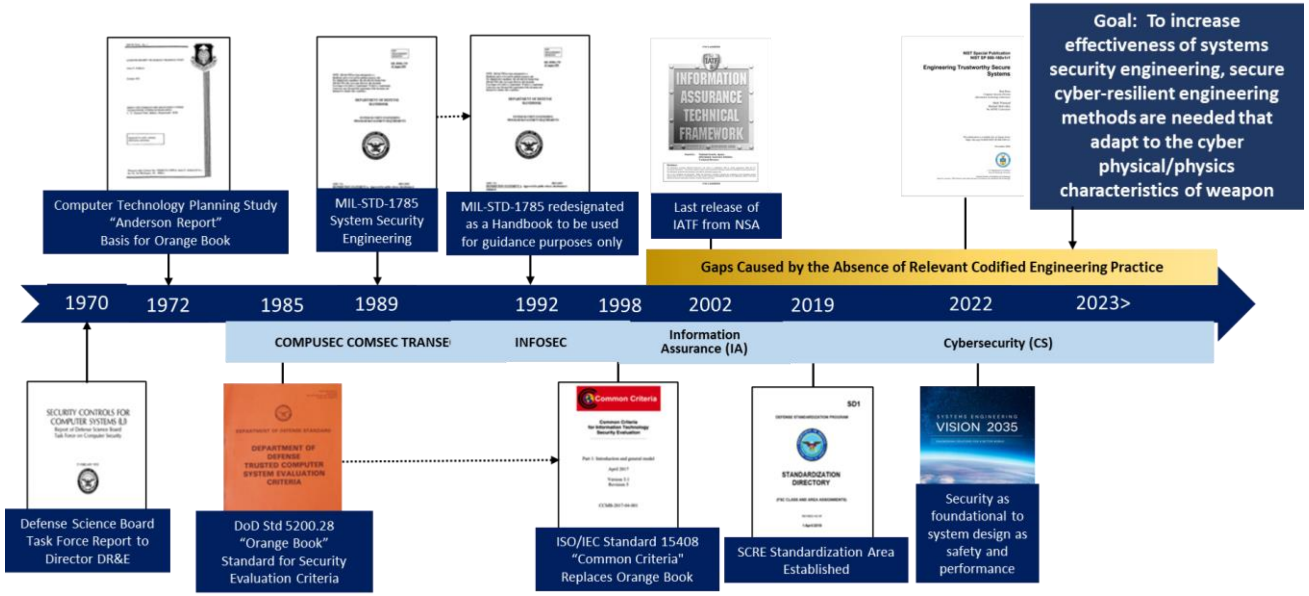
Partnership with Govt, industry, academia stakeholders to address recurring challenges

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Engineering Cyber Resilient Workshops

Provide a forum for DoD, Government, the defense industrial base, and academia to collaboratively address secure cyber resilient engineering:

- *Technical challenges*
- *Workforce competency*



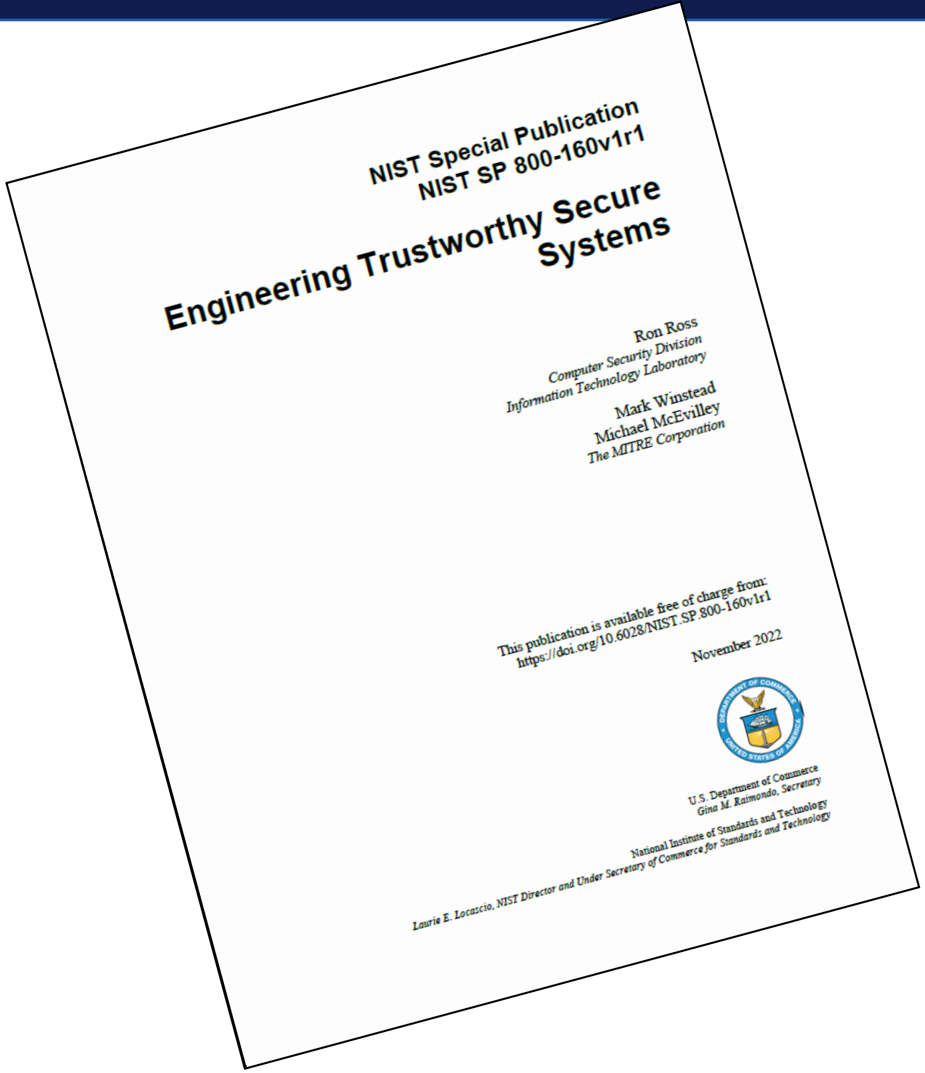
Goal: To increase effectiveness of systems security engineering, secure cyber-resilient engineering methods are needed that adapt to the cyber physical/physics characteristics of weapon

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
INFORMATION ASSURANCE TECHNICAL FRAMEWORK
Last release of IATF from NSA
Engineering Trustworthy Secure Systems
Gaps Caused by the Absence of Relevant Codified Engineering Practice
1970
1972
1985
1989
1992
1998
2002
2019
2022
2023>
COMPUSEC COMSEC TRANSEC
INFOSEC
Information Assurance (IA)
Cybersecurity (CS)
SECURITY CONTROLS FOR COMPUTER SYSTEMS
Defense Science Board Task Force Report to Director DR&E
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
DoD Std 5200.28 "Orange Book" Standard for Security Evaluation Criteria
Common Criteria
ISO/IEC Standard 15408 "Common Criteria" Replaces Orange Book
SD1
STANDARDIZATION DIRECTORY
SCRE Standardization Area Established
SYSTEMS ENGINEERING
VISION 2035
Security as foundational to system design as safety and performance

Secure Cyber Resilient Engineering Vision

- Secure cyber resilient engineered systems that embody a system-centric and effects-oriented perspective to address the ubiquitous nature of security concerns associated with the design, development, fielding and sustainment of military systems.
- The approach seeks to establish and maintain a strategic, principled, and effective engineering capability for delivery of cost-effective secure cyber resilient engineered weapon systems to the warfighter

