



Standardization for the Engineering of Secure and Cyber Resilient Weapons Systems

Ms. Melinda Reed

Strategic Technology Protection & Exploitation

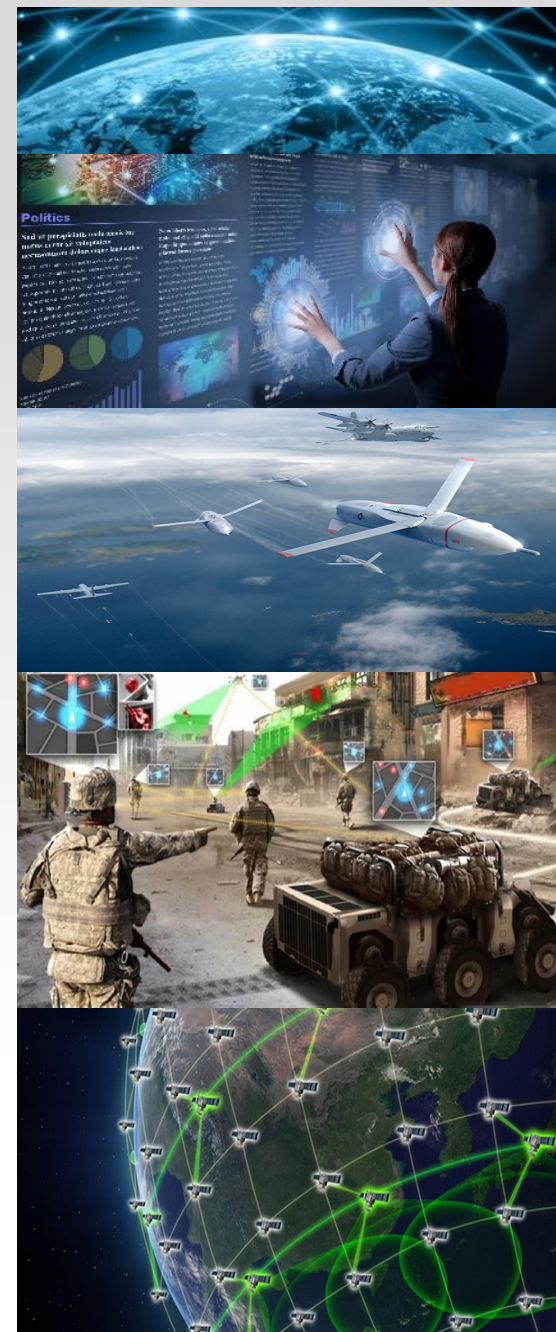
Office of the Under Secretary of Defense (Research & Engineering)

Mr. Michael McEvilley

MITRE Corporation

22nd Annual NDIA Systems and Mission Engineering Conference

Tampa, FL | October 23, 2019





Agenda

- **Secure Cyber Resilient Engineering (SCRE) Background**
- **Secure Cyber Resilient Engineering (SCRE) Standardization Area**
- **Next Steps**



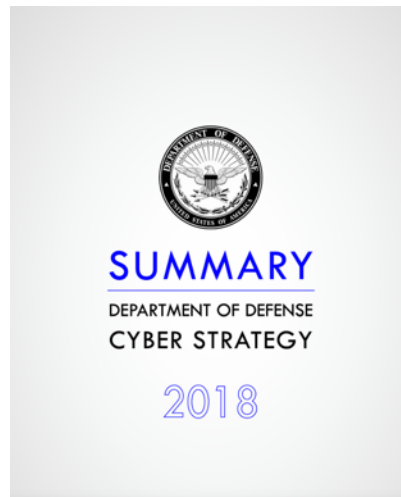
Background DoD Cyber Strategy

Engineering Cyber Resilient Weapon Systems Goal:

Improve resiliency of weapons system designs to cyber attack

Objectives:

- Determine set of engineering design patterns, standards and methods for cyber resilient weapon systems, addressing both systems in development and systems in sustainment
- Establish a foundation to grow the engineering practices and strengthen engineering agility



Innovate to foster agility:

The Department must innovate to keep pace with rapidly evolving threats and technologies in cyberspace. We will accept and manage operational and programmatic risk in a deliberate manner that moves from a “zero defect” culture to one that fosters agility and innovation because success in this domain requires the Department to innovate faster than our strategic competitors.



Background: Design for Cyber Threat Environments



- Allocate cybersecurity and related system security requirements to the system architecture; design and assess for vulnerabilities.
- The system architecture and design will address, at a minimum, how the system:
 - Manages access to and use of the system and system resources
 - Is structured to protect and preserve system functions or resources, (e.g., through segmentation, separation, isolation, or partitioning)
 - Is configured to minimize exposure of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides and patch management in the development environment (including integration and T&E), in production and throughout sustainment.
 - Monitors, detects, and responds to security anomalies.
 - Maintains priority system functions under adverse conditions; and
 - Interfaces with DoD Information Network (DoDIN) or other external security services

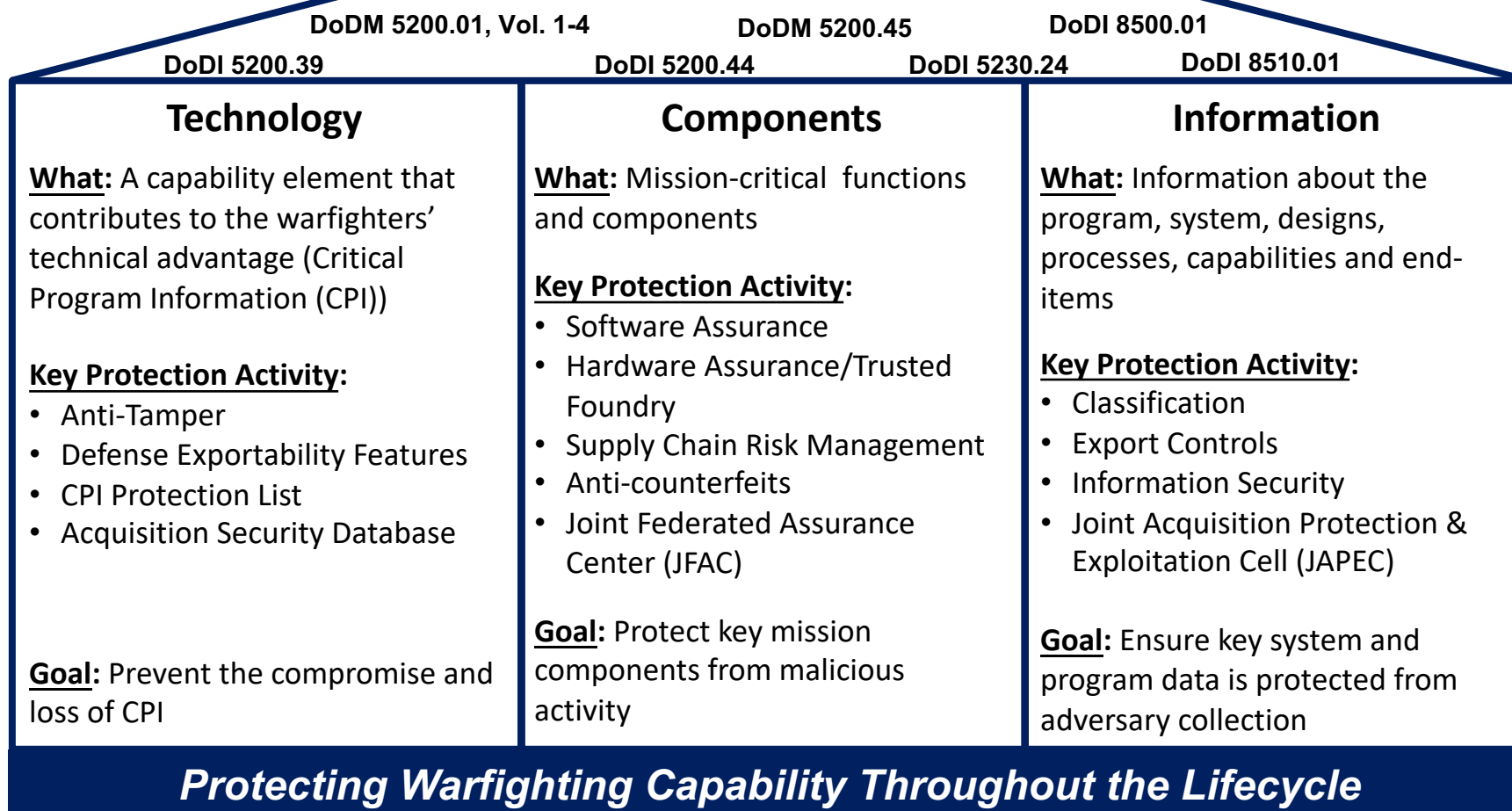
Design Considerations to Mitigate Cybersecurity Implications to the System



