Standardization for the Engineering of Secure Cyber Resilient Weapons Systems

Ms. Melinda Reed

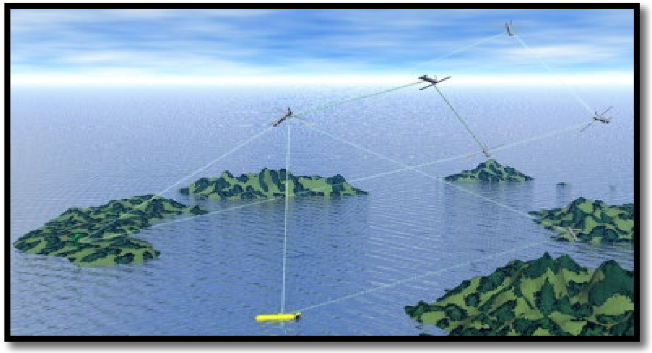
Director, Resilient Systems
Strategic Technology Protection & Exploitation
Office of the Under Secretary of Defense
for Research and Engineering

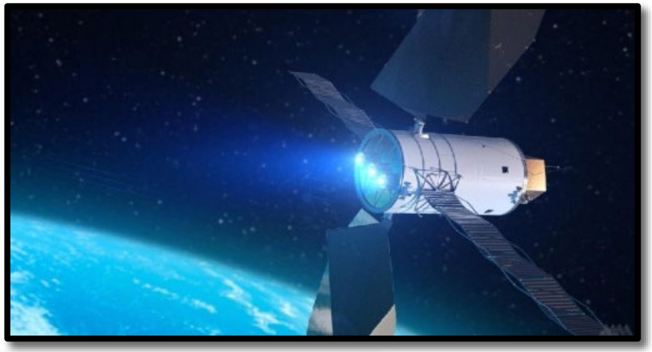
Defense Standardization Council
October 14, 2020

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

- **Ensure Technological Superiority for the U.S. Military**
  - Set the technical direction for the Department of Defense (DoD)
  - Champion and pursue new capabilities, concepts, and prototyping activities throughout DoD research and development enterprise

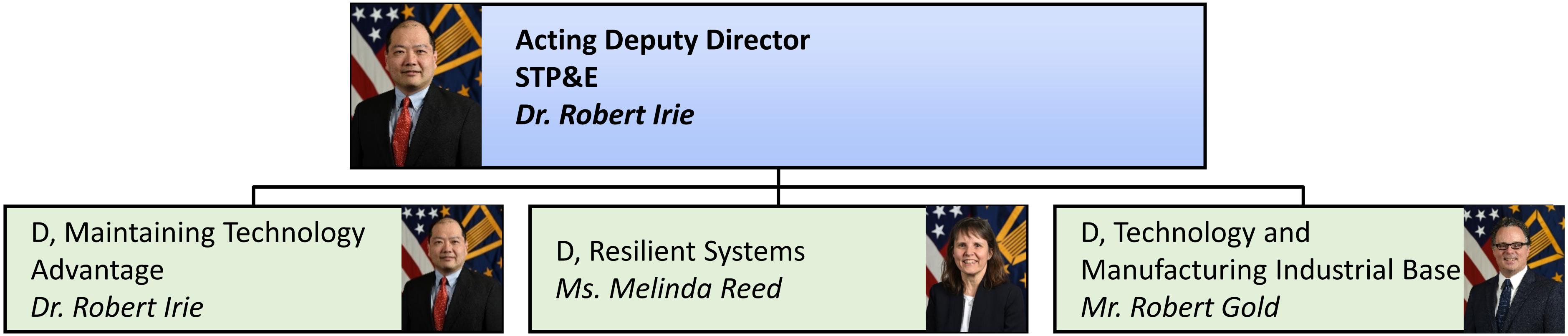
- **Bolster Modernization**
  - Pilot new acquisition pathways and concepts of operation
  - Accelerate capabilities to the Warfighter





Distribution Statement A: Approved for public release. DOPSR case #20-S-2038 applies. Distribution is unlimited.

Strategic Technology Protection & Exploitation (STP&E) Organization and Mission



Acting Deputy Director
STP&E
Dr. Robert Irie

D, Maintaining Technology Advantage
Dr. Robert Irie

Maintain Leadership in Critical Technology Modernization Areas

D, Resilient Systems
Ms. Melinda Reed

Foster Assured Resilient Missions, Systems and Components

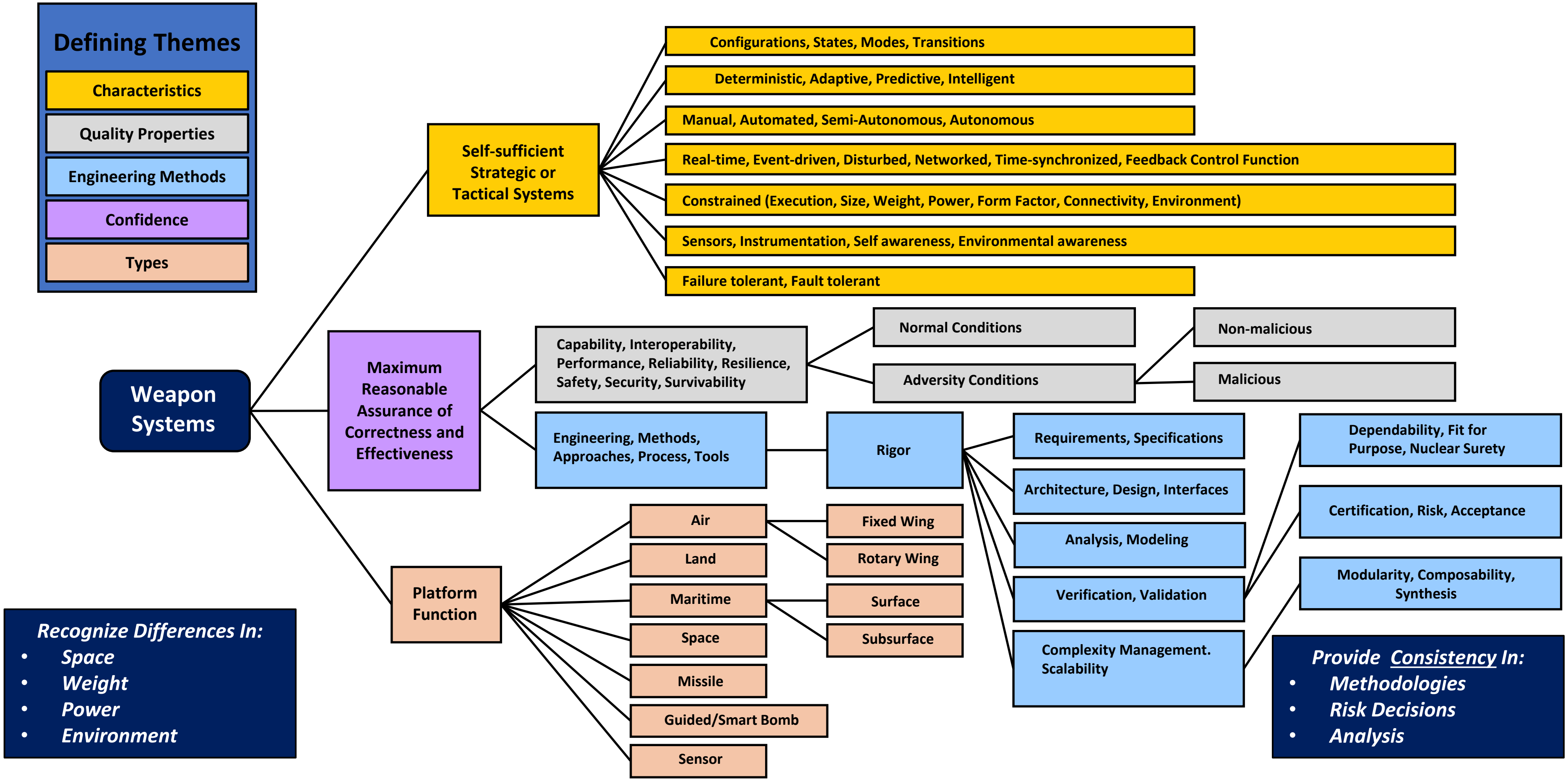
D, Technology and Manufacturing Industrial Base
Mr. Robert Gold

Advance Domestic Innovation Base to Deliver Modernization Goals

STP&E MISSION:

Promote and protect technology advantage and counter unwanted technology transfer to ensure Warfighter dominance through superior, assured, and resilient systems, and a healthy, viable national security innovation base.

Background: Weapon Systems Characteristics



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, Disturbed, 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, Process, Tools
  - Rigor
    - Requirements, Specifications
    - Architecture, Design, Interfaces
    - Analysis, Modeling
    - Verification, Validation
    - Complexity Management. Scalability
      - Dependability, Fit for Purpose, Nuclear Surety
      - Certification, Risk, Acceptance
      - 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*

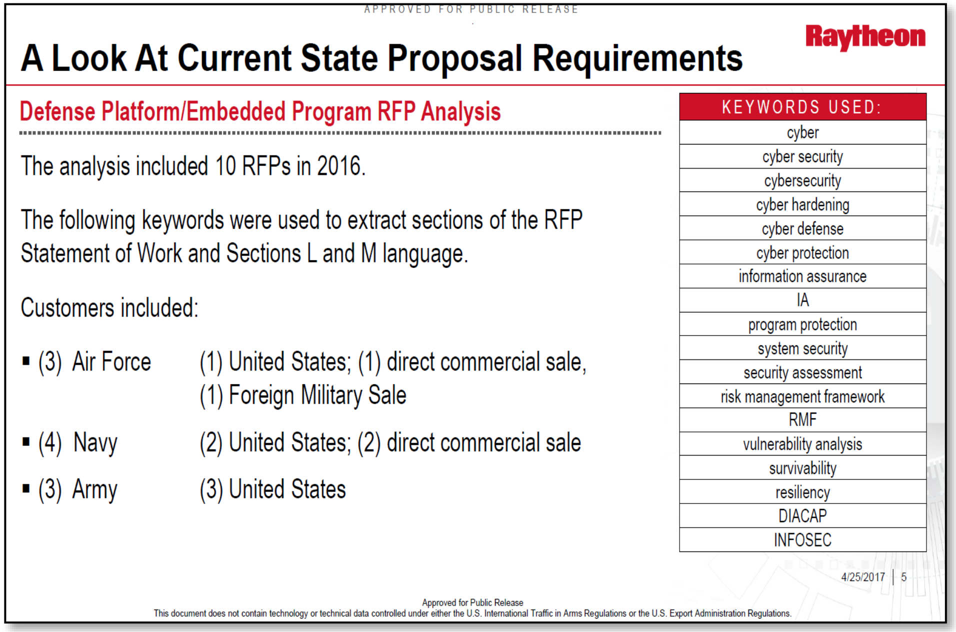
Provide Consistency In:

- *Methodologies*
- *Risk Decisions*
- *Analysis*

Weapon Systems Deliver Lethal Force with the Intent to Cause Harm

Background: Industry Observations

- **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

A Look At Current State Proposal Requirements

Raytheon

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.