Engineering Cyber Resilient Workshops



NIST Special Publication
NIST SP 800-160v1r1

Engineering Trustworthy Secure Systems

Ron Ross
Computer Security Division
Information Technology Laboratory

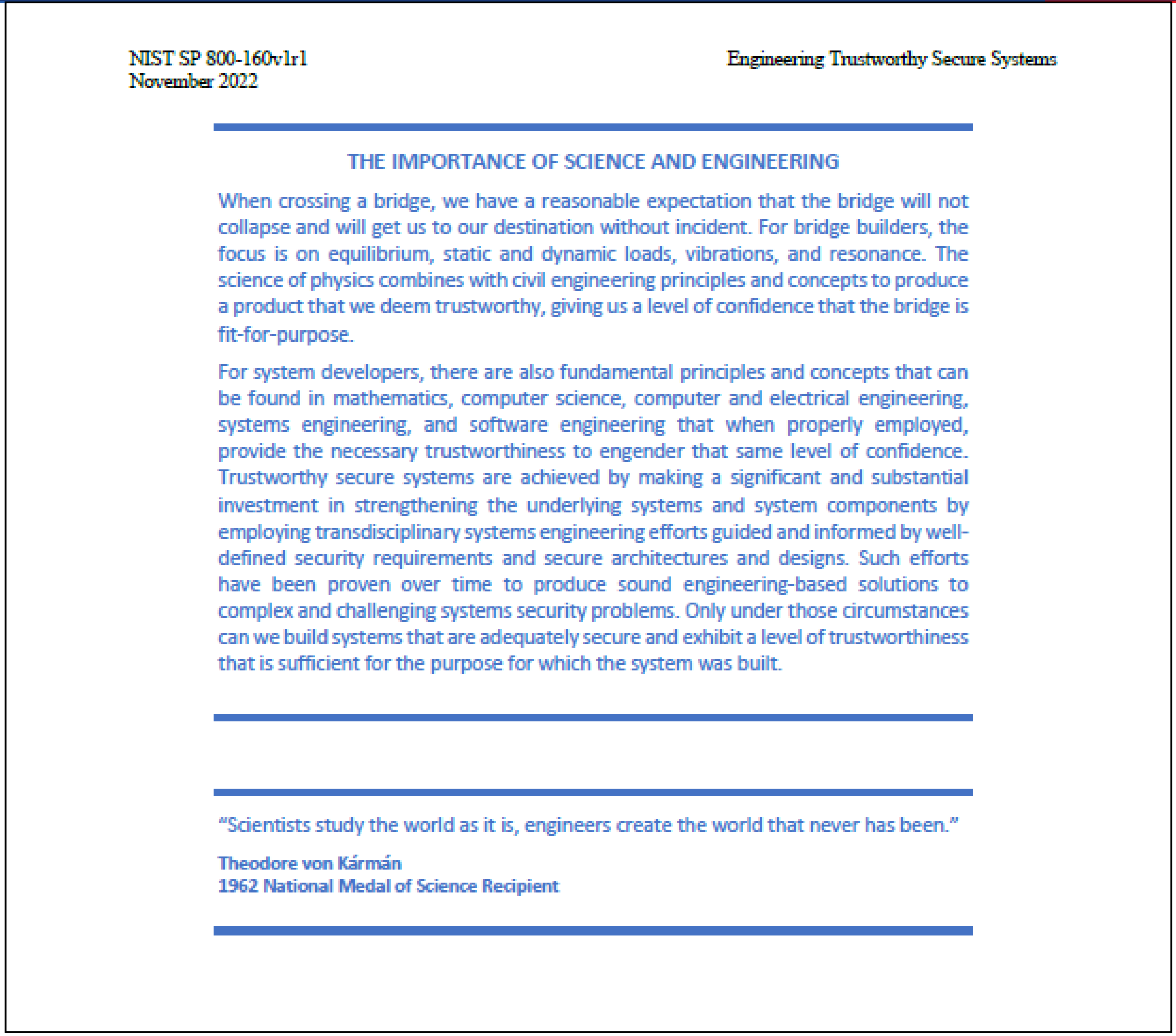
Mark Winstead
Michael McEvilley
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v1r1

November 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology



NIST SP 800-160v1r1
November 2022

Engineering Trustworthy Secure Systems

THE IMPORTANCE OF SCIENCE AND ENGINEERING

When crossing a bridge, we have a reasonable expectation that the bridge will not collapse and will get us to our destination without incident. For bridge builders, the focus is on equilibrium, static and dynamic loads, vibrations, and resonance. The science of physics combines with civil engineering principles and concepts to produce a product that we deem trustworthy, giving us a level of confidence that the bridge is fit-for-purpose.

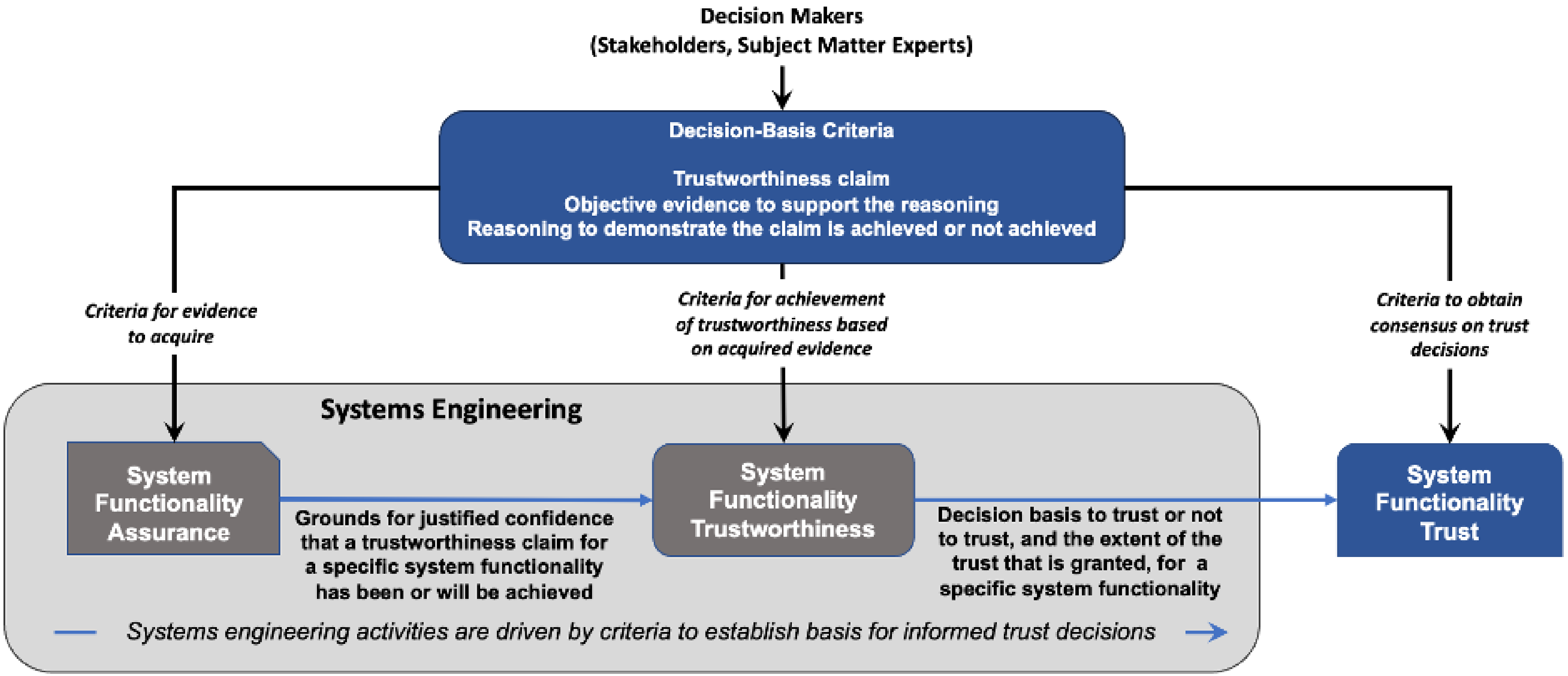
For system developers, there are also fundamental principles and concepts that can be found in mathematics, computer science, computer and electrical engineering, systems engineering, and software engineering that when properly employed, provide the necessary trustworthiness to engender that same level of confidence. Trustworthy secure systems are achieved by making a significant and substantial investment in strengthening the underlying systems and system components by employing transdisciplinary systems engineering efforts guided and informed by well-defined security requirements and secure architectures and designs. Such efforts have been proven over time to produce sound engineering-based solutions to complex and challenging systems security problems. Only under those circumstances can we build systems that are adequately secure and exhibit a level of trustworthiness that is sufficient for the purpose for which the system was built.

"Scientists study the world as it is, engineers create the world that never has been."

Theodore von Kármán
1962 National Medal of Science Recipient

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

… building assured system trustworthiness



Decision Makers
(Stakeholders, Subject Matter Experts)

Decision-Basis Criteria

Trustworthiness claim
Objective evidence to support the reasoning
Reasoning to demonstrate the claim is achieved or not achieved

Criteria for evidence to acquire

Criteria for achievement of trustworthiness based on acquired evidence

Criteria to obtain consensus on trust decisions

Systems Engineering

System Functionality Assurance

Grounds for justified confidence that a trustworthiness claim for a specific system functionality has been or will be achieved