Protection Activities for Contested Cyberspace Environments

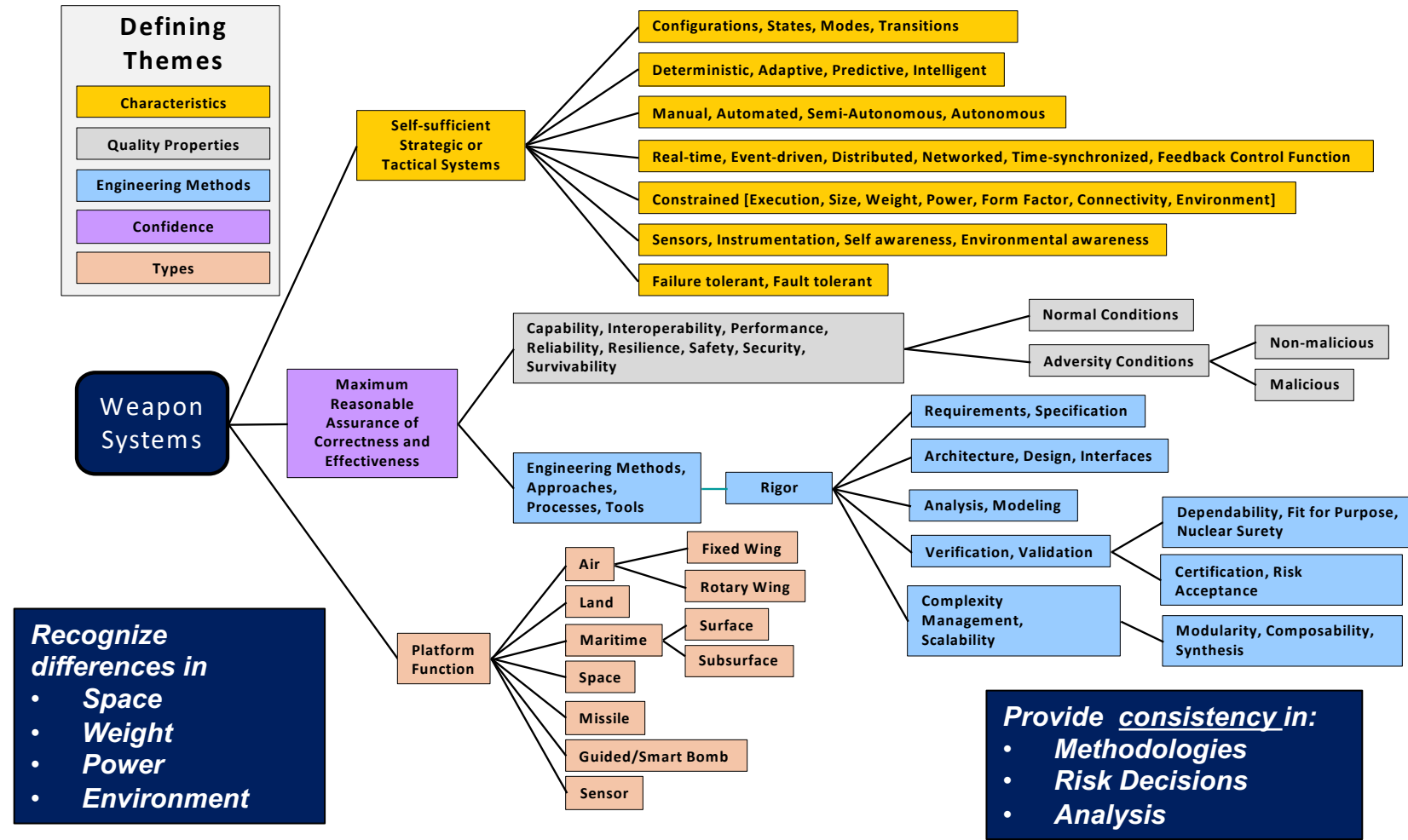
Program Protection & Cybersecurity

DoDI 5000.02, Enclosures 3 & 14





Weapon Systems Characteristics



Weapon Systems Deliver Lethal Force with the Intent to Cause Harm



Defense Standardization Program



- Military Specification - Defines requirements & tests for military-unique items
- Military Standard - Defines requirements for military-unique processes, test methods, practices
- Military Handbook - Provides guidance for selection of items or engineering approaches
- Data Item Description (DID) – Provides content and format requirements for data deliverables listed on Contract Data Requirements Lists (CDRL)
- Federal Specification – Defines requirements & tests for federal government unique items
- Federal Standard – Defines requirements for federal government unique processes, test methods, practices
- Commercial Item Description (CID) - Defines requirements for commercially available items

DoD specifications, standards, and other related DoD standardization documents shall be developed and maintained in accordance with DoD Manual 4120.24, Defense Standardization Program



Example of a DoD Standard


MIL-STD-461G

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.

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.