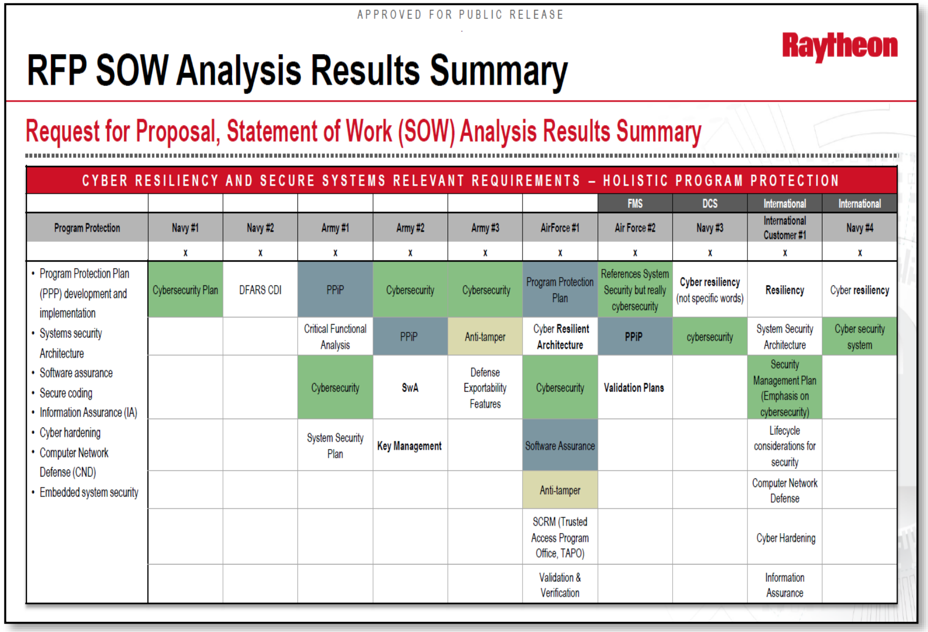
Customers included:

▪ (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

RFP SOW Analysis Results Summary

Raytheon

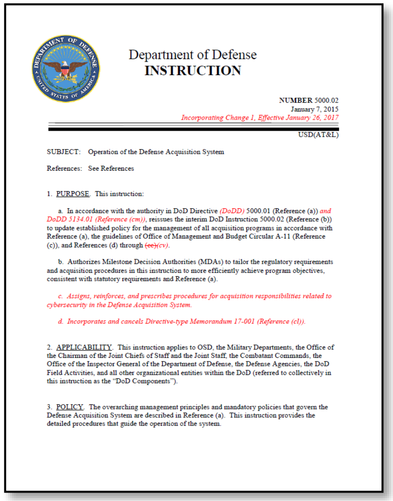
Request for Proposal, Statement of Work (SOW) Analysis Results Summary

CYBER RESILIENCY AND SECURE SYSTEMS RELEVANT REQUIREMENTS – HOLISTIC PROGRAM PROTECTION

							FMS	DCS	International	International
Program Protection	Navy #1	Navy #2	Army #1	Army #2	Army #3	AirForce #1	Air Force #2	Navy #3	International Customer #1	Navy #4
	x	x	x	x	x	x	x	x	x	x
• Program Protection Plan (PPP) development and implementation • Systems security Architecture • Software assurance • Secure coding • Information Assurance (IA) • Cyber hardening • Computer Network Defense (CND) • Embedded system security	Cybersecurity Plan	DFARS CDI	PPiP	Cybersecurity	Cybersecurity	Program Protection Plan	References System Security but really cybersecurity	**Cyber resiliency** (not specific words)	**Resiliency**	Cyber **resiliency**
			Critical Functional Analysis	PPiP	Anti-tamper	Cyber **Resilient Architecture**	**PPiP**	cybersecurity	System Security Architecture	Cyber security system
			Cybersecurity	**SwA**	Defense Exportability Features	Cybersecurity	**Validation Plans**		Security Management Plan (Emphasis on cybersecurity)	
			System Security Plan	**Key Management**		Software Assurance			Lifecycle considerations for security	
						Anti-tamper			Computer Network Defense	
						SCRM (Trusted Access Program Office, TAPO)			Cyber Hardening	
						Validation & Verification			Information Assurance	

FY16 Sample Set Request for Proposal (RFP) Requirements for Cybersecurity

Background: DoD Acquisition Policy



Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
Incorporating Change 1, Effective January 26, 2017

USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive *(DoDD)* 5000.01 (Reference (a)) *and DoDD 5134.01 (Reference (cm))*, reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through ~~(cc)~~*(cv)*.

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

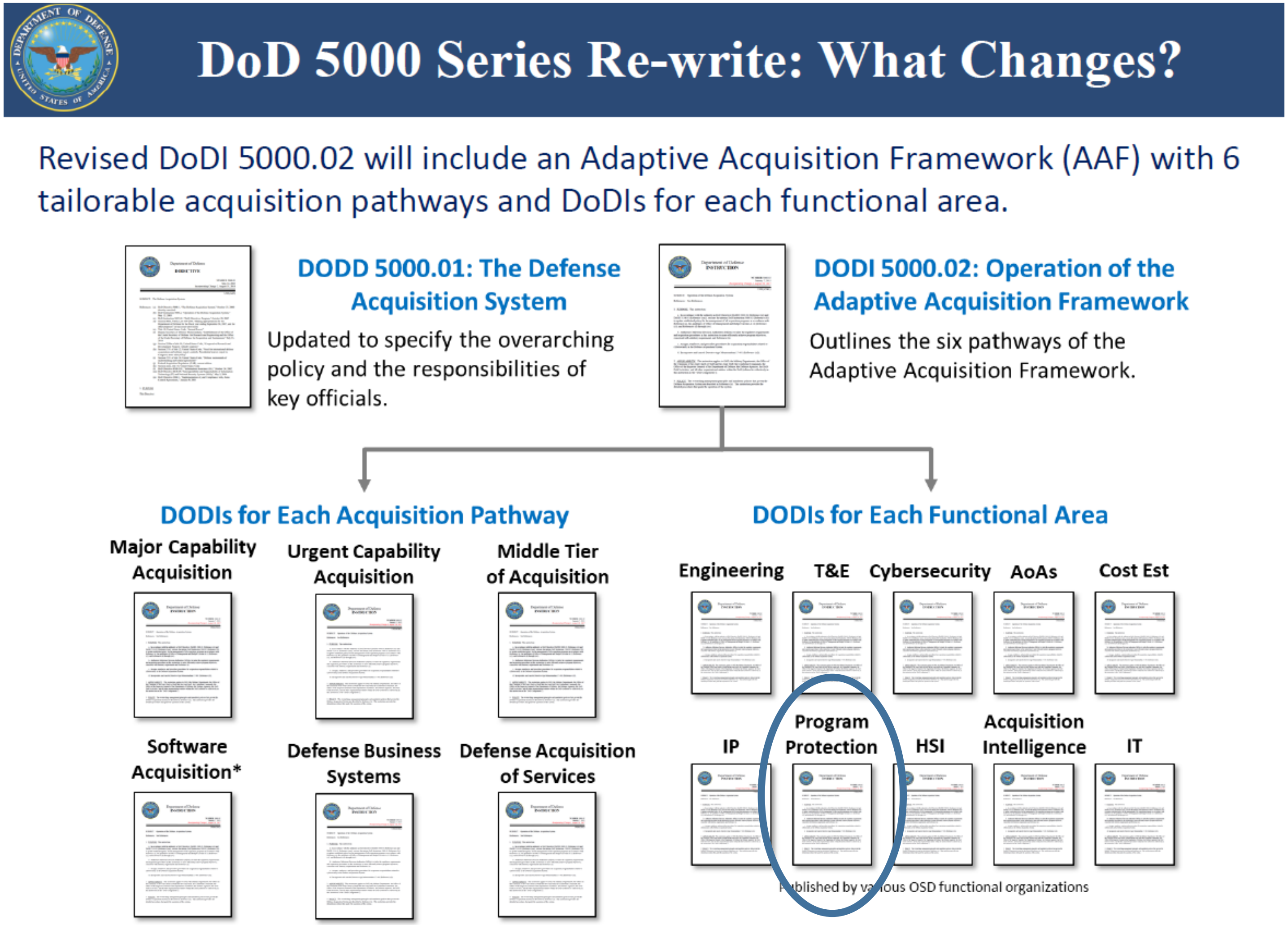
c. Assigns, reinforces, and prescribes procedures for acquisition responsibilities related to cybersecurity in the Defense Acquisition System.

d. Incorporates and cancels Directive-type Memorandum 17-001 (Reference (cl)).

2. APPLICABILITY. This instruction applies to 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 instruction as the "DoD Components").

3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

DoD 5000.02 2017



DoD 5000 Series Re-write: What Changes?

Revised DoDI 5000.02 will include an Adaptive Acquisition Framework (AAF) with 6 tailorable acquisition pathways and DoDIs for each functional area.

DODD 5000.01: The Defense Acquisition System

Updated to specify the overarching policy and the responsibilities of key officials.

DODI 5000.02: Operation of the Adaptive Acquisition Framework

Outlines the six pathways of the Adaptive Acquisition Framework.

DODIs for Each Acquisition Pathway

Major Capability Acquisition
Urgent Capability Acquisition
Middle Tier of Acquisition
Software Acquisition*
Defense Business Systems
Defense Acquisition of Services

* Interim

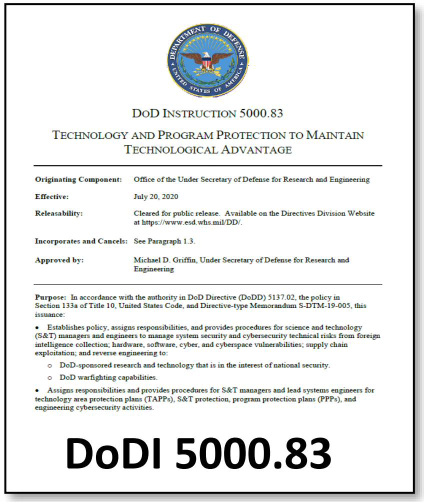
DODIs for Each Functional Area

Published by various OSD functional organizations

*https://www.acq.osd.mil/ae/assets/docs/Transforming%20Defense%20Acq%20Policy%20(15Jan2020).pdf

Distribution Statement A: Approved for public release. DOPSR case #20-S-2038 applies. Distribution is unlimited.