System Functionality Trustworthiness

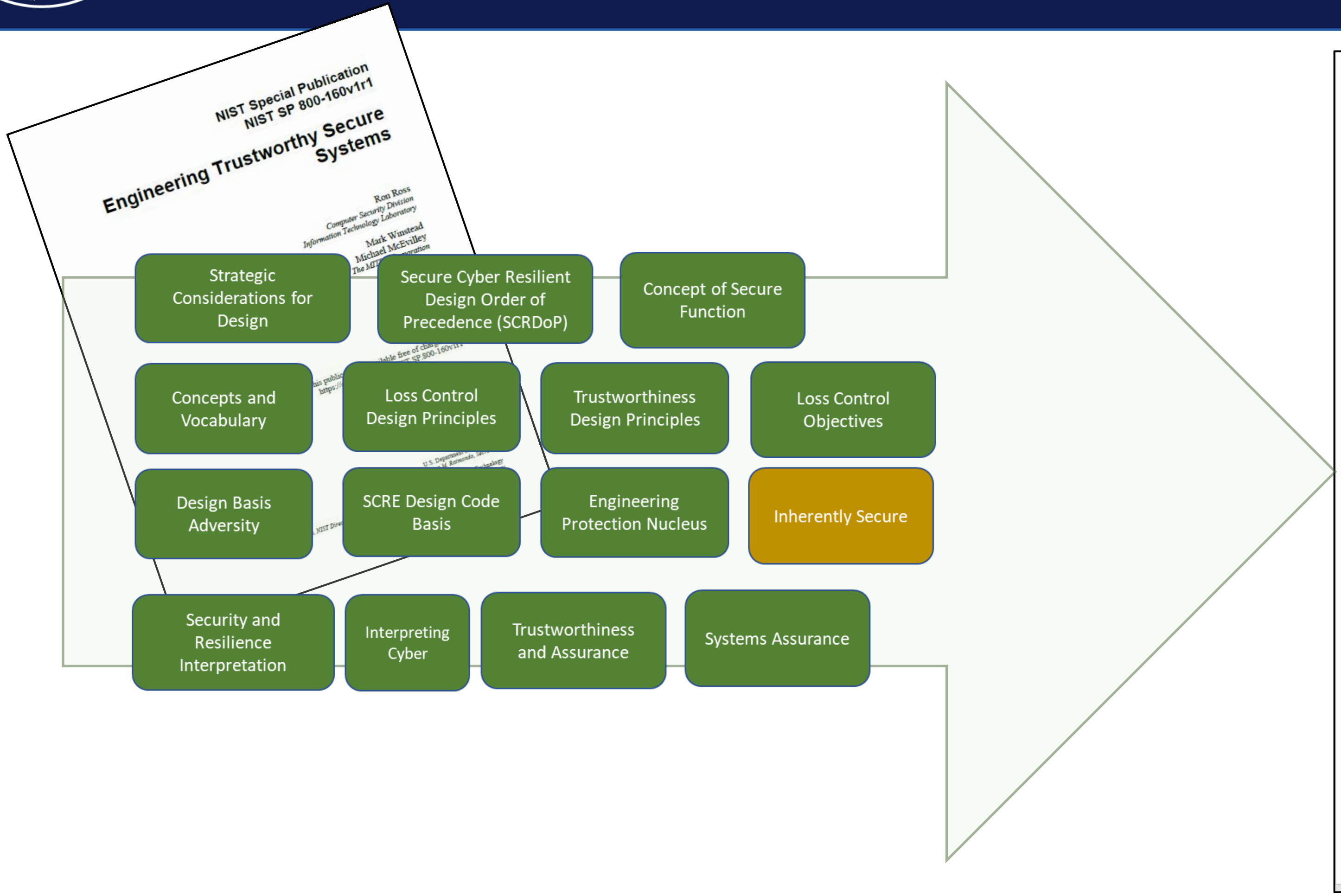
Decision basis to trust or not to trust, and the extent of the trust that is granted, for a specific system functionality

System Functionality Trust

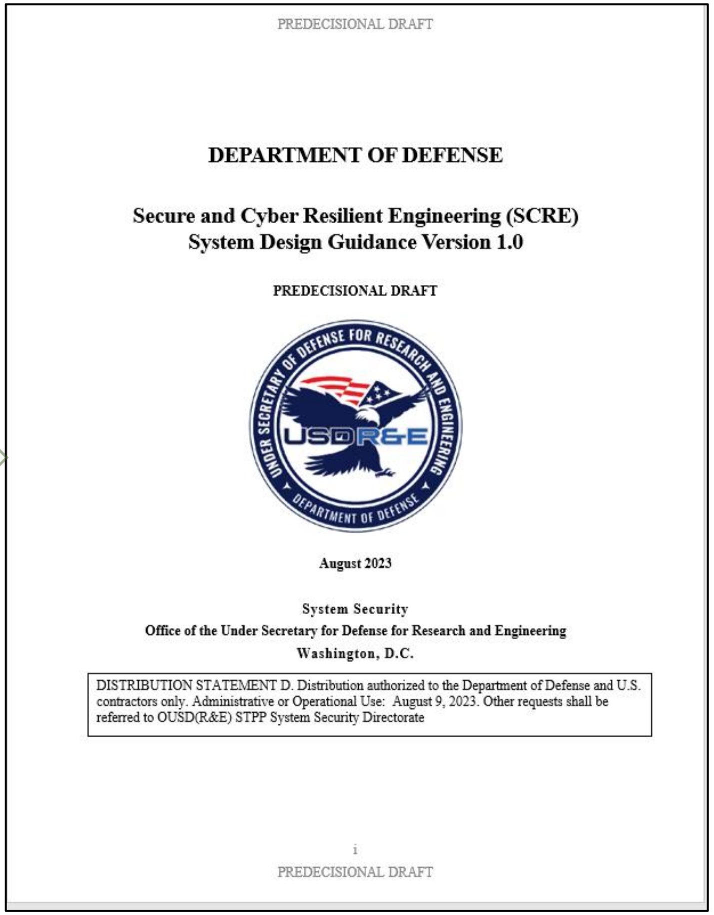
Systems engineering activities are driven by criteria to establish basis for informed trust decisions

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

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

Design Guidance Under Development

Workforce Competency

System Security Engineering

Secure Cyber Resilient Engineering

Defense Acquisition University

- Program Protection Credential Program
  - ACQ 160: Program Protection Planning Awareness
  - ACQ
  - ENG 260: Program Protection for Practitioners
- CLE 022: Program Manager Introduction to Anti-Tamper

Defense Acquisition University

- Secure Cyber Resilient Engineering Credential Program

Partnering with NDIA System Security Engineering Committee and DAU

- Hardware Assurance Tabletop Tutorial initiative

Partnered with National Defense University and National Security Agency

- Included “Integrating Cross Domain Solutions” in the fall 2023 NDU Cybersecurity Awareness course syllabus

Summary

Building enduring advantage requires:

- A world-class system security and secure cyber resilient engineering workforce that can engineer inherently safe and secure designs

- Partnerships across government, industry, academia, Allies and partners

- Technology and Program Protection Policy, guidance and standards that can adapt to an ever shifting and fast moving global environment to create and field capabilities at speed and scale

- System security and secure cyber resilient engineering tools to build cost effective inherently safe and secure systems

Customer-Focused: Outcome-Based

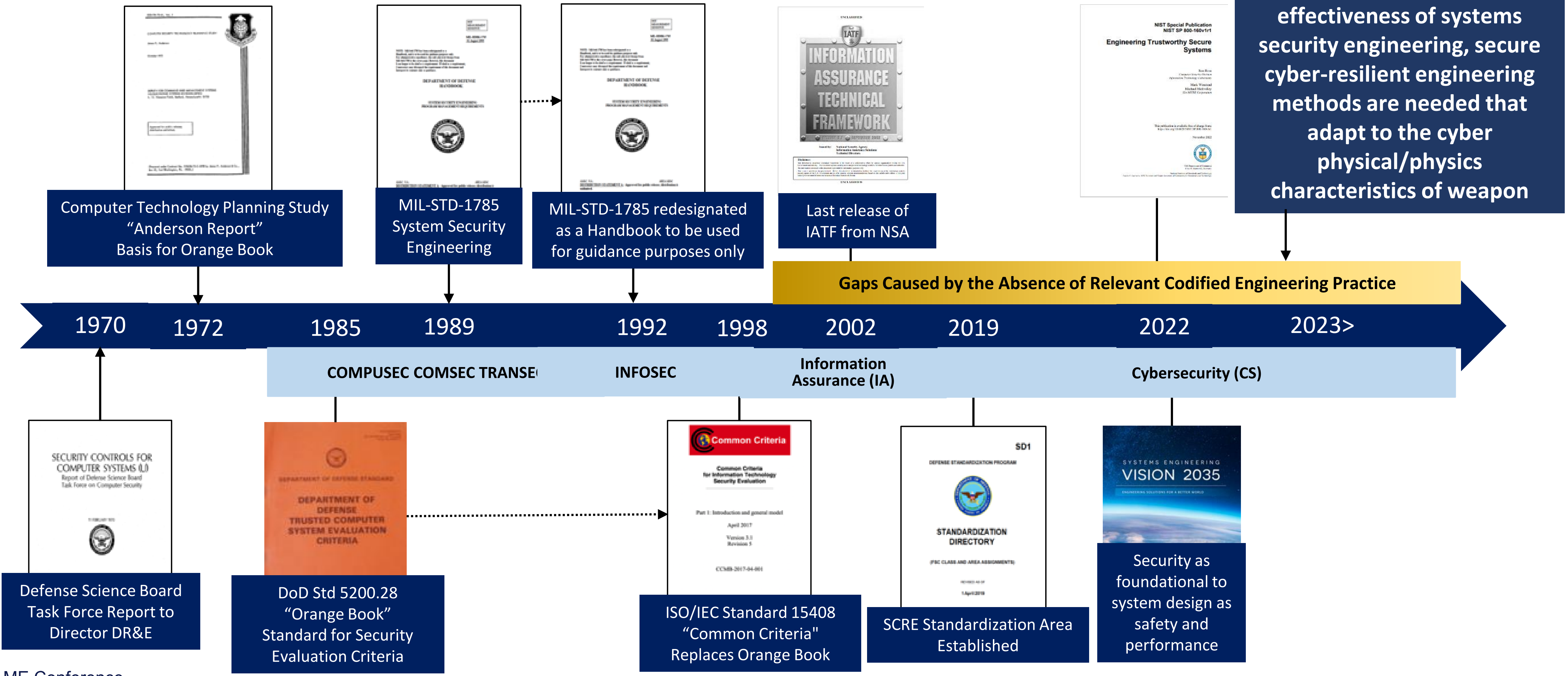
Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Questions?