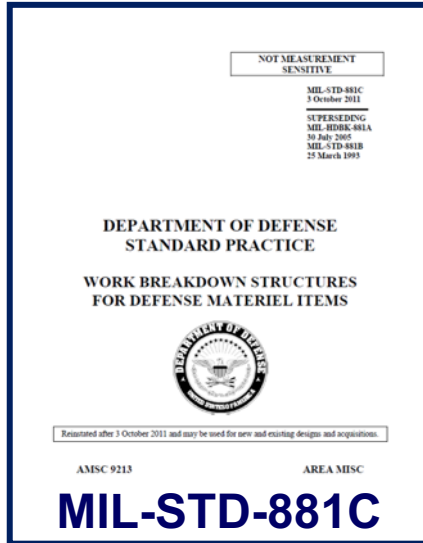
Equipment and Subsystems Installed In, On, or Launched From the Following Platforms or Installations	Requirement Applicability																		
	CE101	CE102	CE106	CS101	CS103	CS104	CS105	CS109	CS114	CS115	CS116	CS117	CS118	RE101	RE102	RE103	RS101	RS103	RS105
Surface Ships	A	A	L	A	S	L	S	L	A	S	A	L	S	A	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.



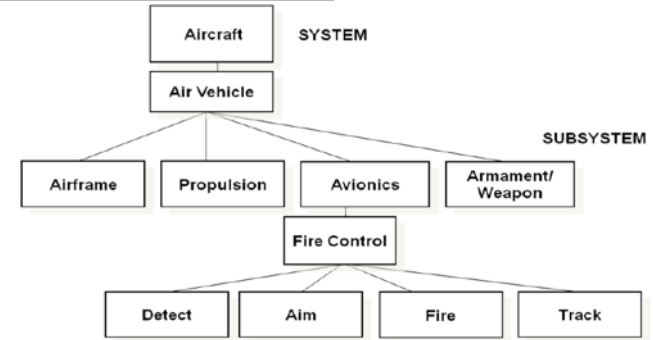
Standard Practices for Work Breakdown Structures



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



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	Customs 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



Standard for Data Item Descriptions MIL-STD-963C



Database last updated: Oct 23, 2015 [Home](#) | [About Quick Search](#) | [ASSIST](#) | [ASSIST Updates](#)

NOTICE: The assistdocs.com website has been discontinued; however, the public may access releasable DSP documents from ASSIST Quick Search (<http://quicksearch.dla.mil>).
 Enter search criteria in one or more of three text fields: Document ID, Document Number, Find Term(s). Filter search results by selecting Status or FSC/Area from drop-down lists, or by checking the box and specifying a range of document dates. Click a label for a detailed description and sample search results.

Basic Search **Text Search**

Document ID: Document Number: Status:
 Find Term1,Term2,.... For In
 FSC/Area: Document Date: Through

[About Quick Search](#) | [ASSIST](#)

DLA Document Services, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.
 If you have any questions, please contact the ASSIST-Help Desk team at 215-697-8396 [DSN: 442-8396].
[Privacy and Security Information](#) and [Section 508 Compliance Information](#). Questions or comments: [ASSIST Feedback](#).

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 1996) AND CAN RESULT IN ADMINISTRATIVE, DISCIPLINARY OR CRIMINAL PROCEEDINGS.

General Guidance:

- New DIDs shall not be prepared if an existing DID is adequate to define the required data product as is or with tailoring.
- A DID shall cover a single deliverable data product.
- If a single work task generates more than one deliverable data product, a separate DID shall be selected or prepared for each.

Do's and Don'ts

- DIDs shall not contain requirements to perform work tasks (i.e., inspection or test) or otherwise direct or constrain the data preparation activity – these are in the SOW.
- DIDs shall be structured to facilitate tailoring (deletion) of requirements.
- Prohibited terms: “unless otherwise specified in the contract,” “the contractor shall,” “shall include as a minimum,” and others.

- Data Item Descriptions (DIDs) are available on ASSIST, <http://quicksearch.dla.mil/>
- The DID is used to describe the SOW-required data format and content
- The SOW, and not the DID, must task the contractor to perform work
- For certain elements of data that are not needed, the CRDL should provide directions to tailor the DID requirement appropriately, noting deletions in CDRL Block 16



Example of DoD Standard for a Data Item Description: Program Protection Implementation Plan

DATA ITEM DESCRIPTION
 Title: F/A-18 and EA-18 AIRCRAFT / SYSTEM PROGRAM PROTECTION IMPLEMENTATION PLAN

Number: DI-MGMT-81826D
 AMSC Number: N9951
 DTIC Applicable: N/A

Approval Date: 20180612
 Limitation: N/A
 GIDEP Applicable: Yes
<http://www.giddep.org/data/submittal.htm>
 Project Number: MGMT-2018-035

Preparing Activity: AS
 Applicable Form: N/A

Use/relationship: The Contractor F/A-18 (All Series) and EA-18G Program Protection Implementation Plan (PPIP) shall be defined within the F/A-18 (All Series) and EA-18 Aircraft / System Contractors Program Protection Implementation Plan (PPIP) which is a result of the program protection requirements set forth in the DD-254, Statement of Work (SOW), DoD Contract, the Government's F/A-18 and EA-18G Program Protection Plan (PPP) (including Addendums) most current issuance, the Security Guidance for F/A-18 Hornet (All Series) and the EA-18G Growler Aircraft / Systems and Security Classification Guides, applicable for the F/A-18 (All Series) and EA-18G Aircraft / Systems.

This Data Item Description (DID) contains the format, content, and intended information for the data product resulting from the work task described in the contract SOW.

This DID DI-MGMT-81826D cancels and replaces DI-MGMT-81826C.

Requirements:

- Reference documents.** The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions, shall be as specified in the contract. Note: For PPIP Reference Documents see Paragraph 4 and its subparagraphs.
- Format.** The required document shall be in Contractor format.
 - The PPIP shall be used as the Contractor Program Security. The PPIP is derived from the PPP and should not restate what is written in the PPP but simply state "how" the contractor will implement Program Protection.
 - The PPIP is used to identify and monitor how a Contractor develops and performs Program Protection / Operations Security (OPSEC) activities during performance of the contract.
- Content.** The Contractor's PPIP shall contain the following:
 - Delivered document at a minimum shall include a cover page identifying the Subject, Contractors Name and Address, Contract number, DID identification, Distribution Statement, Export Control, and Destruction Notice.
 - Security Management organization.
 - The Contractor's Program Security / OPSEC Management structure, including relationships with the corporate hierarchy, program subcontractors and suppliers.
 - A section detailing the Contractor's approach to the PPIP.
 - General methodologies that will be applied to protection requirements.
 - Critical Program Information including the following: Critical Components (CC), Critical Program Information (CPI), Critical Systems (CS), and Critical Technologies (CT), hereafter referred to as CPI.
 - The Contractor's process for identifying any existing / proposed CPI during development and RDT&E phases, and its protection / identification in the ECP process prior to ECP acceptance by the Government.

DI-MGMT-81816D

Scope: The Contractors F/A-18 (All Series) and EA-18G Program Protection Implementation shall be defined within the F/A-18 (All Series) and EA-18 Aircraft / System Contractors PPIP which is a result of the program protection requirements set forth in the DD-254, Statement of Work (SOW), DoD Contract, ...