Technology and Program Protection to Maintain Technological Advantage



DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	July 20, 2020
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

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum S-DTM-19-005, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

DoDI 5000.83

- Establishes policy, assigns responsibilities, and provides procedures for DoD S&T managers and engineers to mitigate risks and protect critical U.S. research, military technologies, and programs
- Contributes to a National Defense Strategy (NDS) line of effort (increasing lethality) through promotion and implementation of enhanced technology protection across the DoD enterprise
- The Department of Defense Instruction (DoDI) recommends activities for DoD S&T managers and engineers to mitigate threats to U.S. technology and programs, including:

- ▪ Safeguarding classified and unclassified Controlled Technical Information
- ▪ Supervising DoD-sponsored research involving joint ventures, academic collaborations, and cooperative research partnerships
- ▪ Designing systems for security and cyber resiliency
- ▪ Protecting against cyberattacks
- ▪ Protecting fielded systems from changing threat environments
- ▪ Enhancing protection for critical programs and technologies through Technology Area Protection Plans (TAPPs), S&T protection plans, and Program Protection Plans (PPPs)

- Released 20 July 2020; available on https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf?ver=2020-07-20-150345-930/

DoDI 5000.83 Activities

1. **GENERAL ISSUANCE INFORMATION**

2. **RESPONSIBILITIES**

   USD(R&E), USD(A&S), USD(I&S), DoD CIO, USD(P), DoD Component Heads

3. **PROCEDURES**

   3.1. General

   3.2. TECHNOLOGY AND PROGRAM PROTECTION

   a. Adversary Impact on Technology and Programs
   b. Science and Technology Managers and Lead Systems Engineers Responsibilities

   3.3. ACTIVITIES TO MITIGATE ADVERSARY THREATS TO TECHNOLOGY AND PROGRAMS

   a. Safeguard Information
   b. Control DoD-sponsored Research
   c. Design for Security and Cyber Resiliency
   d. Protect the System Against Cyber Attacks from Enabling and Supporting Systems
   e. Protect Fielded Systems
   f. Enhanced Protections for Critical Programs and Technologies

3.4 **TECHNOLOGY AND PROGRAM PROTECTION MANAGEMENT**

a. TAPP
b. S&T Protection Plan
c. PPP
d. Independent Technical Risk Assessment
e. System Engineering Plan
f. Test and Evaluation Master Plan
g. Life-cycle Sustainment Plan

3.5 **TAILORED PROGRAM PROTECTION FOR SELECTED ACQUISITION PATHWAYS**

a. Major Capability Acquisition
b. Urgent Operational Needs
c. Operation of the Middle Tier of Acquisition
d. Software Acquisition

S&T manager and engineering activities are informed by:

- **Intelligence, counterintelligence and security activities**

Distribution Statement A: Approved for public release. DOPSR case #20-S-2038 applies. Distribution is unlimited.

Technology and Program Protection & Cybersecurity Policies and Initiatives

Technology

Key Protection Activities:

- Export Control
- Anti-Tamper
- Defense Exportability Features
- DoD Horizontal Protection Guide
- Acquisition Security Database

Goal: Prevent compromise or loss of critical technology transfer

- **DoDI 5200.39 Critical Program Information**
- **DoDD 5200.47E Anti-Tamper**
- **DFARS 225.7901 Export-controlled items**

Mission Components

Key Protection Activities:

- Software Assurance
- Hardware Assurance
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center

Goal: Protect mission-critical components (hardware, software) from malicious exploitation

- **DoDI 5200.44 Trusted Systems & Networks**
- **PL 113-66 Sec 937 (FY14 NDAA) JFAC**
- **DFARS 239.73 Requirements for information relating to supply chain risk**
- **NDAA FY11 Sec 806; Requirements for Information Relating to Supply Chain Risk**
- **NDAA FY18 Sec 1659. Supply Chain Risk Management of Critical Missions**
- **NDAA FY20 Sec 224, Trusted Supply Chain Standards**
- **NDAA FY17 Sec 231 DoDI Microelectronics**

Information

Key Protection Activities:

- Classification
- Information Security
- Cybersecurity Protections and Technology Solutions
- Joint Acquisition Protection & Exploitation Cell (JAPEC)
- Damage Assessment Management

Goal: Safeguard system and technical data from adversary collection and disruption

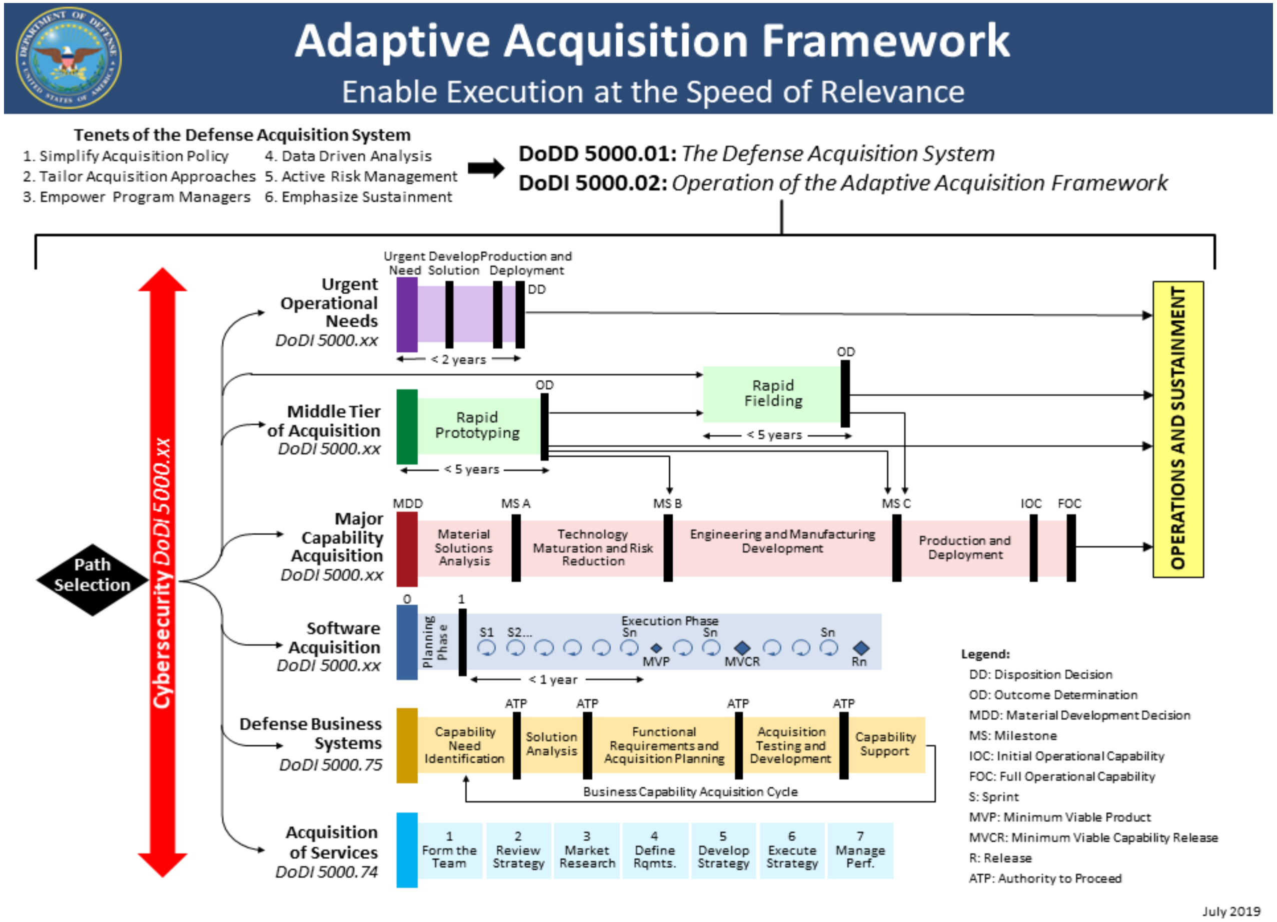
- **DoDI 5230.24 Distribution Statements on Technical Information**
- **DoDI 5200.48 Controlled Unclassified Information**
- **DFARS 252.204-7012 Safeguarding covered defense information and cyber incident reporting (includes requirement to implement NIST SP800-171)**
- **DCMA NIST SP 800-171 Strategic Assessments**
- **32 CFR 2002: Controlled Unclassified Information**

Goal: Ensure Warfighter dominance through superior, assured, and resilient systems

Technology and Program Protection Planning Across the Lifecycle

Technology Modernization Priorities

- 5G Network Technology
- Autonomy
- Biotechnology
- Cyber
- Directed Energy
- Fully Networked Command, Control, and Communications
- Hypersonics
- Machine Learning / Artificial Intelligence
- Microelectronics
- Quantum Science
- Space



Adaptive Acquisition Framework

Enable Execution at the Speed of Relevance

Tenets of the Defense Acquisition System

1. Simplify Acquisition Policy
2. Tailor Acquisition Approaches
3. Empower Program Managers
4. Data Driven Analysis
5. Active Risk Management
6. Emphasize Sustainment

DoDD 5000.01: *The Defense Acquisition System*
DoDI 5000.02: *Operation of the Adaptive Acquisition Framework*

Path Selection
Cybersecurity DoDI 5000.xx
Urgent Operational Needs DoDI 5000.xx
Urgent Need
Develop Solution
Production and Deployment
DD
< 2 years
Middle Tier of Acquisition DoDI 5000.xx
Rapid Prototyping
OD
< 5 years
Rapid Fielding
OD
< 5 years
Major Capability Acquisition DoDI 5000.xx
MDD
MS A
MS B
MS C
IOC
FOC
Material Solutions Analysis
Technology Maturation and Risk Reduction
Engineering and Manufacturing Development
Production and Deployment
Software Acquisition DoDI 5000.xx
0
1
Planning Phase
Execution Phase
S1
S2...
Sn
Sn
Sn
MVP
MVCR
Rn
< 1 year
Defense Business Systems DoDI 5000.75
ATP
ATP
ATP
ATP
Capability Need Identification
Solution Analysis
Functional Requirements and Acquisition Planning
Acquisition Testing and Development
Capability Support
Business Capability Acquisition Cycle
Acquisition of Services DoDI 5000.74
1 Form the Team
2 Review Strategy
3 Market Research
4 Define Rqmts.
5 Develop Strategy
6 Execute Strategy
7 Manage Perf.
OPERATIONS AND SUSTAINMENT

Legend:

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

July 2019

S&T Protection | **Program Protection**

Technology Area Protection Plans for DoD Modernization Priorities

Design for Cyber Threat Environments

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:

- Manages access to, and use of, the system and system resources
- Is structured to protect and preserve system functions or resources, through segmentation, separation, isolation, or partition
- Maintains priority system functions under adverse conditions
- 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
- Monitors, detects, and responds to security anomalies
- Interfaces with the DoD Information Network or other external services