Backup

Backup

DoD-centric System Security Engineering Timeline


INFORMATION ASSURANCE TECHNICAL FRAMEWORK
NIST Special Publication NIST SP 800-160v1r1
Engineering Trustworthy Secure Systems
SECURITY CONTROLS FOR COMPUTER SYSTEMS (U)
Report of Defense Science Board Task Force on Computer Security
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
Common Criteria
Common Criteria for Information Technology Security Evaluation
SD1
STANDARDIZATION DIRECTORY
SYSTEMS ENGINEERING
VISION 2035
1970
1972
1985
1989
1992
1998
2002
2019
2022
2023>
COMPUSEC COMSEC TRANSE
INFOSEC
Information Assurance (IA)
Cybersecurity (CS)

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

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

Gaps Caused by the Absence of Relevant Codified Engineering Practice

Defense Science Board Task Force Report to Director DR&E

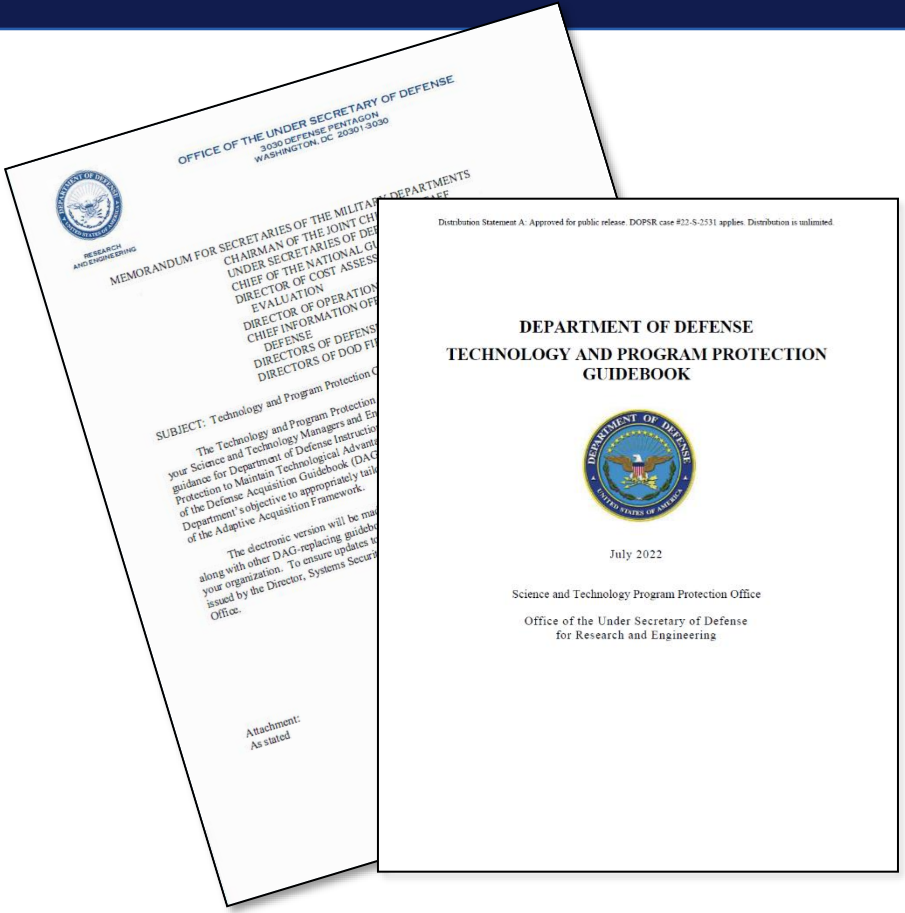
DoD Std 5200.28
"Orange Book"
Standard for Security Evaluation Criteria

ISO/IEC Standard 15408
"Common Criteria"
Replaces Orange Book

SCRE Standardization Area Established

Security as foundational to system design as safety and performance

Technology and Program Protection Guidebook



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CH
UNDER SECRETARIES OF DE
CHIEF OF THE NATIONAL GU
DIRECTOR OF COST ASSESS
EVALUATION
DIRECTOR OF OPERATION
CHIEF INFORMATION OF
DEFENSE
DIRECTORS OF DEFENS
DIRECTORS OF DOD FI

SUBJECT: Technology and Program Protection G

The Technology and Program Protection
your Science and Technology Managers and En
guidance for Department of Defense Instructio
Protection to Maintain Technological Advanta
of the Defense Acquisition Guidebook (DAG
Department's objective to appropriately tail
of the Adaptive Acquisition Framework.

The electronic version will be ma
along with other DAG-replacing guideb
your organization. To ensure updates t
issued by the Director, Systems Securi
Office.

Attachment:
As stated

Distribution Statement A: Approved for public release. DOPSR case #22-S-2531 applies. Distribution is unlimited.

DEPARTMENT OF DEFENSE

TECHNOLOGY AND PROGRAM PROTECTION
GUIDEBOOK

July 2022

Science and Technology Program Protection Office

Office of the Under Secretary of Defense
for Research and Engineering

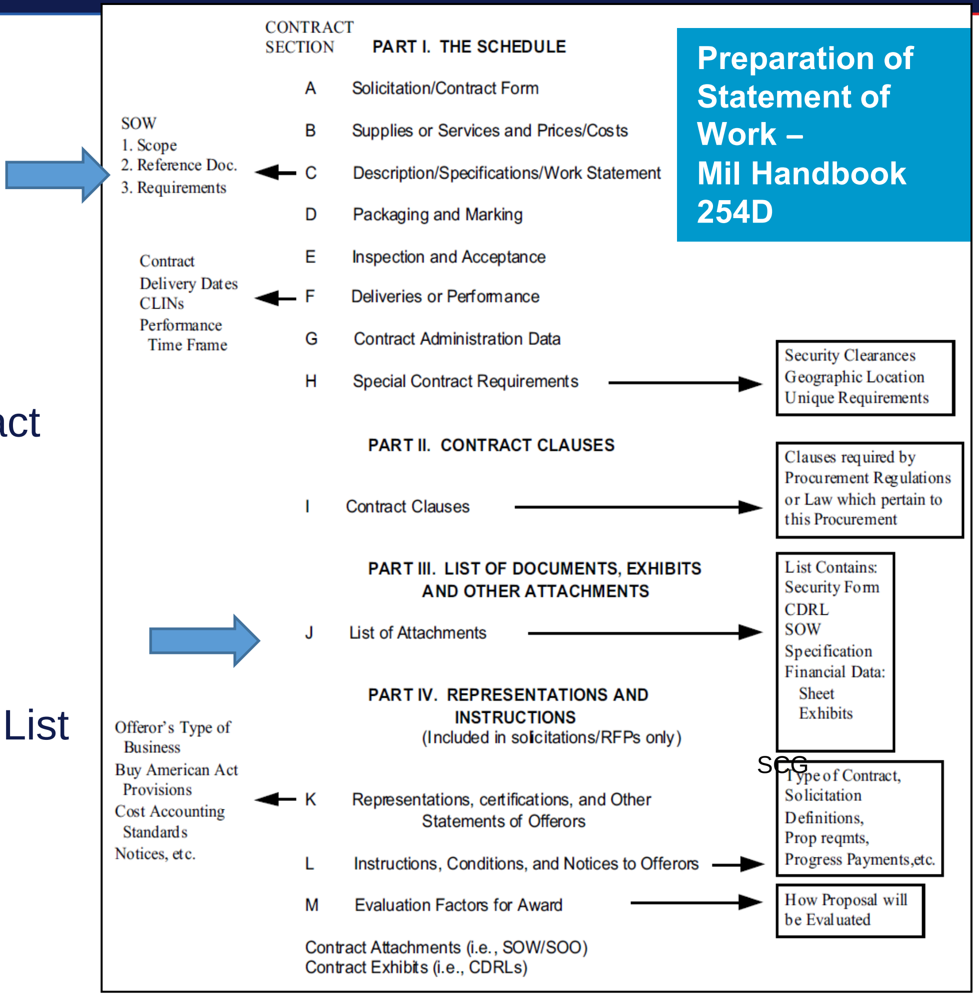
- **Provides implementing guidance for DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage"**
  - Replaces Defense Acquisition Guidebook (DAG) Chapter 9, "Program Protection"
- **Incorporates technology protection activities for DoD-sponsored research and technology**
- **Emphasizes the S&T manager and engineering responsibilities for technology protection, program protection, and cyber**
- **Aligns S&T manager and engineering procedures with DoDI 5000.02, "Operation of the Adaptive Acquisition Framework"**

Supports the Department's objective to tailor acquisition of capabilities through the Adaptive Acquisition Framework pathways

Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Acquiring Capability Through FAR-Based Contracting

- Statement of Work (Section C)
  - Prepared by Program Office (PM)/ Requiring Activity (RA)
- Contract Clauses (Section I),
  - Prepared by Contracting Officer
  - FAR Clause 52.204-2, when contract involves access to Confidential, Secret, or Top Secret information
  - FAR Clause 52.204-21, when contract involves Federal Contract Information
  - DFARS Clause 252.204-7012 in all contracts except COTS
- List of Attachments (Section J)
  - Attachments collected by Program Office
  - Data deliverables as identified in Contract Data Requirements List (CDRL): Prepared by PM/RA
  - Security Classification Guides
  - Specifications: Prepared by PMO/RA
  - Other Government Furnished Information: Various



CONTRACT SECTION — PART I. THE SCHEDULE

A Solicitation/Contract Form

B Supplies or Services and Prices/Costs

C Description/Specifications/Work Statement ← SOW 1. Scope 2. Reference Doc. 3. Requirements

D Packaging and Marking

E Inspection and Acceptance

F Deliveries or Perfomance ← Contract Delivery Dates CLINs Performance Time Frame

G Contract Administration Data

H Special Contract Requirements → Security Clearances Geographic Location Unique Requirements

PART II. CONTRACT CLAUSES

I Contract Clauses → Clauses required by Procurement Regulations or Law which pertain to this Procurement

PART III. LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

J List of Attachments → List Contains: Security Form CDRL SOW Specification Financial Data: Sheet Exhibits

PART IV. REPRESENTATIONS AND INSTRUCTIONS (Included in solicitations/RFPs only)

K Representations, certifications, and Other Statements of Offerors ← Offeror's Type of Business Buy American Act Provisions Cost Accounting Standards Notices, etc.