DATA ITEM DESCRIPTION
 Title: Naval Aviation Program Protection Implementation Plan

Number: DI-MGMT-82144
 AMSC Number: N99843
 DTIC Applicable: N/A
 Preparing Activity: AS
 Applicable Form: N/A

Approval Date: 20170726
 Limitation: N/A
 GIDEP Applicable: N/A
 Project Number: MGMT-2017-043

Use/relationship: This report is meant to be used in identification of the approach to implementing the Program Protection Plan (PPP). The Program Protection Implementation Plan (PPIP) is derived from the PPP and will not restate what is written in the PPP.

This DID contains the format, content, and intended use information for the data product resulting from the work task.

Requirements:

- Referenced Documents: The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions, shall be as specified in the contract.
- Format: Contractor format is acceptable.
- Content: The Contractor's PPIP will contain the following:
 - A section detailing the Contractor's approach to implementing the PPP.
 - General methodologies that will be applied to protection requirements.
 - Critical Program Information (Critical Components (CC), Critical Program Information (CPI) / Critical Systems (CS) / Critical Technologies, (CT) hereafter identified as CPI.
 - The Contractor's process for identifying any existing / proposed CPI during development and RDT&E phases, and its protection / identification in the ECP process prior to ECP acceptance by the Government.
 - A section describing an effective and efficient protection of CPI, which will include the following:
 - The Contractor's Program Security / OPSEC Management structure, including relationships with the corporate hierarchy and program subcontractors and suppliers.
 - An overview of all Contractor's activities, operations, tests, and other associated activities to be undertaken in performance of the contract, identifying those in which CPI could manifest itself, and when the CPI is embodied in the hardware.

DI-MGMT-82144

Scope: This report is meant to be used in identification of the approach to implementing the Program Protection Plan (PPP). The Program Protection Implementation Plan (PPIP) is derived from the PPP and will not restate what is written in the PPP.

DATA ITEM DESCRIPTION

Public reporting burden for this collection of information is estimated to average 10 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Service, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0707-0188), Washington, DC 20503.

1. TITLE: Program Protection Implementation Plan (PPIP)

2. IDENTIFICATION NUMBER: DI-ADMIN-81306

3. DESCRIPTION/PURPOSE: 3.1 This plan outlines and defines the contractor's implementation of the Government developed Program Protection Plan (PPP). The PPIP is the principal communications means for validation and approval by the DoD or Component Program Manager of the specific methods used by the contractor to (1) identify the means chosen to implement the PPP at contractor, sub-contractor, vendor controlled locations and (2) provide protection inputs to the system acquisition process. (Continued on Page 2)

4. APPROVAL DATE (FORMS): 930125

5. OFFICE OF PRIMARY RESPONSIBILITY (OPR): CASD/CPI/CI4SCH (ASFO)

6a. DTIC APPLICABLE: N/A

6b. GIDEP APPLICABLE: N/A

7. APPLICATION/INTERRELATIONSHIP: 7.1 This DID contains the format and content preparation instructions for the Program Protection Implementation Plan (PPIP) resulting from the program protection requirements set forth in DODI 5000.2, Part 5, Section F, "Program Protection Planning and Technology Controls". 7.2 This DID is applicable to all DoD acquisition programs regulated by DODD 5000.1, DODI 5000.2, and DoB 3000.2-M. 7.3 It is intended that all requirements contained (Continued on Page 2)

8. APPROVAL LIMITATION: N/A

9a. APPLICABLE FORMS: N/A

9b. AMSC NUMBER: D6821

10.1 Content Requirements: The PPIP shall include the following:

- A section detailing the overall approach to the PPIP and the general methodologies which will be applied to the protection requirements indicated in the PPP.
- A section(s) describing fully the activities and methodologies planned to satisfy the PPIP requirements and justification as to why these specific activities were chosen. Narratives, charts, diagrams, or matrices shall be used to illustrate the methodology(ies) chosen to establish effective and efficient countermeasures to program specific vulnerability(ies). Explain these planned actions through all applicable milestones, at all contractor, sub-contractor or vendor controlled locations where the identified vulnerability(ies) exist.
- A list of documents which applies as directive or guidance during execution of the PPIP. This list shall include pertinent legal, regulatory and other published or draft protection requirements applicable to the system under development. Program protection requirements and objectives shall be drawn from these documents. (Continued on Page 2)

11. DISTRIBUTION STATEMENT: **DI-ADMIN-81306**

DD Form 1644, FEB 73

Source: <https://ascd.dia.mil/> - Downloaded: 2018-09-29T10:56Z
 Check the source to verify that this is the current version before use.

Scope: This plan outlines and defines the contractor's implementation of the Government developed Program Protection Plan (PPP). The PPIP is the principal communications...

Content and format requirements for data deliverables



Industry Impacts

- Differences in Services' approaches are reflected in Solicitations and Contracts
 - Air Force: Program Protection activities (Hardware Assurance, Software Assurance)
 - Navy: IT Cybersecurity
 - Army: Program Protection, Cyber Network Defense

APPROVED FOR PUBLIC RELEASE

Raytheon

A Look At Current State Proposal Requirements

Defense Platform/Embedded Program RFP Analysis

The analysis included 10 RFPs in 2016.

The following keywords were used to extract sections of the RFP Statement of Work and Sections L and M language.

Customers included:

- (3) Air Force (1) United States; (1) direct commercial sale, (1) Foreign Military Sale
- (4) Navy (2) United States; (2) direct commercial sale
- (3) Army (3) United States

KEYWORDS USED:
cyber
cyber security
cybersecurity
cyber hardening
cyber defense
cyber protection
information assurance
IA
program protection
system security
security assessment
risk management framework
RMF
vulnerability analysis
survivability
resiliency
DIACAP
INFOSEC

4/25/2017 | 5

Approved for Public Release
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

APPROVED FOR PUBLIC RELEASE

Raytheon

RFP SOW Analysis Results Summary

Request for Proposal, Statement of Work (SOW) Analysis Results Summary

Program Protection	CYBER RESILIENCY AND SECURE SYSTEMS RELEVANT REQUIREMENTS – HOLISTIC PROGRAM PROTECTION									
	Navy #1	Navy #2	Army #1	Army #2	Army #3	AirForce #1	AirForce #2	Navy #3	International Customer #1	International
• Program Protection Plan (PPP) development and implementation	x	x	x	x	x	x	x	x	x	x
• Systems security Architecture	Cybersecurity Plan	DFARS CCI	PPP	Cybersecurity	Cybersecurity	Program Protection Plan	References System Security but really cybersecurity	Cyber resiliency (not specific words)	Resiliency	Cyber resiliency
• Software assurance			Critical Functional Analysis	PPP	Anti-tamper	Cyber Resilient Architecture	PPP	cybersecurity	System Security Architecture	Cyber security system
• Secure coding			Cybersecurity	SwA	Defense Exportability Features	Cybersecurity	Validation Plans		Security Management Plan (Emphasis on cybersecurity)	
• Information Assurance (IA)			System Security Plan	Key Management		Software Assurance			Lifecycle considerations for security	
• Cyber hardening						Anti-tamper			Computer Network Defense	
• Computer Network Defense (CND)										
• Embedded system security						SCRM (Trusted Access Program Office, TAPCO)			Cyber Hardening	
						Validation & Verification			Information Assurance	