Design Considerations to Mitigate Cybersecurity Implications to the System

System Security Requirements Derivation

NEED

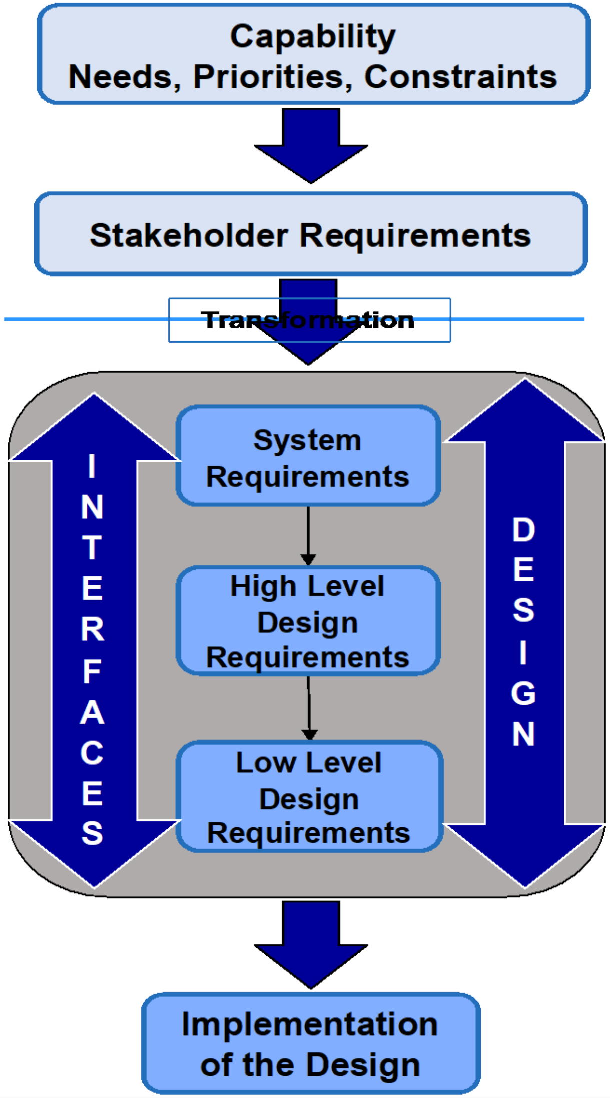
Capability needs, loss concerns, acceptance

- Mission
- System
- Regulatory, statutory, certification, policy
- Assurance

STRUCTURE

System architecture, design, interfaces, interconnections

- Exposure, hazards, vulnerabilities
- Critical functions
  - Mission
  - System
  - Security
  - Safety



Capability
Needs, Priorities, Constraints

Stakeholder Requirements

Transformation

System Requirements

High Level Design Requirements

Low Level Design Requirements

INTERFACES

DESIGN

Implementation of the Design

ADVERSITY

Loss scenarios

- Causal factors
  - Attack, subversion
  - Error, fault, failure
  - Abuse, misuse
- Conditions
  - Exposure, hazard, vulnerability
- Adversarial threat informed
  - Threat data-dependent
  - Threat data-independent

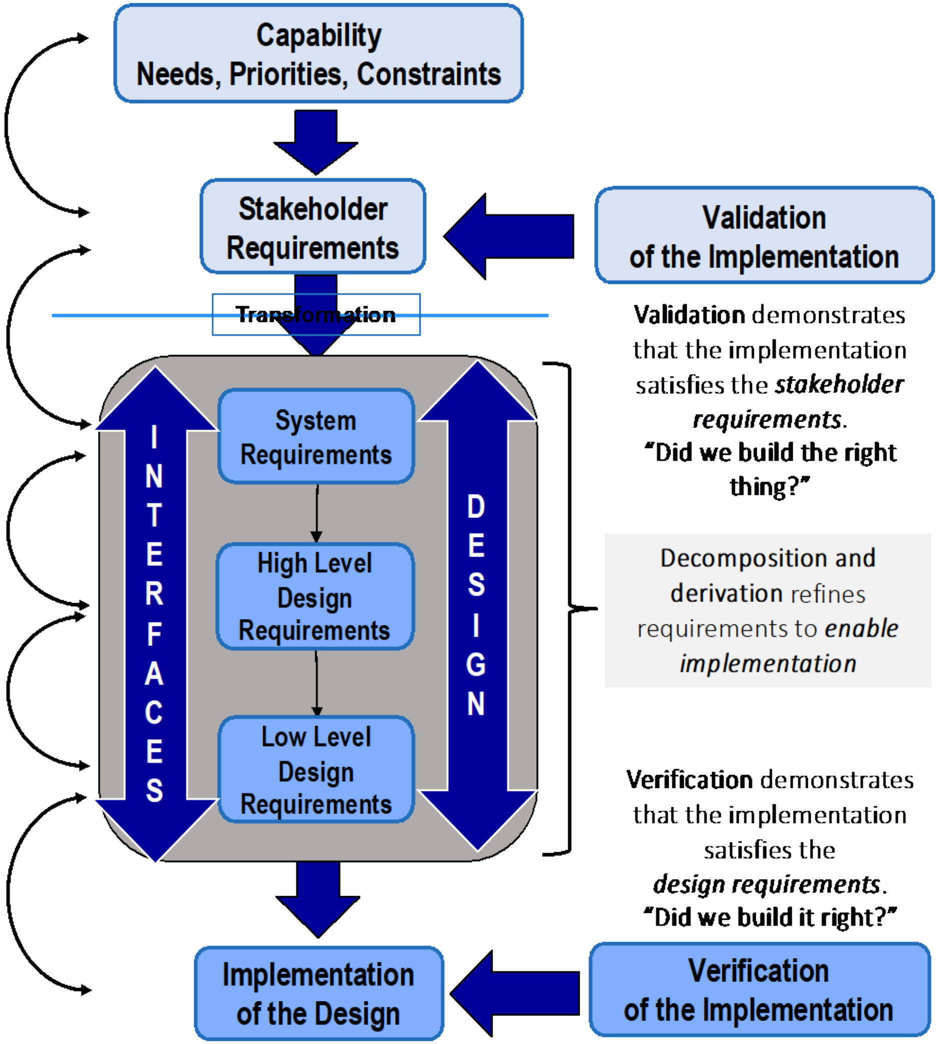
BEHAVIOR

System function, interfaces, data, interconnections

- Functional, data, control flow interactions
- Interactions not anticipated by the system requirements
- Exposure, hazards, vulnerabilities

System Security Engineering Requirements and Security Controls Comparison

Engineering Requirements



Capability
Needs, Priorities, Constraints

Stakeholder Requirements

Validation of the Implementation

Transformation

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

INTERFACES

System Requirements

High Level Design Requirements

Low Level Design Requirements

DESIGN

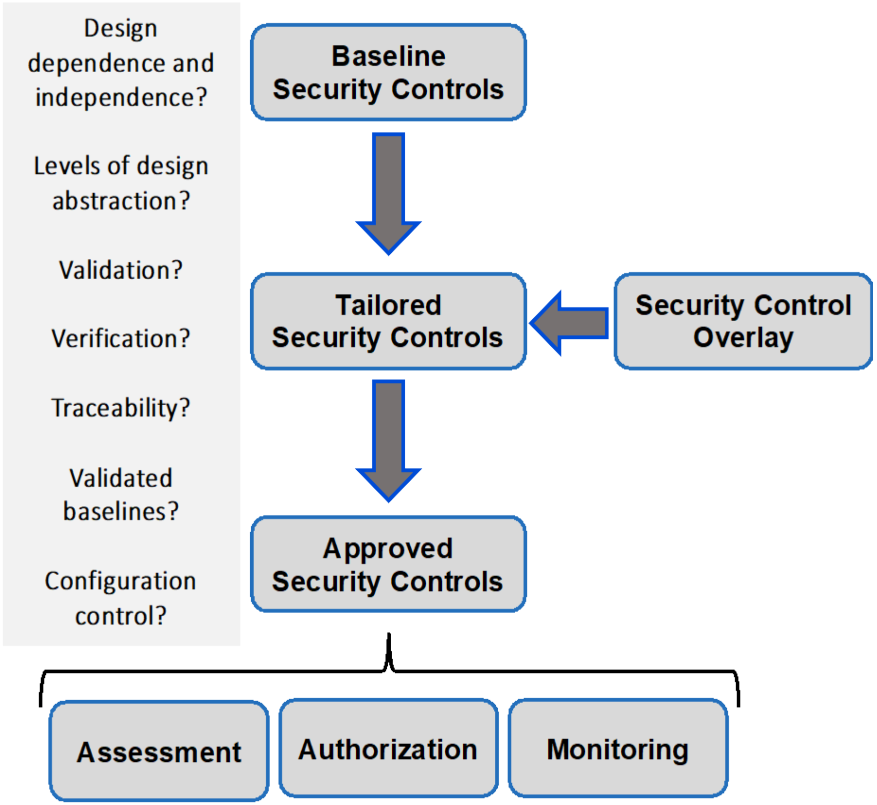
Decomposition and derivation refines requirements to *enable implementation*