L Instructions, Conditions, and Notices to Offerors → SCG Type of Contract, Solicitation Definitions, Prop reqmts, Progress Payments,etc.

M Evaluation Factors for Award → How Proposal will be Evaluated

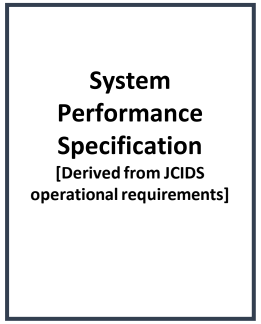
Contract Attachments (i.e., SOW/SOO)
Contract Exhibits (i.e., CDRLs)

Preparation of Statement of Work – Mil Handbook 254D

One approach is a Federal Acquisition Regulation (FAR)-Based Contract

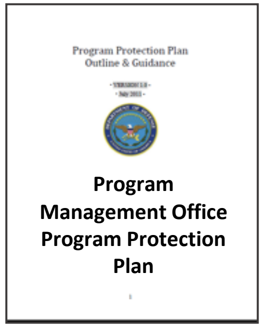
Distribution Statement A: Approved for public release, case #24-T-0021 applies. Distribution is unlimited.

Delivering Assured, Secure, Resilient Systems



System Performance Specification [Derived from JCIDS operational requirements]

Government Furnished Information



Program Protection Plan Outline & Guidance

- VERSION 1.0 -

July 2011

Program Management Office Program Protection Plan

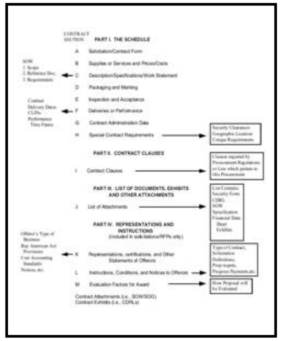
Government Furnished Information

Section C Statement of Work

Contract Data Requirements List (CDRL)

Section I FAR/DFAR Contract Clauses

Consistent implementation will provide balanced and seamless protections



CONTRACT SECTION
PART I. THE SCHEDULE
A Solicitation/Contract Form
B Supplies or Services and Prices/Costs
C Description/Specifications/Work Statement
D Packaging and Marking
E Inspection and Acceptance
F Deliveries or Performance
G Contract Administration Data
H Special Contract Requirements
PART II. CONTRACT CLAUSES
I Contract Clauses
PART III. LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS
J List of Attachments
PART IV. REPRESENTATIONS AND INSTRUCTIONS
(included in solicitations/RFPs only)
K Representations, certifications, and Other Statements of Offerors
L Instructions, Conditions, and Notices to Offerors
M Evaluation Factors for Award
Contract Attachments (i.e., SOW/SOO)
Contract Exhibits (i.e., CDRLs)
SOW
1. Scope
2. Reference Doc.
3. Requirements
Contract
Delivery Dates
CLINs
Performance
Time Frame
Security Clearances
Geographic Location
Unique Requirements
Clauses required by Procurement Regulations or Law which pertain to this Procurement
List Contains:
Security Form
CDRL
SOW
Specification
Financial Data
Sheet
Exhibits
Offeror's Type of Business
Buy American Act Provisions
Cost Accounting Standards
Notices, etc.
Type of Contract,
Solicitation
Definitions,
Prop reqmts,
Progress Payments,etc.
How Proposal will be Evaluated

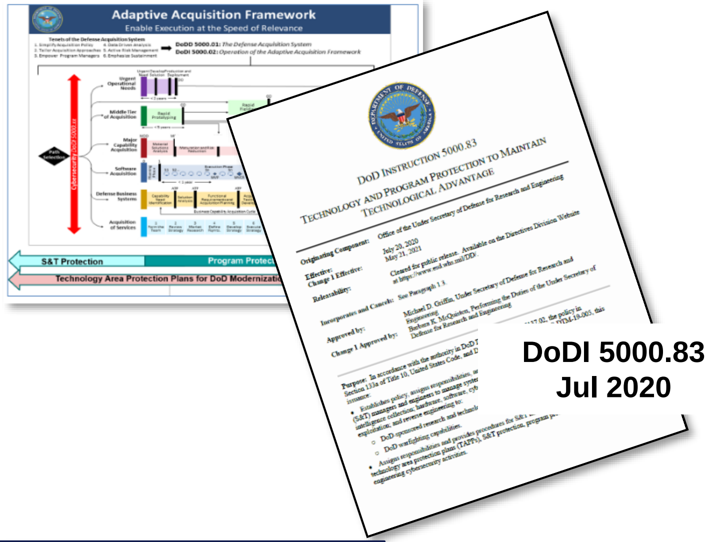
Solicitation/Contract

Increase consistency and repeatability of system assurance, system security, and cybersecurity methods and technologies

Improve expectations across Government, industry, academia and operational stakeholders

Distribution Statement A: Approved for public release. DOPSR case #24-T-0022 applies. Distribution is unlimited.

Alignment to the Adaptive Acquisition Framework



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*

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

Change 1 Effective: May 21, 2021

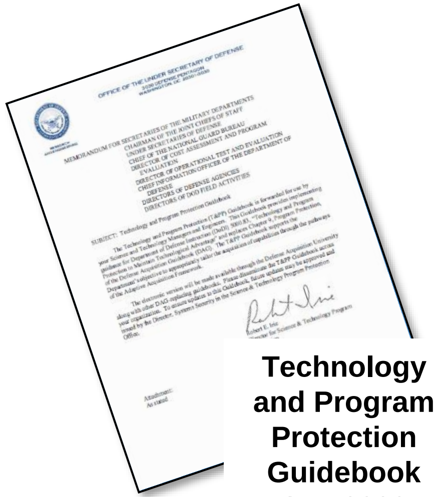
Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Incorporates and Cancels: See Paragraph 1.3.

Approved by: Michael D. Griffin, Under Secretary of Defense for Research and Engineering

Change 1 Approved by: Barbara K. McQuiston, Performing the Duties of the Under Secretary of Defense for Research and Engineering

DoDI 5000.83
Jul 2020

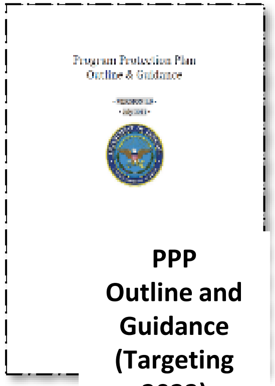


OFFICE OF THE UNDER SECRETARY OF DEFENSE

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP, COMMANDERS OF THE COMBATANT COMMANDS, DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

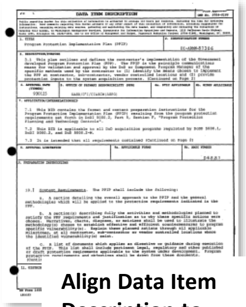
SUBJECT: Technology and Program Protection Guidebook

Technology and Program Protection Guidebook Sep 2022



Program Protection Plan Outline & Guidance

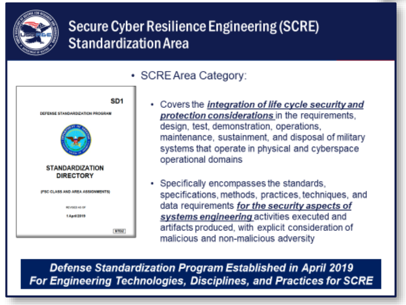
PPP Outline and Guidance (Targeting 2023)



DATA ITEM DESCRIPTION

Align Data Item Description to Updated Tables

- Fact of Life Policy Updates
- Acquisition Regulations updates
- Standardization
- Remove duplication
- Lessons Learned



Secure Cyber Resilience Engineering (SCRE) Standardization Area

- 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

SD1

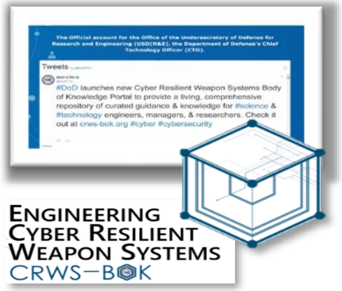
DEFENSE STANDARDIZATION PROGRAM

STANDARDIZATION DIRECTORY

(FSC CLASS AND AREA ASSIGNMENTS)

1 April 2019

Defense Standardization Program Established in April 2019
For Engineering Technologies, Disciplines, and Practices for SCRE



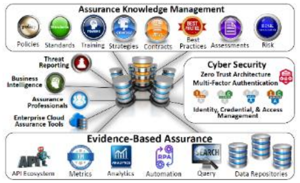
The Official account for the Office of the Undersecretary of Defense for Research and Engineering (USD(R&E)), the Department of Defense's Chief Technology Officer (CTO).