FY16 Sample Set RFP Requirements for Cybersecurity

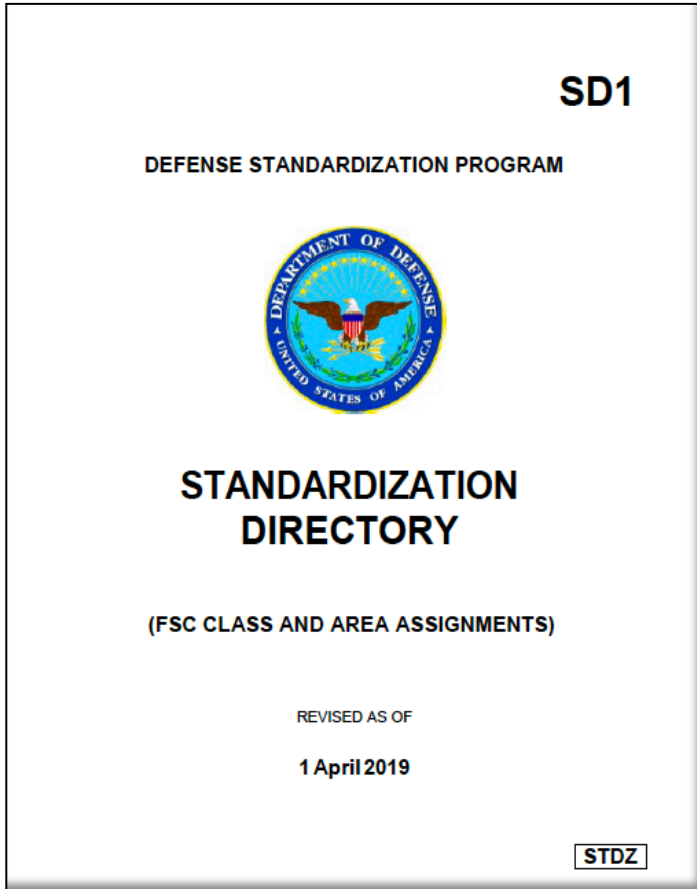
Distribution Statement A: Approved for public release. Distribution is unlimited.

Distrib

ited.



Secure Cyber Resilience Engineering (SCRE) Standardization Area



■ SCRE Definition

- This 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.
- This AREA 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 Established Secure Cyber Resilient Engineering Standardization Area in March 2019



Secure Cyber Resilient Engineering Standardization Objectives

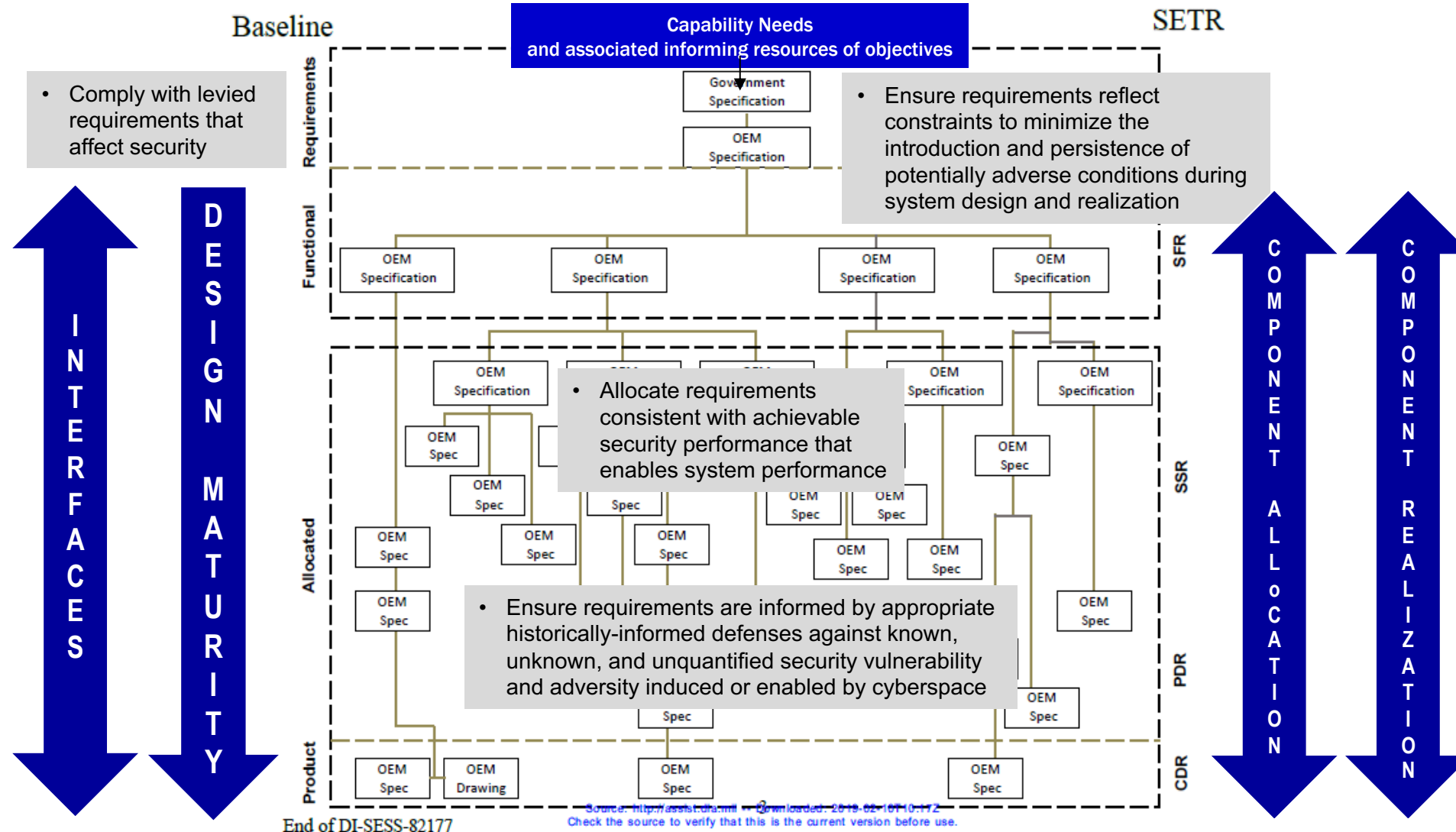


- **Improve the efficiency and effectiveness of weapon systems engineering practice**
- **Increase consistency and repeatability of resilient engineering methods and standards**
- **Improve the communication between government, industry, and operational stakeholders**



Security Requirements Derivation Consistent with DI-SESS-82177

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



End of DI-SESS-82177


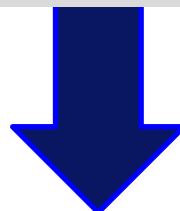
Source: <http://assist.dau.mil> - Downloaded: 2019-02-10 10:17Z
Check the source to verify that this is the current version before use.