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

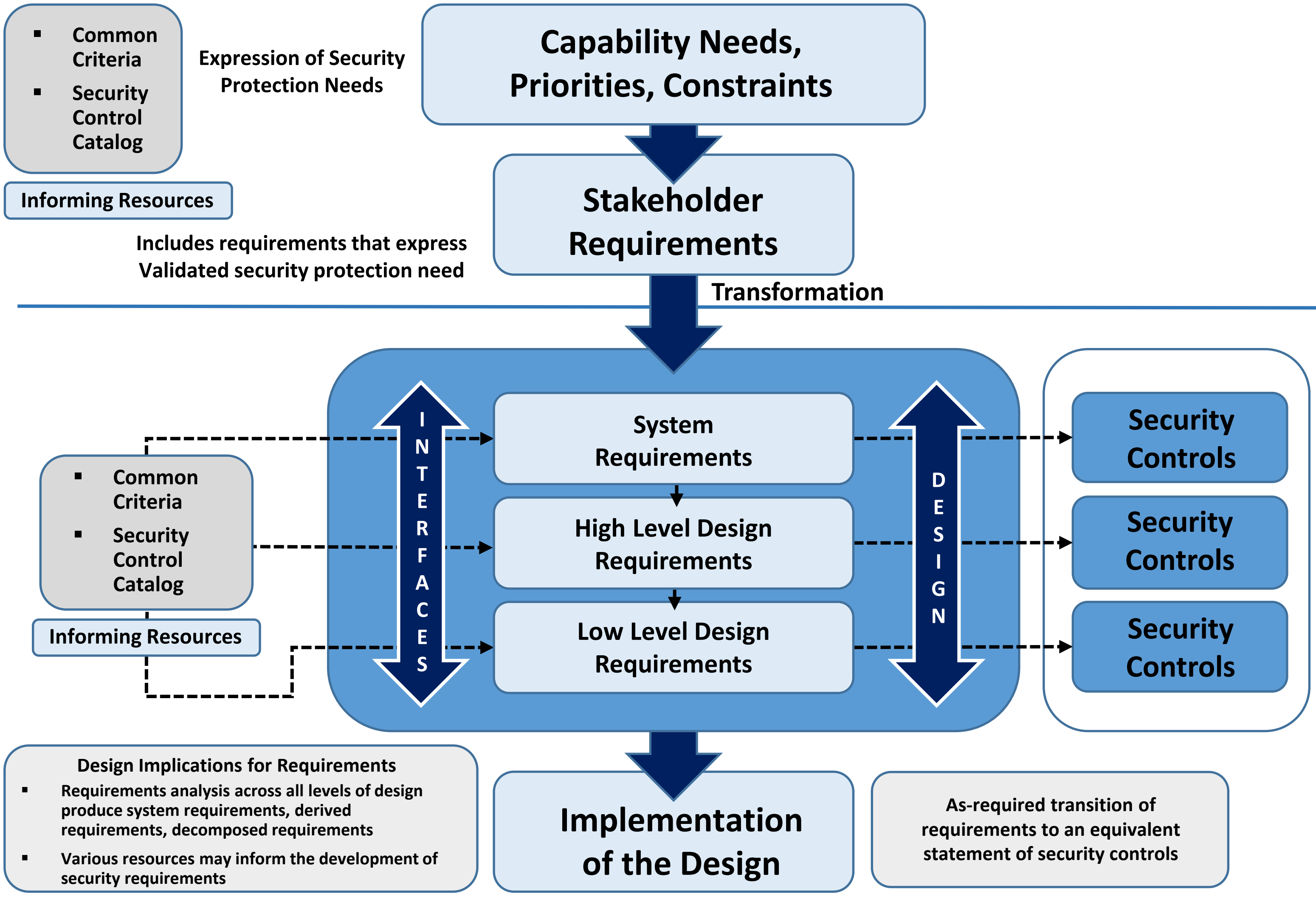
Approved Security Controls

Assessment

Authorization

Monitoring

Systems Security Engineering Use of Security Controls


Common Criteria
Security Control Catalog
Informing Resources
Expression of Security Protection Needs
Capability Needs, Priorities, Constraints
Stakeholder Requirements
Includes requirements that express Validated security protection need
Transformation
INTERFACES
System Requirements
High Level Design Requirements
Low Level Design Requirements
DESIGN
Security Controls
Security Controls
Security Controls
Common Criteria
Security Control Catalog
Informing Resources
Implementation of the Design
As-required transition of requirements to an equivalent statement of security controls

Design Implications for Requirements

- Requirements analysis across all levels of design produce system requirements, derived requirements, decomposed requirements
- Various resources may inform the development of security requirements

Security controls cannot replace requirements

- May be used as input to analysis to determine design-independent need
- May be used as input to system design analysis and development of derived and decomposed system requirements

Security controls must be traceable to their derivation source

- Performance objectives and adverse effects
- System design requirements

Security Requirements Derivation Consistent with DI-SESS-82177

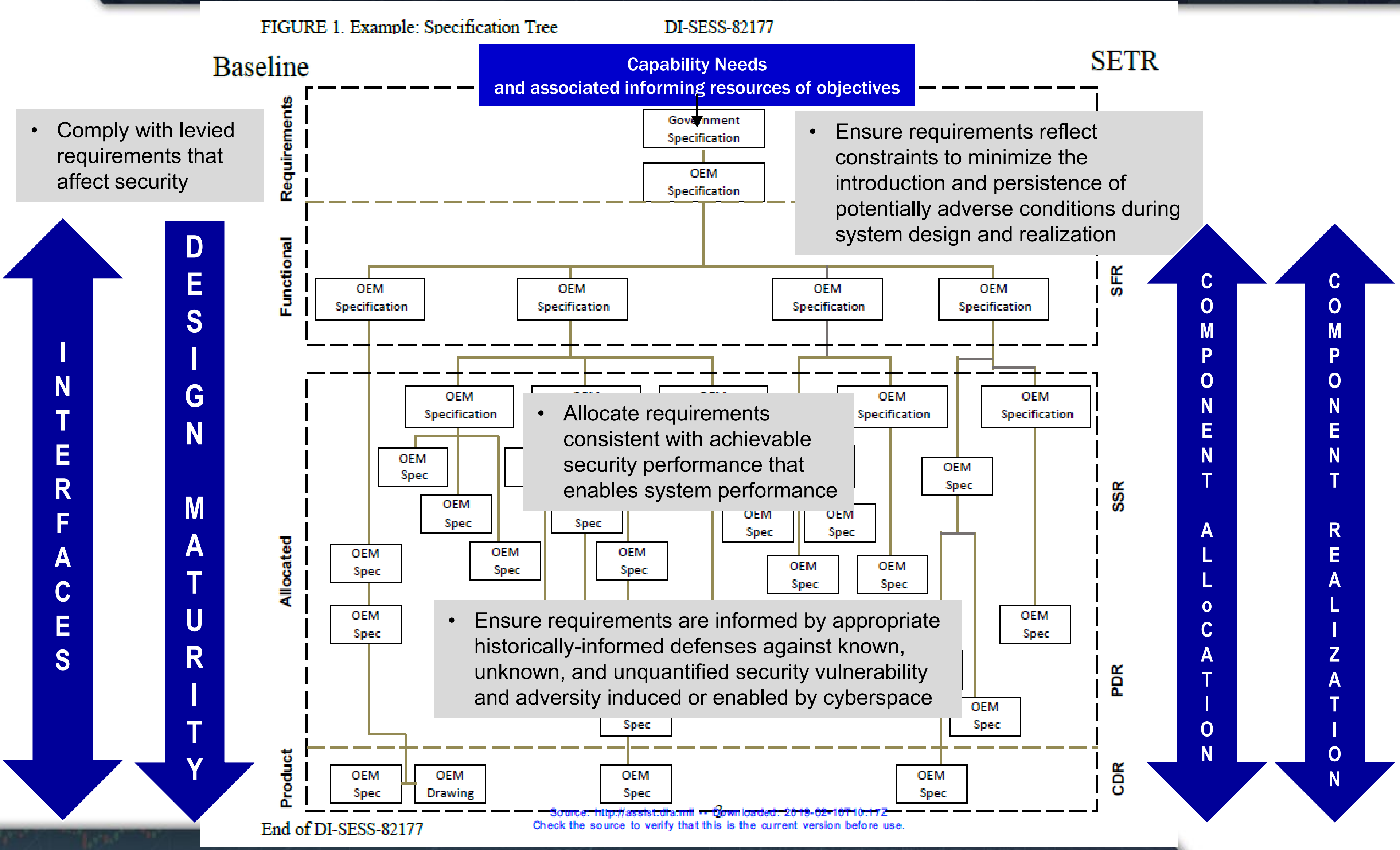


FIGURE 1. Example: Specification Tree

DI-SESS-82177

- Comply with levied requirements that affect security

- Ensure requirements reflect constraints to minimize the introduction and persistence of potentially adverse conditions during system design and realization

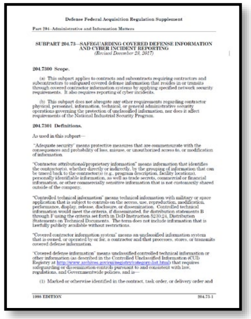
- Allocate requirements consistent with achievable security performance that enables system performance

- Ensure requirements are informed by appropriate historically-informed defenses against known, unknown, and unquantified security vulnerability and adversity induced or enabled by cyberspace

~~Source: http://assist.dla.mil -- Downloaded: 2019-02-16T10:17Z~~ 2
Check the source to verify that this is the current version before use.

End of DI-SESS-82177

Program Protection Planning, Includes Cyber Activities



Defense Federal Acquisition Regulation Supplement

Part 204—Administrative and Information Matters

SUBPART 204.73—SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING
(Revised December 28, 2017)

204.7300 Scope.

(a) This subpart applies to contracts and subcontracts requiring contractors and subcontractors to safeguard covered defense information that resides in or transits through covered contractor information systems by applying specified network security requirements. It also requires reporting of cyber incidents.

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information, nor does it affect requirements of the National Industrial Security Program.

204.7301 Definitions.

As used in this subpart—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

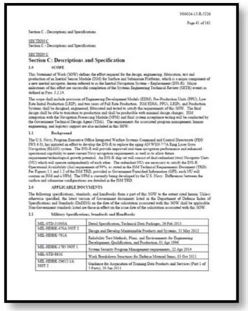
"Covered defense information" means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and

1998 EDITION 204.73-1

Section I FAR/DFAR Contract Clauses

+



N00024-15-R-5226

Page 41 of 161

Section C - Descriptions and Specifications

SECTION C
Section C - Descriptions and Specifications

SECTION C
Section C: Descriptions and Specification

1.0 SCOPE

This Statement of Work (SOW) defines the effort required for the design, engineering, fabrication, test and production of an Inertial Sensor Module (ISM) for Surface and Submarine Platforms, which is a major component of a new inertial navigator, herein referred to as the Inertial Navigation System – Replacement (INS-R). Major milestones of this effort are successful completion of the Systems Engineering Technical Review (SETR) events as defined in Para. 3.2.14.

The scope shall include provision of Engineering Development Models (EDM), Pre-Production Units (PPU), Low Rate Initial Production (LRIP), and two years of Full Rate Production. ISM EDMs, PPUs, LRIPs, and Production Systems shall be designed, engineered, fabricated and tested to satisfy the requirements of this SOW. The final design shall be able to transition to production and shall be producible with minimal design changes. ISM integration with the Navigation Processing Module (NPM) and final system acceptance testing will be conducted by the Government Technical Design Agent (TDA). The requirements for associated program management, human engineering, and logistics support are also included in this SOW.

1.1 Background

The U.S. Navy, Program Executive Office Integrated Warfare Systems Command and Control Directorate (PEO IWS 6.0), has initiated an effort to develop the INS-R to replace the aging AN/WSN-7/7A Ring Laser Gyro Navigation (RLGN) system. The INS-R will provide improved real-time navigation performance and enhanced operational capability to meet current Navy navigation requirements as well as to allow future requirement/technological growth potential. An INS-R ship set will consist of dual redundant (two) Navigator Units (NU) which will operate independently of each other. The redundant NUs are necessary to satisfy the INS-R Operational Availability (Ao) requirement of 99%, as stated in the ISM Technical Requirements Document (TRD). Per Figures 1.1 and 1.2 of the ISM TRD, provided as Government Furnished Information (GFI), each NU will contain an ISM and a NPM. The NPM is currently being developed by the U.S. Navy. Differences between the surface and submarine configurations are detailed in the ISM TRD.

2.0 APPLICABLE DOCUMENTS

The following specifications, standards, and handbooks form a part of this SOW to the extent cited herein. Unless otherwise specified, the latest version of Government documents listed in the Department of Defense Index of Specifications and Standards (DoDISS) on the date of the solicitation associated with this SOW shall be applicable. Non-Government standards listed are those in effect on the issue date of the solicitation associated with this SOW.