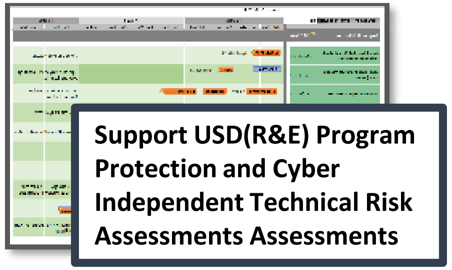
Tweets

#DoD launches new Cyber Resilient Weapon Systems Body of Knowledge Portal to provide a living, comprehensive repository of curated guidance & knowledge for #science & #technology engineers, managers, & researchers. Check it out at crws-bok.org #cyber #cybersecurity

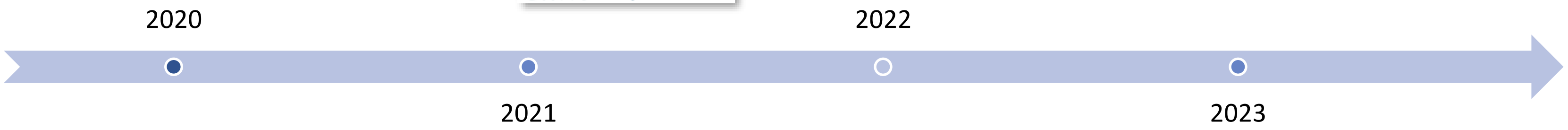
ENGINEERING CYBER RESILIENT WEAPON SYSTEMS

CRWS—BOK



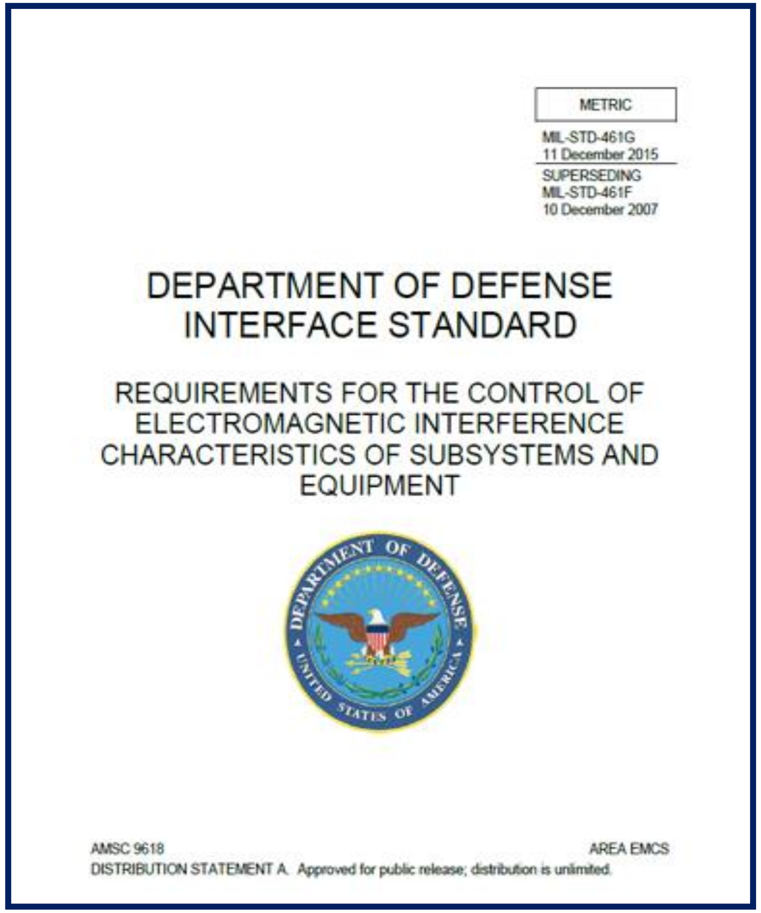


Support USD(R&E) Program Protection and Cyber Independent Technical Risk Assessments Assessments



Distribution Statement A: Approved for public release. DOPSR case #24-T-0021 applies. Distribution is unlimited.

Example of a DoD Standard



METRIC

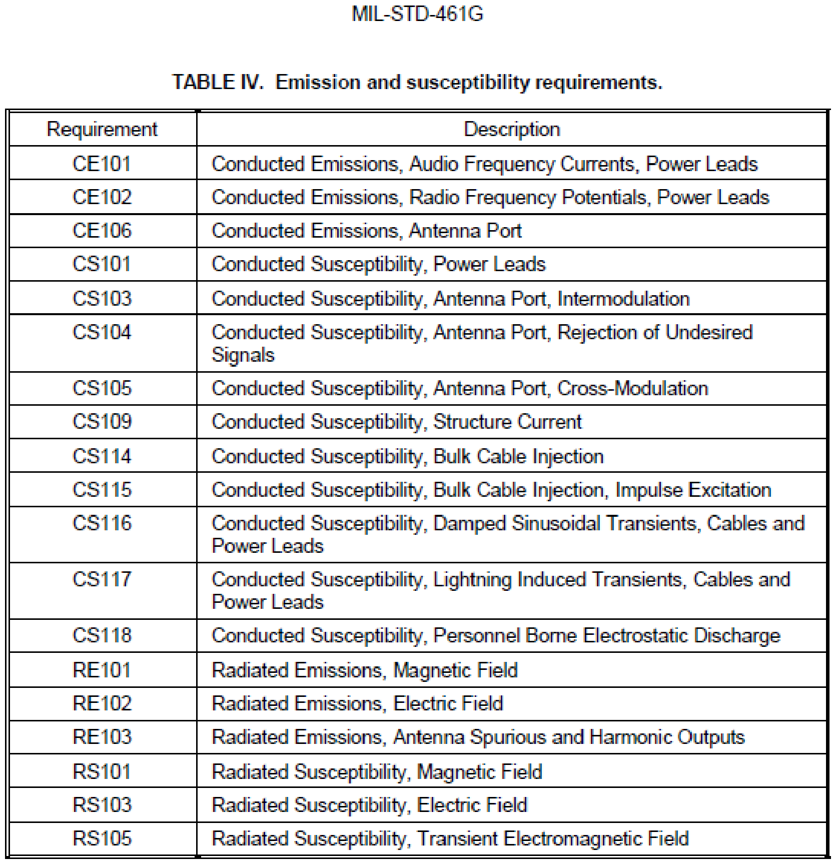
MIL-STD-461G
11 December 2015
SUPERSEDING
MIL-STD-461F
10 December 2007

DEPARTMENT OF DEFENSE
INTERFACE STANDARD

REQUIREMENTS FOR THE CONTROL OF ELECTROMAGNETIC INTERFERENCE CHARACTERISTICS OF SUBSYSTEMS AND EQUIPMENT

AMSC 9618 AREA EMCS

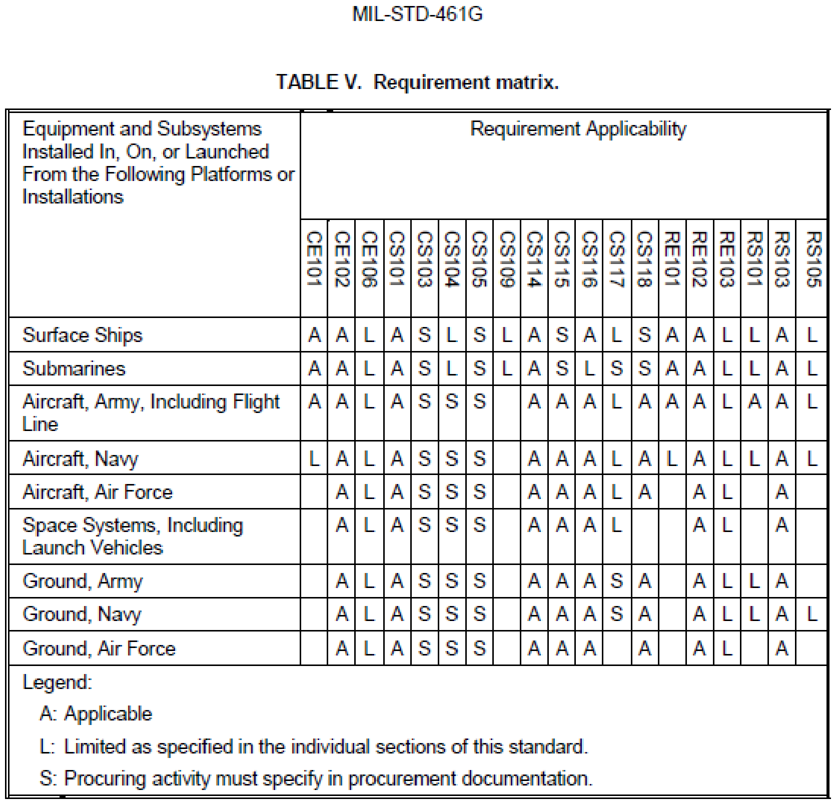
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.



MIL-STD-461G

TABLE IV. Emission and susceptibility requirements.