Strategy for Standardization

E
S
T
A
B
L
I
S
H
M
E
N
T

- **Develop Framework that defines the scope and focus**
 - Develop “Tree of Data”
 - Identify and describe representative categories/classes/topics/tasks
 - Framework based on Program Protection and Engineering Cyber activities
- **Identify existing security and protection standards**
 - Identify required security and protection standards, handbooks, guidance, documents, and DIDs
- **Conduct gap analysis**
 - Identify set of existing standards that would reside in the new Area
 - Identify courses of actions for relevant standards
- **Develop Recommendations and coordinate with DoD Components**
- **Manage and maintain**
 - Ongoing revision, introduction of new, retirement of no longer used
 - Influence future standards


 Leverage ongoing OUSD(R&E) efforts and other standardization AREAs to inform the identification and elaboration of engineering security activities, methods, data, artifacts, and lexicon


Steady State



Next Steps

- **Develop SCRE “Tree” of Data**
 - Data drives execution and judgements of suitability
- **Conduct gap analysis of active Handbooks, Standards, and Data Items**
 - Remove duplication and conflict
- **Work with Service Leads to assess cyber and PPP-related standards, including data item descriptions, and recommend where updates may be appropriate**



Summary

- **Standardization of systems engineering approaches, methods, and data is necessary to improve efficiency and effectiveness to respond to concerns presented by cyberspace**
 - Cyber resilience
 - Cyber security
 - Cyber survivability
- **Standardization should be principle-based to enable tailoring to:**
 - Meet capability, performance, and loss considerations relative to operational doctrine for use of the system and acquisition model
 - Mature requirements, expertise, and tools to achieve engineering cyber, resilience, and survivability objectives
- **Opportunities for government, industry and academia to engage**
 - Inform processes and technical requirements standards for engineering cyber resilient weapon systems



<https://www.cto.mil>

Questions?

Follow us @DoDCTO





For Additional Information

Ms. Melinda Reed

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

571.372.6562 | melinda.k.reed4.civ@mail.mil

Mr. Michael McEvilley

Contractor Support Team, MITRE Corporation

703.472.5409 | mcevilley@mitre.org



BACK UP



Approach to Acquire Data Deliverables

Example of requesting delivery of the Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information

Data Item Description (DID) provides the format and content requirements for data item, with non-essential references tailored out of the DID. (e.g. DI-SCRE-82258, "Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information")

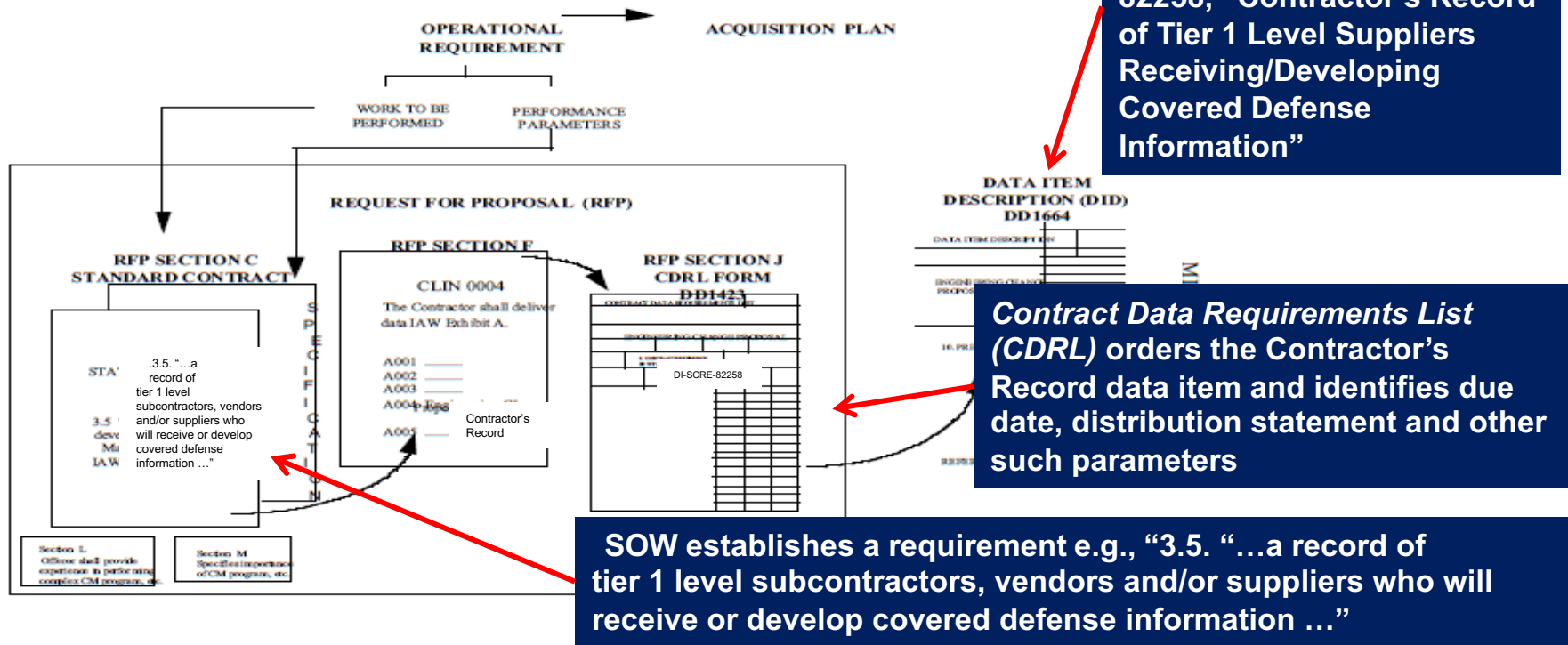
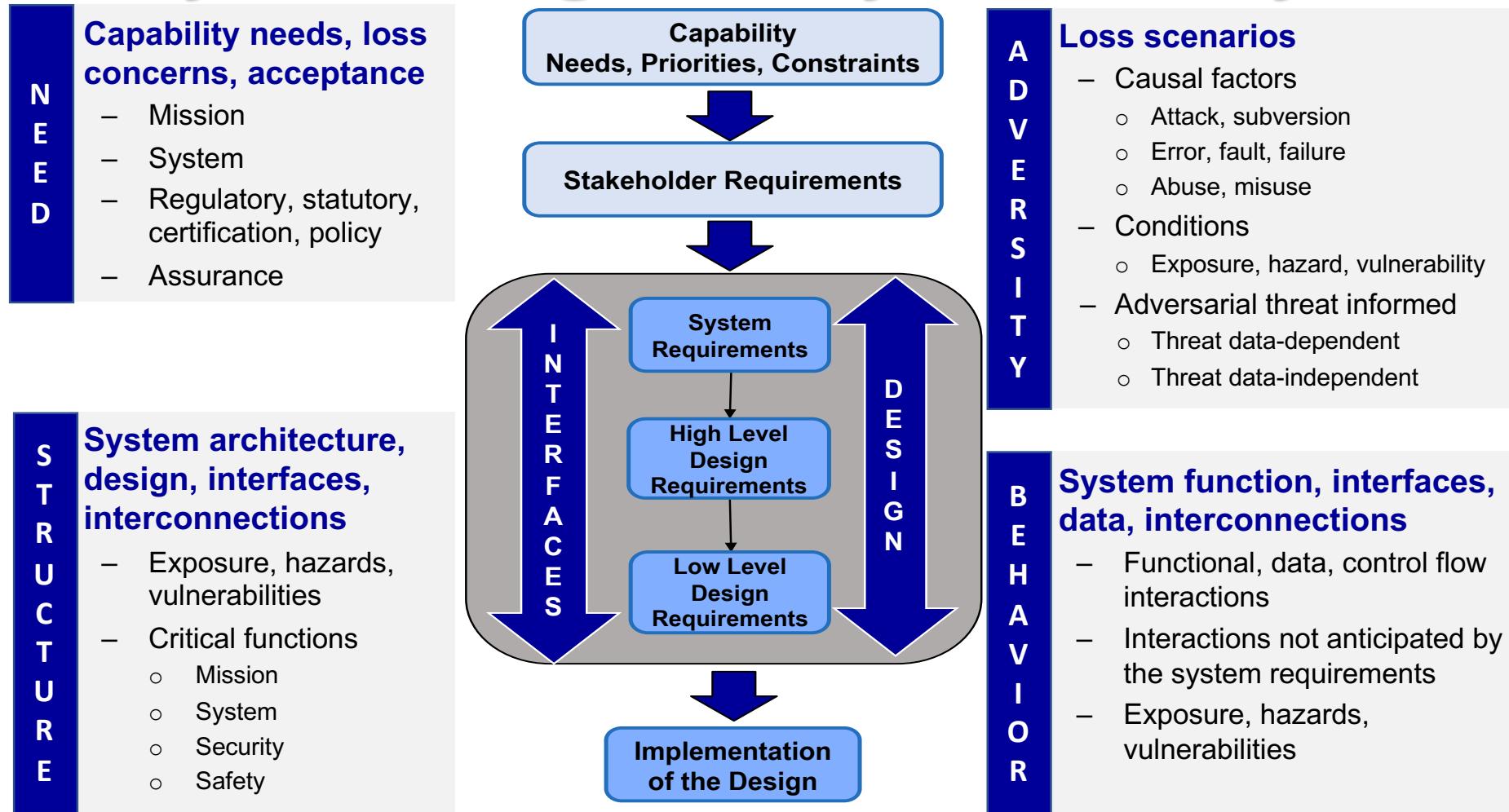