2.1 Military Specifications, Standards and Handbooks

MIL-STD-31000A	Detail Specification, Technical Data Packages, 26 Feb 2013
MIL-HDBK-470A NOT 2	Design and Develop Maintainable Products and Systems, 31 May 2012
MIL-HDBK-781A	Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production, 01 Apr 1996
MIL-HDBK-1785 NOT 1	System Security Program Management requirements, 22 Apr 2014
MIL-STD-881C	Work Breakdown Structures for Defense Material Items, 03 Oct 2011
MIL-HDBK-29612-1A NOT 2	Guidance for Acquisition of Training Data Products and Services (Part 1 of 5 Parts), 20 Jun 2011

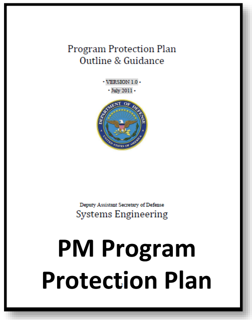
Section C Statement of Work

+

System Performance Specification

Government Furnished Information

+



Program Protection Plan
Outline & Guidance

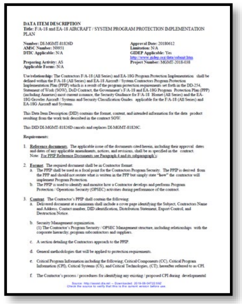
• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

PM Program Protection Plan

Government Furnished Information

+



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

Preparing Activity: AS
Applicable Forms: N/A

Approval Date: 20180612
Limitation: N/A
GIDEP Applicable: Yes
http://www.gidep.org/data/submit.htm
Project Number: MGMT-2018-038

Use/relationship: 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 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 Annexes) 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 and 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.

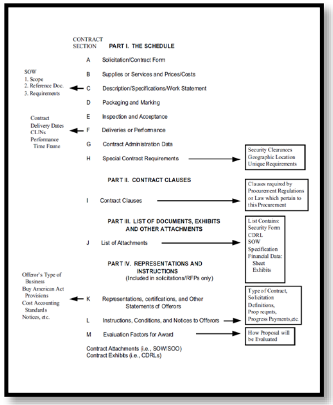
Requirements:

1. 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 subparagraph's:
2. Format. The required document shall be in Contractor format:
   a. The PPIP shall be used as a focal point for the Contractors 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.
   b. 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.
3. Content. The Contractor's PPIP shall contain the following:
   a. Delivered document at a minimum shall include a cover page identifying the Subject, Contractors Name and Address, Contact number, DID identification, Distribution Statement, Export Control, and Destruction Notice.
   b. Security Management organization.
      (1) The Contractor's Program Security / OPSEC Management structure, including relationships with the corporate hierarchy, program subcontractors and suppliers.
   c. A section detailing the Contractors approach to the PPIP.
   d. General methodologies that will be applied to protection requirements.
   e. 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.
   f. The Contactor's process / procedures for identifying any existing / proposed CPI during developmental

Source: http://assist.dla.mil -- Downloaded: 2019-08-04T22:59Z
Check the source to verify that this is the current version before use.

Contractor Program Protection Implementation Plan

- **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
Offeror's Type of Business
Buy American Act Provisions
Cost Accounting Standards
Notices, etc.
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
Type of Contract,
Solicitation
Definitions,
Prop reqmts,
Progress Payments,etc.
How Proposal will be Evaluated

Solicitation/Contract

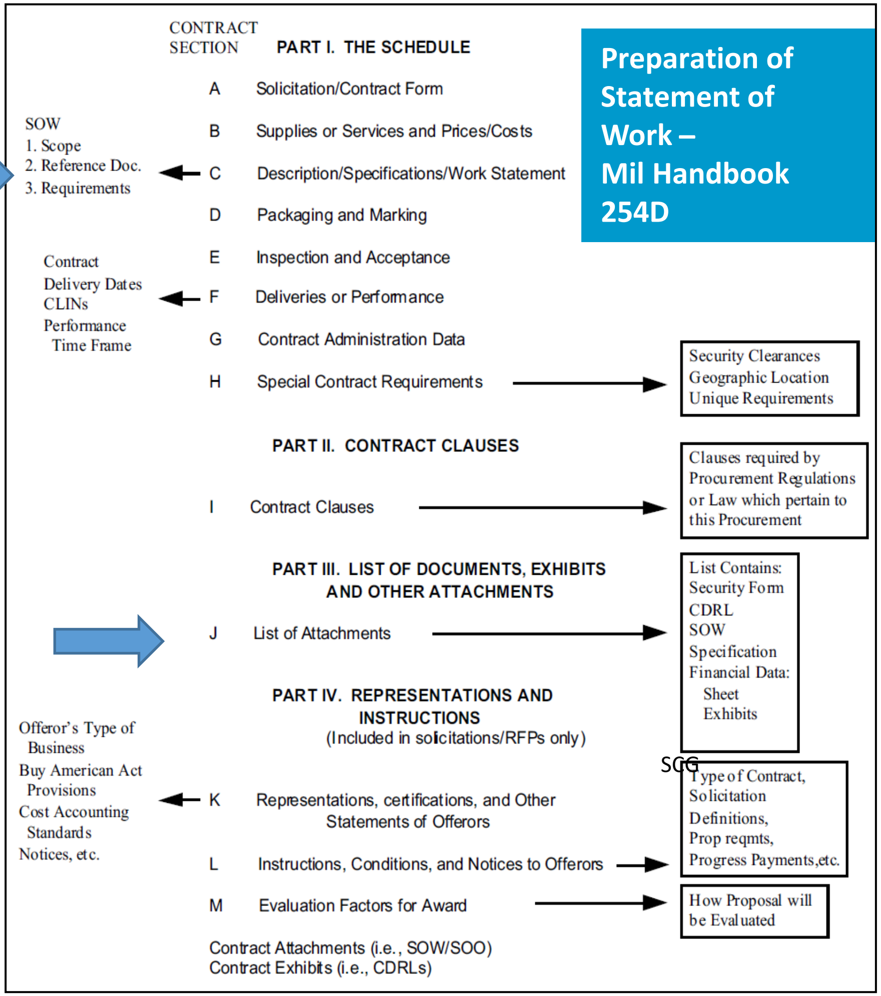
My Goal

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

Improve expectations across Government, industry, academia and operational stakeholders

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



Preparation of Statement of Work – Mil Handbook 254D

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 Performance ← 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.

SGG

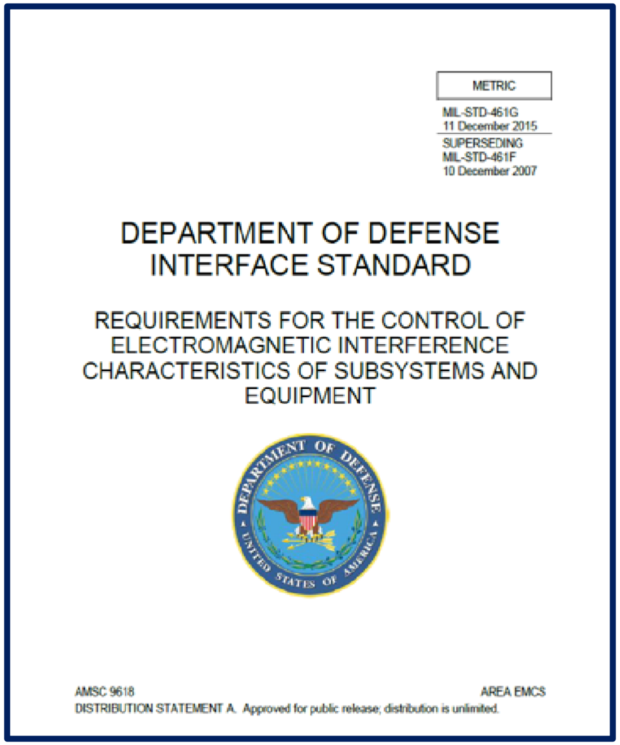
L Instructions, Conditions, and Notices to Offerors → Type of Contract, Solicitation Definitions, Prop reqmts, Progress Payments,etc.

M Evaluation Factors for Award → How Proposal will be Evaluated

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

Using a Federal Acquisition Regulation (FAR)-Based Contract

Example of a DoD Standard



METRIC

MIL-STD-461G
11 December 2015

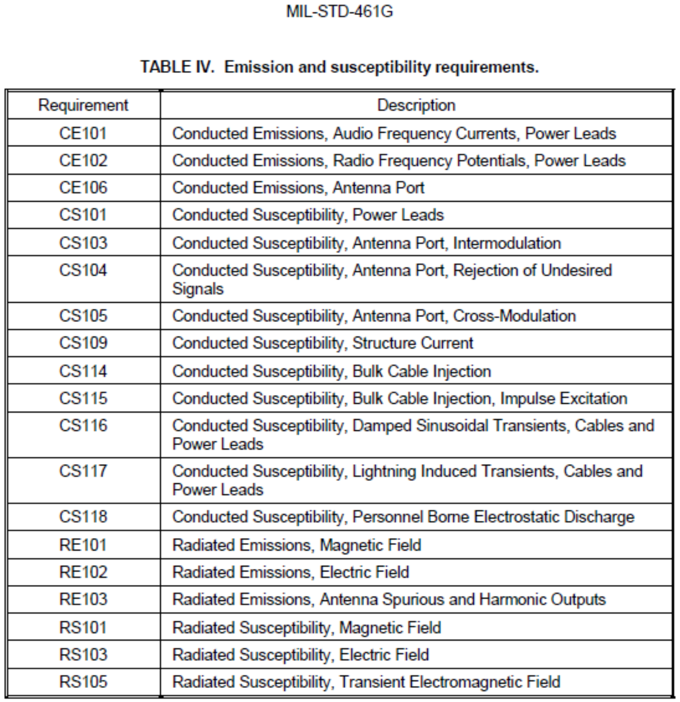
SUPERSEDING
MIL-STD-461F
10 December 2007

DEPARTMENT OF DEFENSE
INTERFACE STANDARD

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

AMSC 9618 AREA EMCS

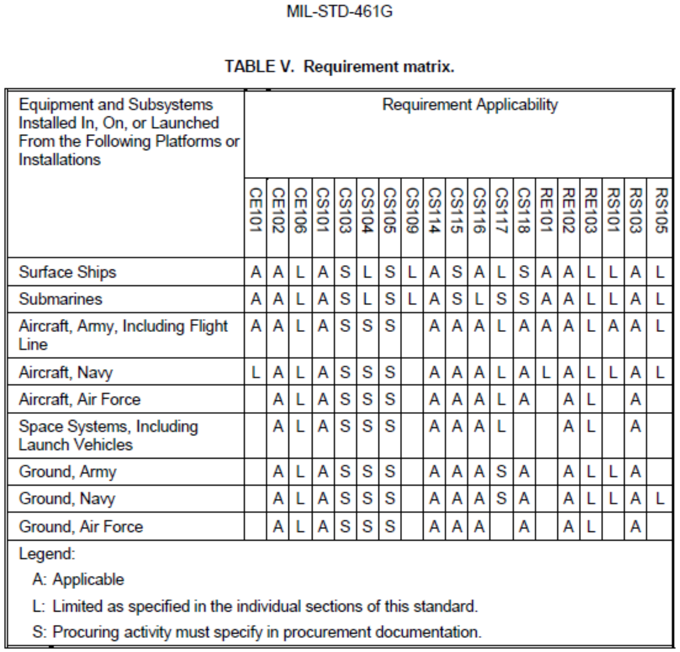
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.