Requirement	Description
CE101	Conducted Emissions, Audio Frequency Currents, Power Leads
CE102	Conducted Emissions, Radio Frequency Potentials, Power Leads
CE106	Conducted Emissions, Antenna Port
CS101	Conducted Susceptibility, Power Leads
CS103	Conducted Susceptibility, Antenna Port, Intermodulation
CS104	Conducted Susceptibility, Antenna Port, Rejection of Undesired Signals
CS105	Conducted Susceptibility, Antenna Port, Cross-Modulation
CS109	Conducted Susceptibility, Structure Current
CS114	Conducted Susceptibility, Bulk Cable Injection
CS115	Conducted Susceptibility, Bulk Cable Injection, Impulse Excitation
CS116	Conducted Susceptibility, Damped Sinusoidal Transients, Cables and Power Leads
CS117	Conducted Susceptibility, Lightning Induced Transients, Cables and Power Leads
CS118	Conducted Susceptibility, Personnel Borne Electrostatic Discharge
RE101	Radiated Emissions, Magnetic Field
RE102	Radiated Emissions, Electric Field
RE103	Radiated Emissions, Antenna Spurious and Harmonic Outputs
RS101	Radiated Susceptibility, Magnetic Field
RS103	Radiated Susceptibility, Electric Field
RS105	Radiated Susceptibility, Transient Electromagnetic Field



MIL-STD-461G

TABLE V. Requirement matrix.

Equipment and Subsystems Installed In, On, or Launched From the Following Platforms or Installations	Requirement Applicability																		
	CE101	CE102	CE106	CS101	CS103	CS104	CS105	CS109	CS114	CS115	CS116	CS117	CS118	RE101	RE102	RE103	RS101	RS103	RS105
Surface Ships	A	A	L	A	S	L	S	L	A	S	A	L	S	A	A	L	L	A	L
Submarines	A	A	L	A	S	L	S	L	A	S	L	S	S	A	A	L	L	A	L
Aircraft, Army, Including Flight Line	A	A	L	A	S	S	S		A	A	A	L	A	A	A	L	A	A	L
Aircraft, Navy	L	A	L	A	S	S	S		A	A	A	L	A	L	A	L	L	A	L
Aircraft, Air Force		A	L	A	S	S	S		A	A	A	L	A		A	L		A	
Space Systems, Including Launch Vehicles		A	L	A	S	S	S		A	A	A	L			A	L		A	
Ground, Army		A	L	A	S	S	S		A	A	A	S	A		A	L	L	A	
Ground, Navy		A	L	A	S	S	S		A	A	A	S	A		A	L	L	A	L
Ground, Air Force		A	L	A	S	S	S		A	A	A		A		A	L		A	

Legend:

A: Applicable

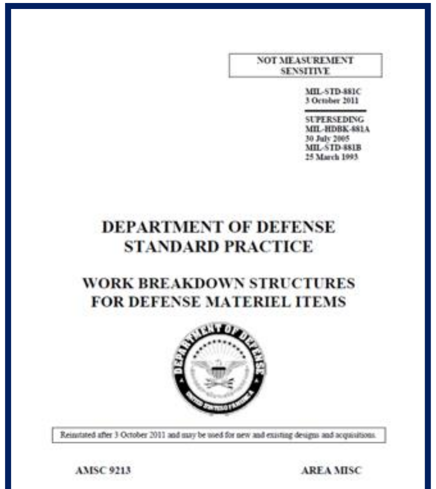
L: Limited as specified in the individual sections of this standard.

S: Procuring activity must specify in procurement documentation.

System requirements vary across weapon system platform, installation, use, and operational environments.

Distribution Statement A: Approved for public release, case #24-T-0021 applies. Distribution is unlimited.

Standard Practices for Work Breakdown Structures



NOT MEASUREMENT SENSITIVE

MIL-STD-881C
3 October 2011

SUPERSEDING
MIL-HDBK-881A
30 July 2005
MIL-STD-881B
25 March 1993

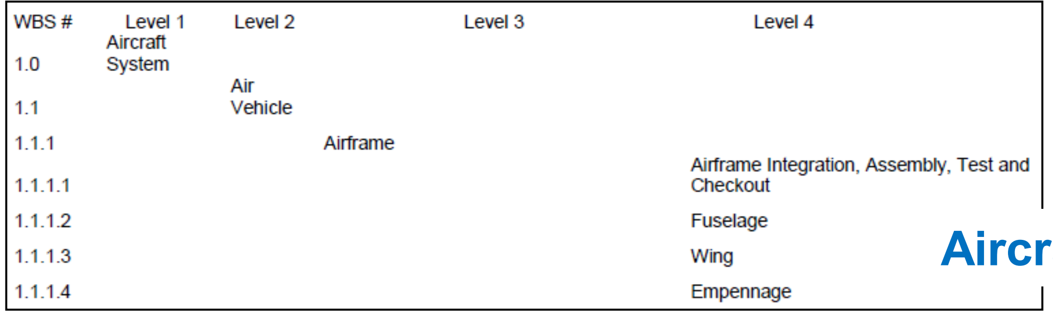
DEPARTMENT OF DEFENSE
STANDARD PRACTICE

WORK BREAKDOWN STRUCTURES
FOR DEFENSE MATERIEL ITEMS

Reinstated after 3 October 2011 and may be used for new and existing designs and acquisitions.

AMSC 9213 AREA MISC

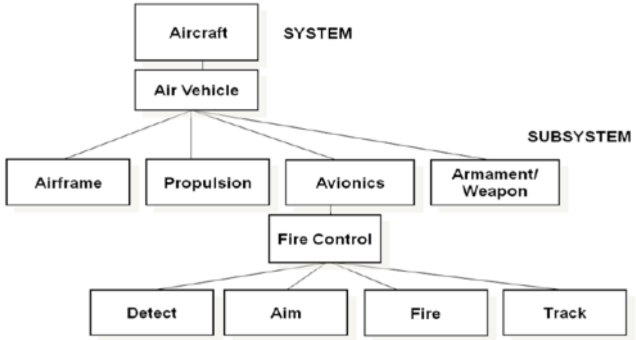
MIL-STD-881C

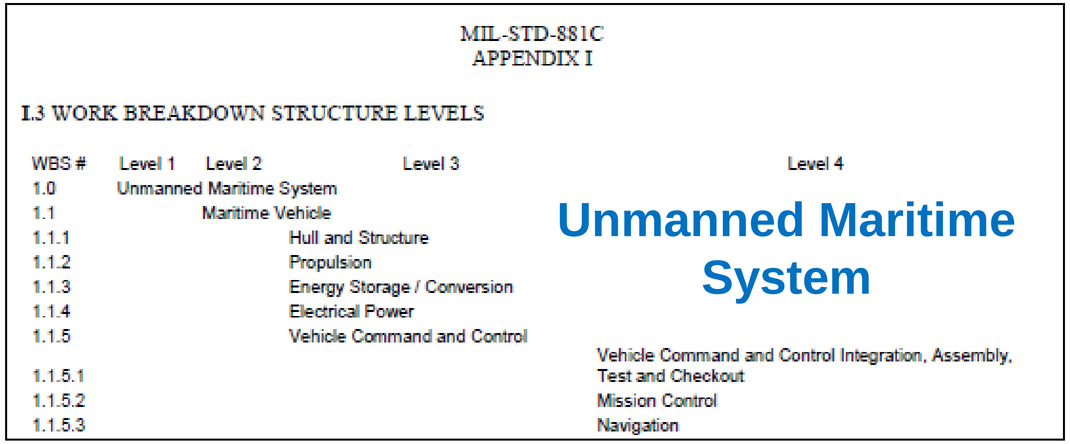


WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Aircraft System			
1.1		Air Vehicle		
1.1.1			Airframe	
1.1.1.1				Airframe Integration, Assembly, Test and Checkout
1.1.1.2				Fuselage
1.1.1.3				Wing
1.1.1.4				Empennage

Aircraft System

Provides a consistent and visible framework for defense materiel items



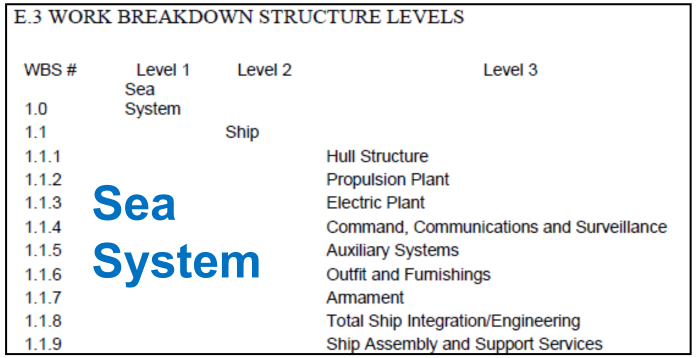


MIL-STD-881C
APPENDIX I

I.3 WORK BREAKDOWN STRUCTURE LEVELS

WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Unmanned Maritime System			
1.1		Maritime Vehicle		
1.1.1			Hull and Structure	
1.1.2			Propulsion	
1.1.3			Energy Storage / Conversion	
1.1.4			Electrical Power	
1.1.5			Vehicle Command and Control	
1.1.5.1				Vehicle Command and Control Integration, Assembly, Test and Checkout
1.1.5.2				Mission Control
1.1.5.3				Navigation