FIGURE 5. SPEC-SOW-CDRL-DID Relationship.



Requirements Derivation, System Design, and Systems Analysis



Applied with rigor necessary to achieve the targeted level of confidence



Contract Data Requirements List (CDRL) – Form DD1423

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)				Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.					
A. CONTRACT LINE ITEM NO. 0065		B. EXHIBIT A		C. CATEGORY TCP ___ TM ___ OTHER <input checked="" type="checkbox"/> ADMN	
D. SYSTEM/ITEM Electronic Warfare Systems		E. CONTRACT/PR NO. N50024-18-R-8200		F. CONTRACTOR Contractor TBD	
1. DATA ITEM NO. A036	2. TITLE OF DATA ITEM Program Protection Implementation Plan (PPIP)		3. SUBTITLE		
4. AUTHORITY (Data Acquisition Document No.) DI-ADMIN-81360		5. CONTRACT REFERENCE SOW Para 3.3.1.1		6. REQUIRING OFFICE NAVSEA PMS435	
7. DD 250 REQ LT	9. DIST STATEMENT REQUIRED D	10. FREQUENCY SEE BLK 10 N/A	11. AS OF DATE N/A	12. DATE OF FIRST SUBMISSION SEE BLK 10	13. DATE OF SUBSEQUENT SUBMISSION SEE BLK 10
8. APP CODE A	14. DISTRIBUTION	a. ADDRESSEE	b. COPIES		
			Draft	Final	
			Req	Repr	
16. REMARKS					
BLOCK 8: Review will be for technical content. The Government will review and comment within 30 calendar days. Resubmittal is due 15 calendar days after receipt of Government review comments.					
BLOCK 9: DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. DoD contractors only. Critical Technology: (insert date). Other requests for this document shall be referred to PEO SUB (PMS435).					
BLOCKS 10, 12 AND 13: Submission shall be delivered 30 calendar days after completion of work as specified in the IMS or individual TI.					
BLOCK 14: Unclassified Data Item shall be submitted electronically by uploading to the PMS435 site on the Integrated Product Data Management (IPDM) System. Electronic notification that the Data Item has been uploaded shall be sent to the distribution list. If CDRL contains classified data, contact COR for direction on delivery.					
		PMS435	1	1	
		NWVC NPT	1	1	
		PCO	1	1	
		DCMA	1	1	

Block 2. Identifies the Title of Data Deliverable –

Program Protection Implementation Plan

Block 4. Identifies the Data Item Description –
DI-ADMIN-81360
Program Protection Implementation Plan

Block 9. For technical information, specify requirement for contractor to mark the appropriate distribution statement on the data (ref. DoDI 5230.24); information is controlled when distribution statement is B-F