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:

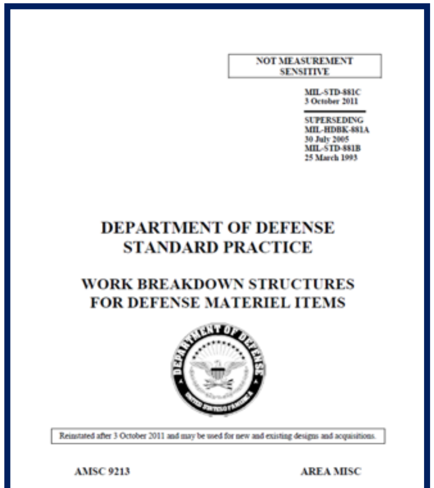
A: Applicable

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.

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

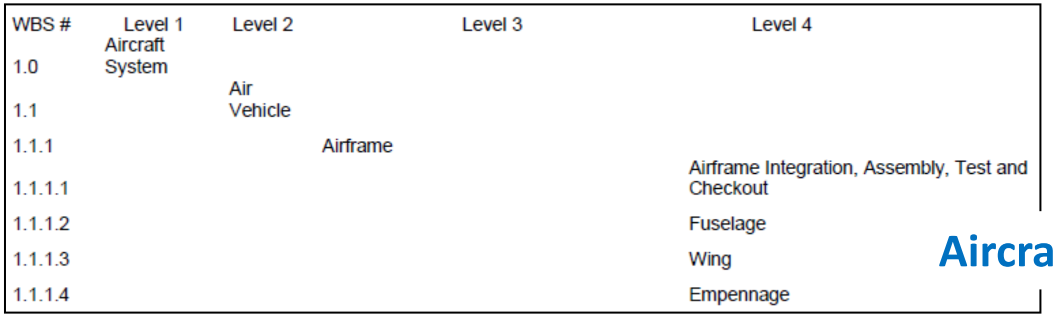
DEPARTMENT OF DEFENSE
STANDARD PRACTICE

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

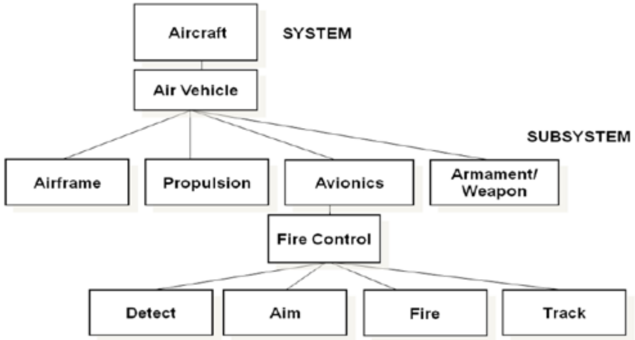
MIL-STD-881C

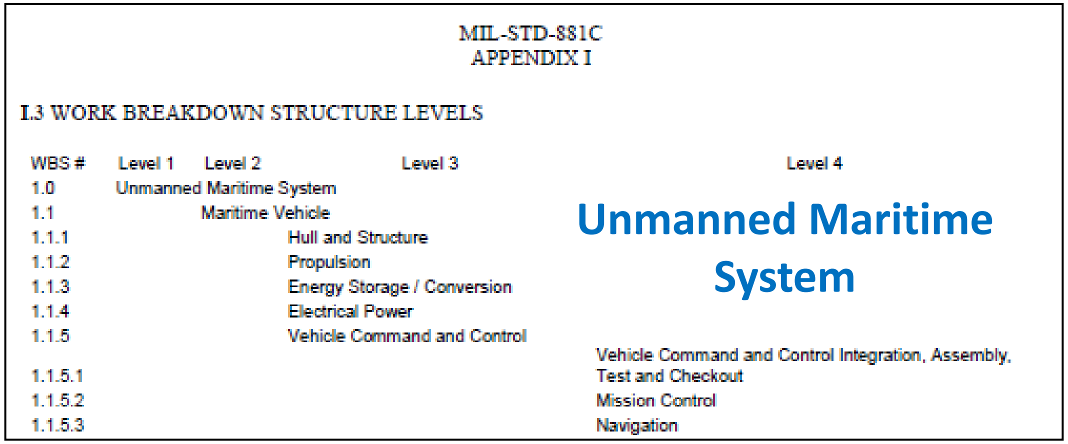


WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Aircraft System			
1.1		Air Vehicle		
1.1.1			Airframe	
1.1.1.1				Airframe Integration, Assembly, Test and Checkout
1.1.1.2				Fuselage
1.1.1.3				Wing
1.1.1.4				Empennage

Aircraft System

Provides a consistent and visible framework for defense materiel items



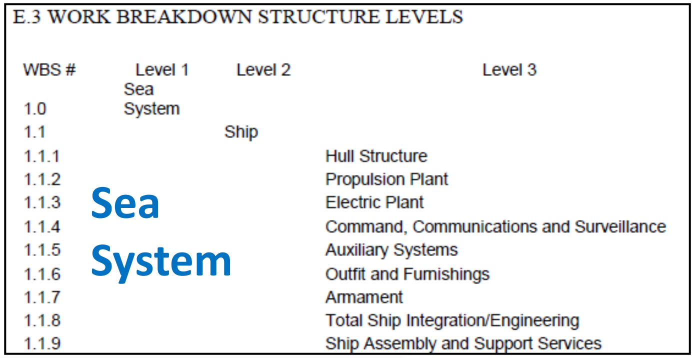


MIL-STD-881C
APPENDIX I

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



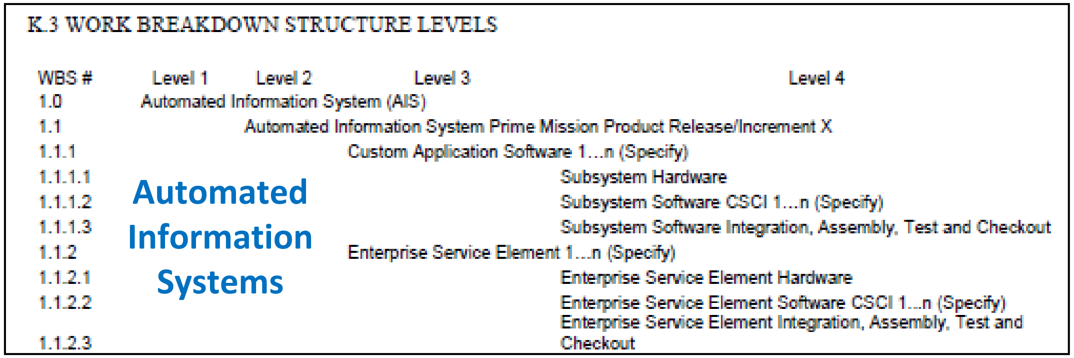
E.3 WORK BREAKDOWN STRUCTURE LEVELS

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 Fumishings
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. DOPSR case #21-S-0008 applies. Distribution is unlimited.

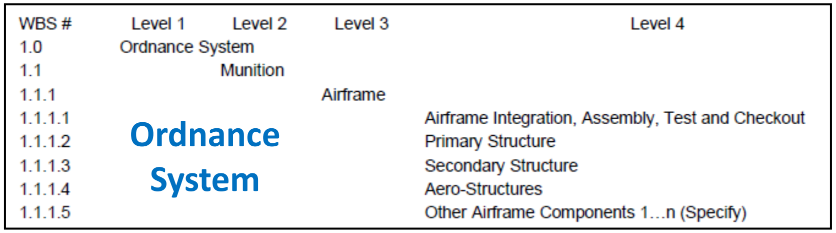
Standard Practices for Work Breakdown Structures – continued



K.3 WORK BREAKDOWN STRUCTURE LEVELS

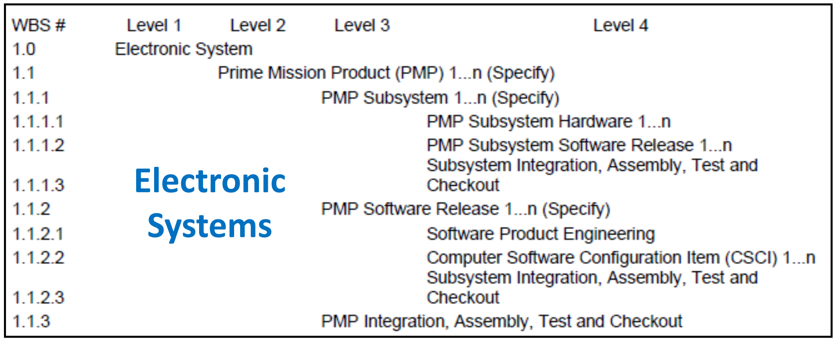
WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Automated Information System (AIS)			
1.1		Automated Information System Prime Mission Product Release/Increment X		
1.1.1			Custom Application Software 1…n (Specify)	
1.1.1.1				Subsystem Hardware
1.1.1.2				Subsystem Software CSCI 1…n (Specify)
1.1.1.3				Subsystem 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



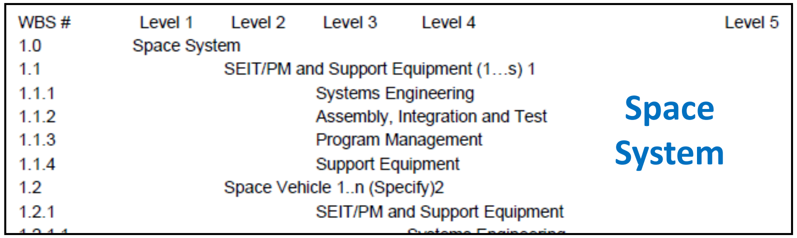
WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Ordnance System			
1.1		Munition		
1.1.1			Airframe	
1.1.1.1				Airframe Integration, Assembly, Test and Checkout
1.1.1.2				Primary Structure
1.1.1.3				Secondary Structure
1.1.1.4				Aero-Structures
1.1.1.5				Other Airframe Components 1…n (Specify)