Unmanned Maritime System



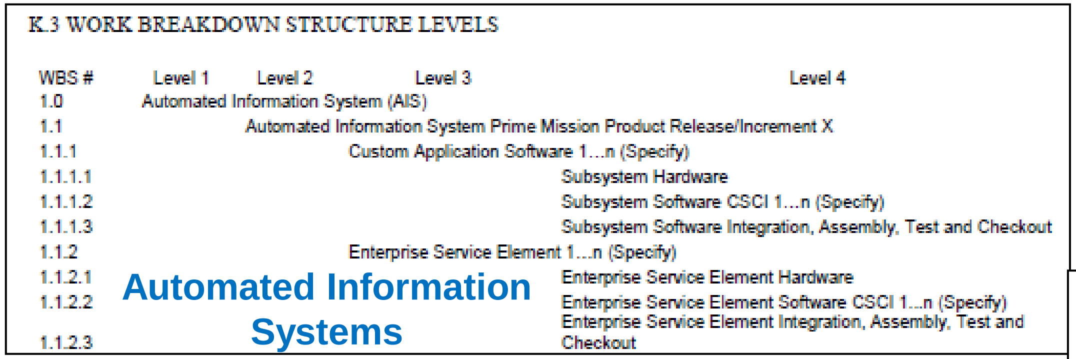
E.3 WORK BREAKDOWN STRUCTURE LEVELS

WBS #	Level 1	Level 2	Level 3
1.0	Sea System		
1.1		Ship	
1.1.1			Hull Structure
1.1.2			Propulsion Plant
1.1.3			Electric Plant
1.1.4			Command, Communications and Surveillance
1.1.5			Auxiliary Systems
1.1.6			Outfit and Furnishings
1.1.7			Armament
1.1.8			Total Ship Integration/Engineering
1.1.9			Ship Assembly and Support Services

Sea System

Distribution Statement A: Approved for public release, case #24-T-0021 applies. Distribution is unlimited.

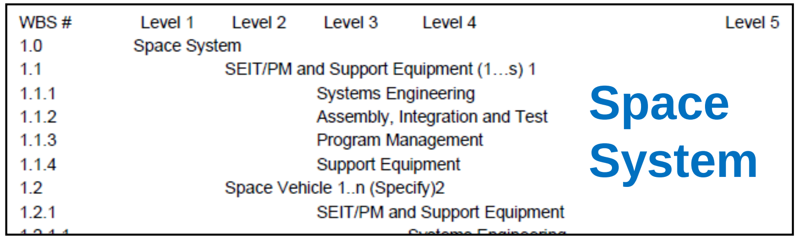
Standard Practices for Work Breakdown Structures – more…



K.3 WORK BREAKDOWN STRUCTURE LEVELS

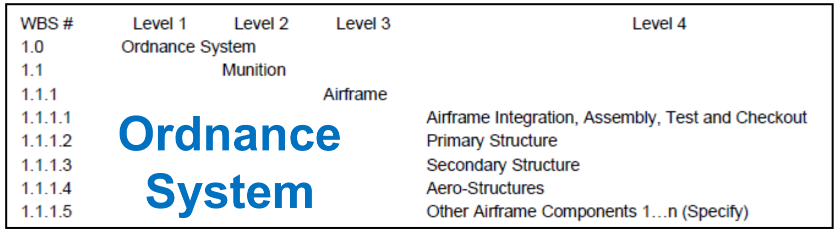
WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Automated Information System (AIS)			
1.1		Automated Information System Prime Mission Product Release/Increment X		
1.1.1			Custom Application Software 1…n (Specify)	
1.1.1.1				Subsystem Hardware
1.1.1.2				Subsystem Software CSCI 1…n (Specify)
1.1.1.3				Subsystem Software Integration, Assembly, Test and Checkout
1.1.2			Enterprise Service Element 1…n (Specify)	
1.1.2.1				Enterprise Service Element Hardware
1.1.2.2				Enterprise Service Element Software CSCI 1…n (Specify)
1.1.2.3				Enterprise Service Element Integration, Assembly, Test and Checkout

Automated Information Systems



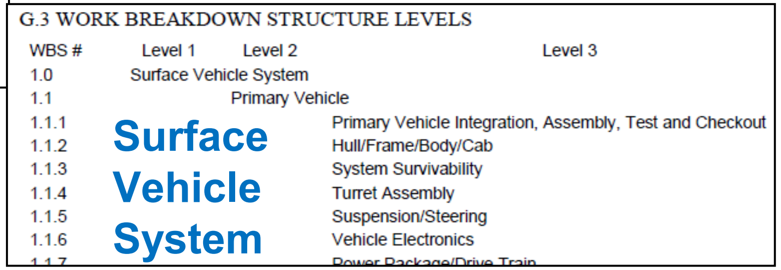
WBS #	Level 1	Level 2	Level 3	Level 4	Level 5
1.0	Space System				
1.1		SEIT/PM and Support Equipment (1…s) 1			
1.1.1			Systems Engineering		
1.1.2			Assembly, Integration and Test		
1.1.3			Program Management		
1.1.4			Support Equipment		
1.2		Space Vehicle 1..n (Specify)2			
1.2.1			SEIT/PM and Support Equipment		
1.2.1.1				Systems Engineering	

Space System



WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Ordnance System			
1.1		Munition		
1.1.1			Airframe	
1.1.1.1				Airframe Integration, Assembly, Test and Checkout
1.1.1.2				Primary Structure
1.1.1.3				Secondary Structure
1.1.1.4				Aero-Structures
1.1.1.5				Other Airframe Components 1…n (Specify)

Ordnance System

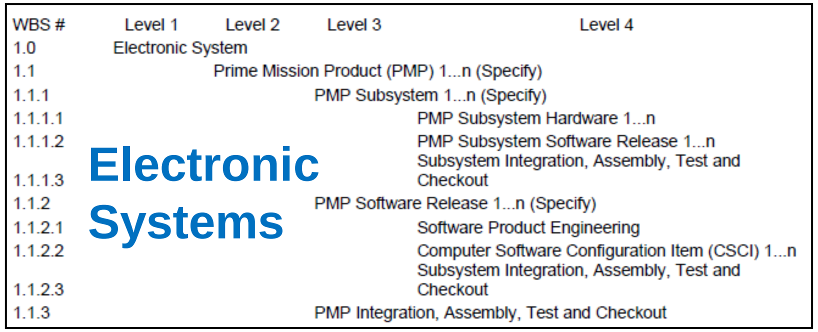


G.3 WORK BREAKDOWN STRUCTURE LEVELS

WBS #	Level 1	Level 2	Level 3
1.0	Surface Vehicle System		
1.1		Primary Vehicle	
1.1.1			Primary Vehicle Integration, Assembly, Test and Checkout
1.1.2			Hull/Frame/Body/Cab
1.1.3			System Survivability
1.1.4			Turret Assembly
1.1.5			Suspension/Steering
1.1.6			Vehicle Electronics
1.1.7			Power Package/Drive Train

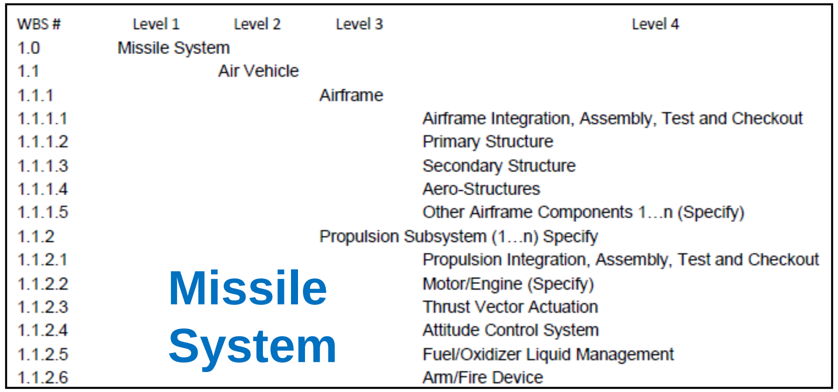
Surface Vehicle System

Complete Work Breakdown Structures can be found in MIL-STD 881



WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Electronic System			
1.1		Prime Mission Product (PMP) 1...n (Specify)		
1.1.1			PMP Subsystem 1...n (Specify)	
1.1.1.1				PMP Subsystem Hardware 1...n
1.1.1.2				PMP Subsystem Software Release 1...n
1.1.1.3				Subsystem Integration, Assembly, Test and Checkout
1.1.2			PMP Software Release 1...n (Specify)	
1.1.2.1				Software Product Engineering
1.1.2.2				Computer Software Configuration Item (CSCI) 1...n
1.1.2.3				Subsystem Integration, Assembly, Test and Checkout
1.1.3			PMP Integration, Assembly, Test and Checkout	

Electronic Systems



WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Missile System			
1.1		Air Vehicle		
1.1.1			Airframe	
1.1.1.1				Airframe Integration, Assembly, Test and Checkout
1.1.1.2				Primary Structure
1.1.1.3				Secondary Structure
1.1.1.4				Aero-Structures
1.1.1.5				Other Airframe Components 1…n (Specify)
1.1.2			Propulsion Subsystem (1…n) Specify	
1.1.2.1				Propulsion Integration, Assembly, Test and Checkout
1.1.2.2				Motor/Engine (Specify)
1.1.2.3				Thrust Vector Actuation
1.1.2.4				Attitude Control System
1.1.2.5				Fuel/Oxidizer Liquid Management
1.1.2.6				Arm/Fire Device

Missile System

Distribution Statement A: Approved for public release, case #24-T-0022 applies. Distribution is unlimited.