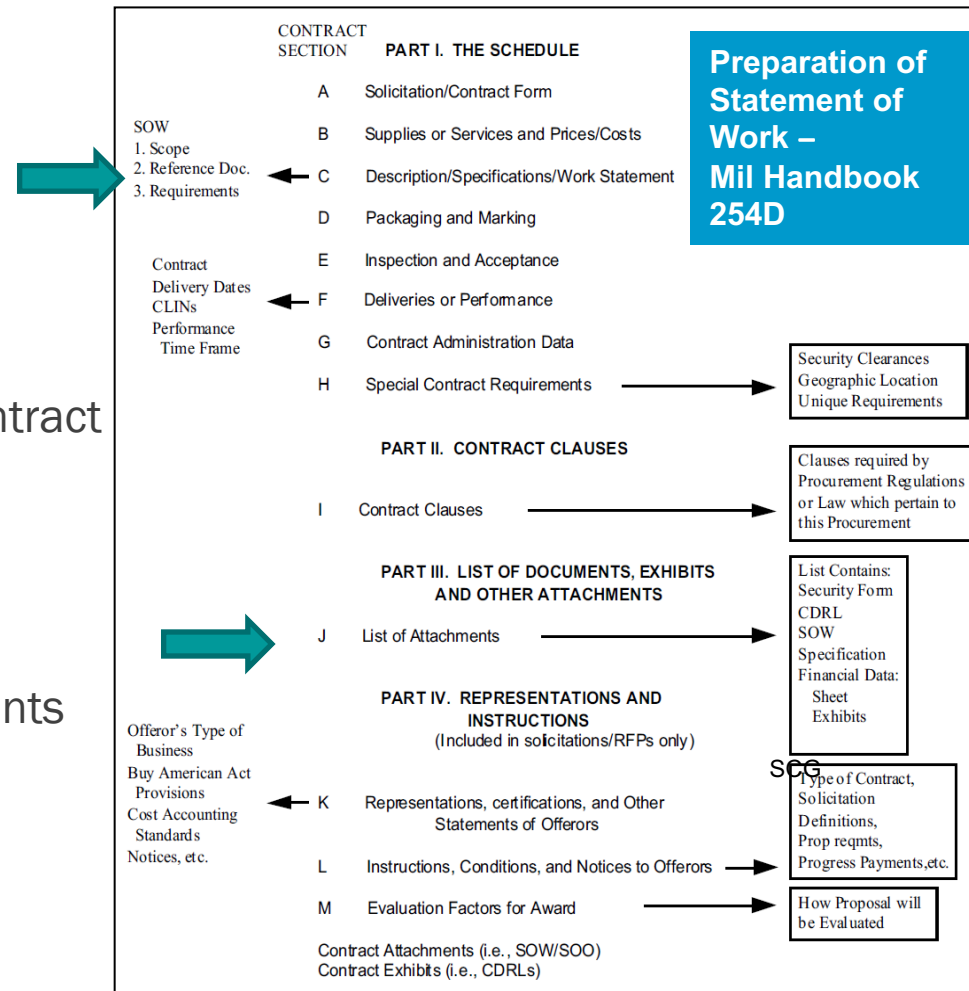
Block 16. Includes additional clarification and the Marking Statement the contractor is to mark the deliverable

Includes Data Item Description for content of the deliverable, and Technical Information Marking and Dissemination Statements



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



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



Standardization Areas with Relevant Data Item Descriptions

Area	Title	LSA	% *
MGMT	Management	EA for DSP	35%
IPSC	Information Processing Stds. for Computers	DISA	16%
MISC	Miscellaneous	EA for DSP	13%
EMCS	Electromagnetic Compatibility Stds.	DISA	11%
SESS	Systems Engineering Specs. and Stds.	ODASD(SE)	11%
QCIC	Quality Control/Assurance and Inspection	ARDEC, Armament Research Devlp & Engr Center	8%
NUOR	Nuclear Ordnance	DTRA	6%

Quick look identified 179 Relevant DIDs found in 23 of 39 Standardization Areas



Initial SCRE Framework

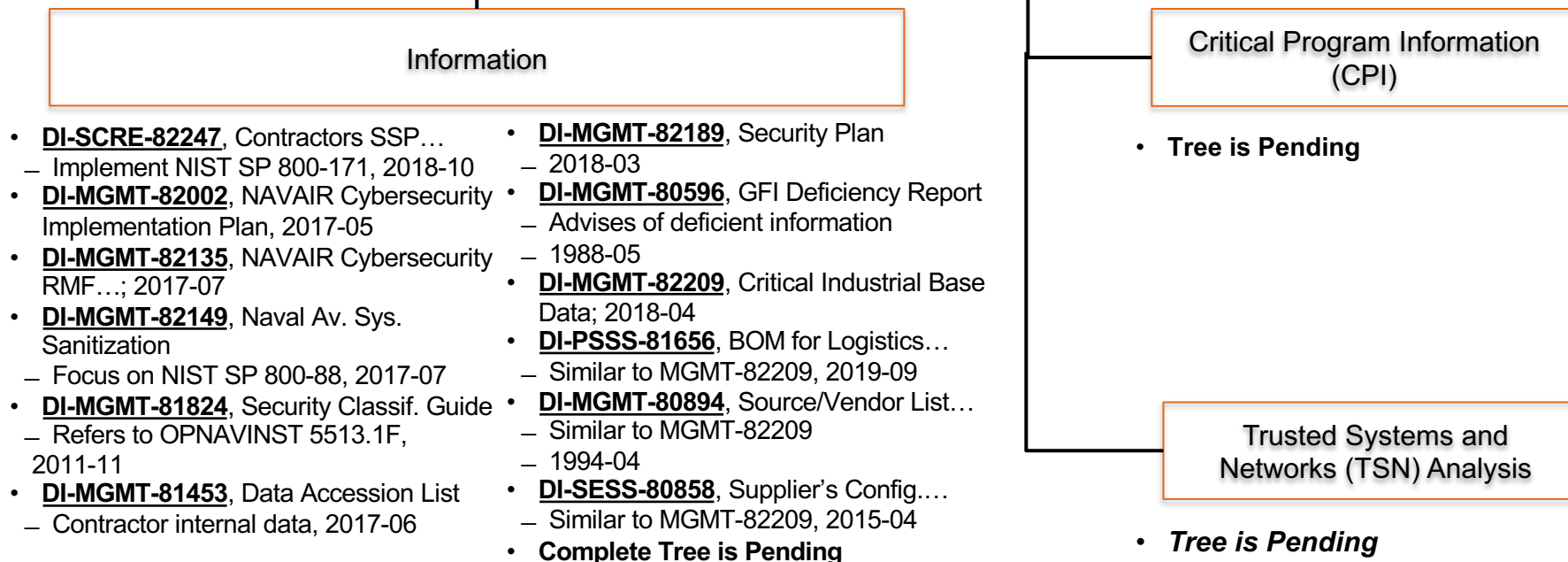
**Next Step:
Establish SCRE “Tree of Data”
to identify relevant Standards
and DIDs with goal to
standardize direction to
industry in contracting**

Program Protection Plan

- **DI-MGMT-81826D**, F/A-18 and EA-18 Aircraft / System Program Protection Implem. Plan
 - 2018-06
- **DI-MGMT-82144**, Naval Aviation PPIP
 - 2017-07
- **DI-ADMIN-81306**, PPIP
 - 1993-01

SCRE LSA responsibility includes

- The maintenance of the SCRE framework and the identification of the relevant artifacts
- The maintenance of artifacts that reside in SCRE
- Trace to other LSAs responsible for the artifacts identified by SCRE but not contained in SCRE





Aligns with Other Standardization Areas

■ System Safety (SAFT)

- This AREA covers the systems engineering integration of life cycle environment, safety, and occupation health (ESOH) considerations in the design, test, demonstration, operations, maintenance, sustainment, and disposal of military systems.

■ Systems Engineering Specifications and Standards (SESS)

- This AREA covers standards, specifications, methods, practices, techniques, and data requirements for analyzing, developing, and defining the technical engineering requirements for new and modified DOD systems.
- This AREA specifically encompasses procedural guidance to address those systems engineering elements executed throughout the acquisition process, which includes configuration management of the technical baseline information, data management, reliability, maintainability, manufacturing producibility, and design, development, and test activities. This AREA does not include Human Factors, Environmental, Product Support, Quality Control, Cybersecurity, or Systems Safety.

■ Secure Cyber Resilient Engineering (SCRE)

- This 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.
- This AREA 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.