Ordnance System



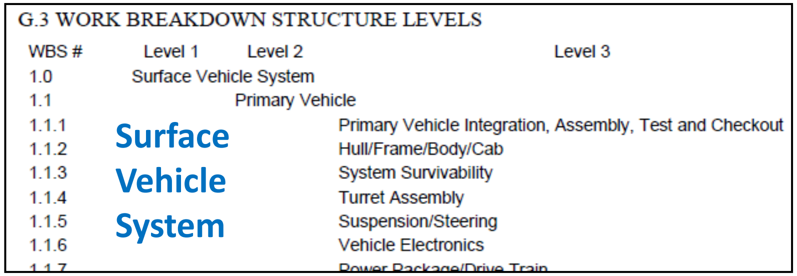
WBS #	Level 1	Level 2	Level 3	Level 4
1.0	Electronic System			
1.1		Prime Mission Product (PMP) 1...n (Specify)		
1.1.1			PMP Subsystem 1...n (Specify)	
1.1.1.1				PMP Subsystem Hardware 1...n
1.1.1.2				PMP Subsystem Software Release 1...n
1.1.1.3				Subsystem Integration, Assembly, Test and Checkout
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	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

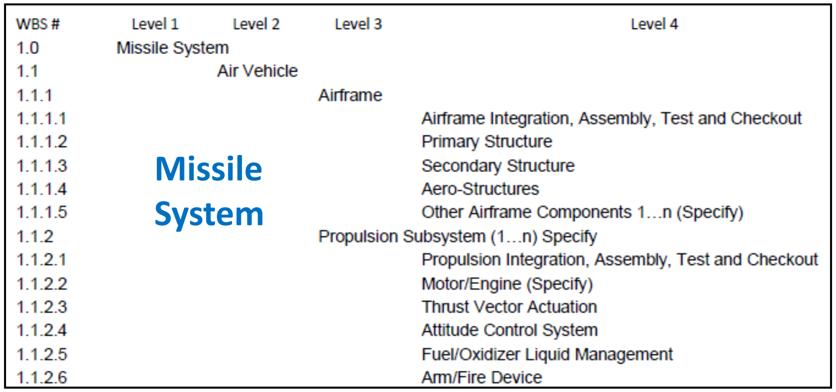


G.3 WORK BREAKDOWN STRUCTURE LEVELS

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	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

Approach to Acquire Data Deliverables

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

SOW establishes a requirement e.g., “3.5. “…a record of tier 1 level subcontractors, vendors and/or suppliers who will receive or develop 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”

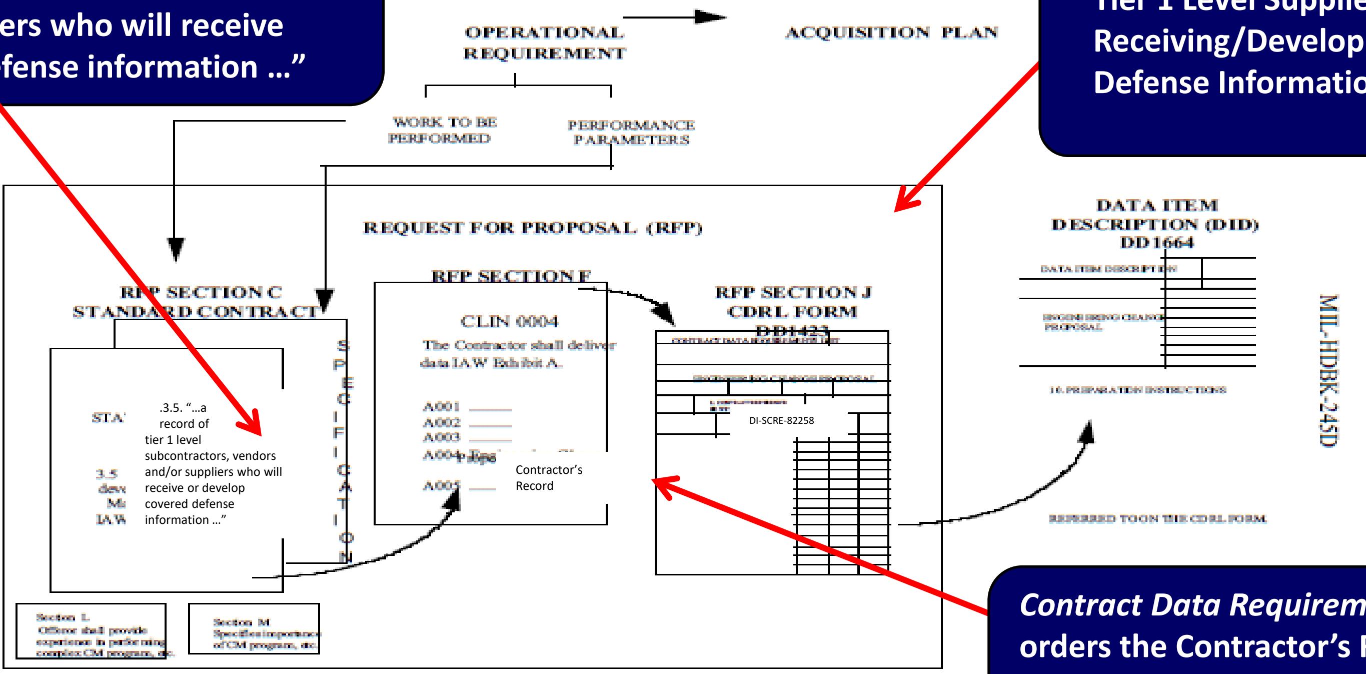
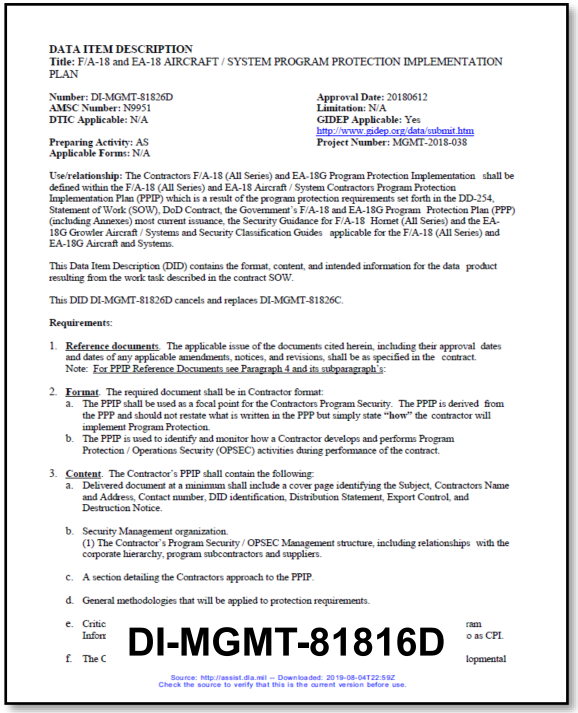

OPERATIONAL REQUIREMENT
ACQUISITION PLAN
WORK TO BE PERFORMED
PERFORMANCE PARAMETERS
REQUEST FOR PROPOSAL (RFP)
RFP SECTION C
STANDARD CONTRACT
STA
.3.5. “…a record of tier 1 level subcontractors, vendors and/or suppliers who will receive or develop covered defense information …”
3.5
SPECIFICATION
RFP SECTION F
CLIN 0004
The Contractor shall deliver data IAW Exhibit A.
A001
A002
A003
A004
A005
Contractor’s Record
RFP SECTION J
CDRL FORM
DD1423
CONTRACT DATA REQUIREMENTS LIST
ENGINEERING CHANGE PROPOSAL
DI-SCRE-82258
Section L
Offeror shall provide experience in performing complex CM program, etc.
Section M
Specifies importance of CM program, etc.
DATA ITEM DESCRIPTION (DID)
DD1664
DATA ITEM DESCRIPTION
ENGINEERING CHANGE PROPOSAL
10. PREPARATION INSTRUCTIONS
REFERRED TO ON THE CDRL FORM
MIL-HDBK-245D

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

Contract Data Requirements List (CDRL) orders the Contractor’s Record data item and identifies due date, distribution statement and other such parameters

Distribution Statement A: Approved for public release. DOPSR case #21-S-0008 applies. Distribution is unlimited.

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

Preparing Activity: AS
Applicable Forms: N/A

Approval Date: 20180612
Limitation: N/A
GIDEP Applicable: Yes
http://www.gidep.org/data/submit.htm
Project Number: MGMT-2018-038

Use/relationship: 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 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 Annexes) 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 and 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:

1. **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 subparagraph's:

2. **Format**. The required document shall be in Contractor format:
   a. The PPIP shall be used as a focal point for the Contractors 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.
   b. 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.

3. **Content**. The Contractor's PPIP shall contain the following:
   a. Delivered document at a minimum shall include a cover page identifying the Subject, Contractors Name and Address, Contact number, DID identification, Distribution Statement, Export Control, and Destruction Notice.

   b. Security Management organization.
   (1) The Contractor's Program Security / OPSEC Management structure, including relationships with the corporate hierarchy, program subcontractors and suppliers.

   c. A section detailing the Contractors approach to the PPIP.

   d. General methodologies that will be applied to protection requirements.

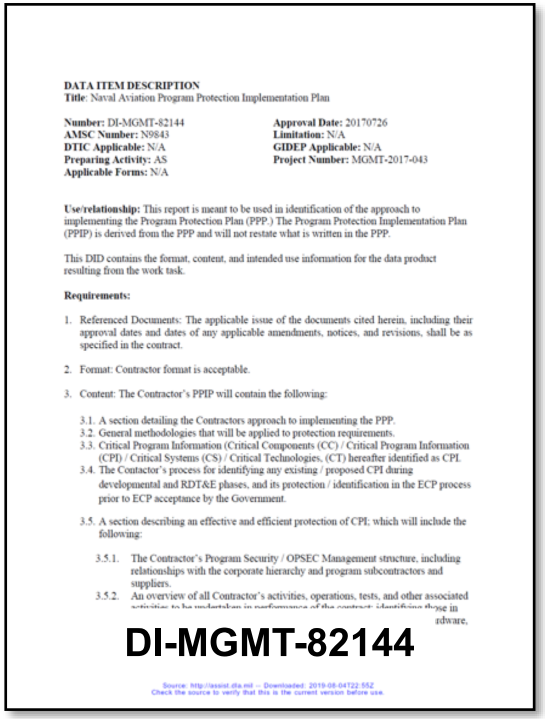
   e. Critic ram
   Infor o as CPI.

   f. The C lopmental

DI-MGMT-81816D

Source: http://assist.dla.mil -- Downloaded: 2019-08-04T22:59Z
Check the source to verify that this is the current version before use.

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: N9843
DTIC Applicable: N/A
Preparing Activity: AS
Applicable Forms: 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:

1. 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.

2. Format: Contractor format is acceptable.

3. Content: The Contractor's PPIP will contain the following:

   3.1. A section detailing the Contractors approach to implementing the PPP.
   3.2. General methodologies that will be applied to protection requirements.
   3.3. Critical Program Information (Critical Components (CC) / Critical Program Information (CPI) / Critical Systems (CS) / Critical Technologies, (CT) hereafter identified as CPI.
   3.4. The Contactor's process for identifying any existing / proposed CPI during developmental and RDT&E phases, and its protection / identification in the ECP process prior to ECP acceptance by the Government.

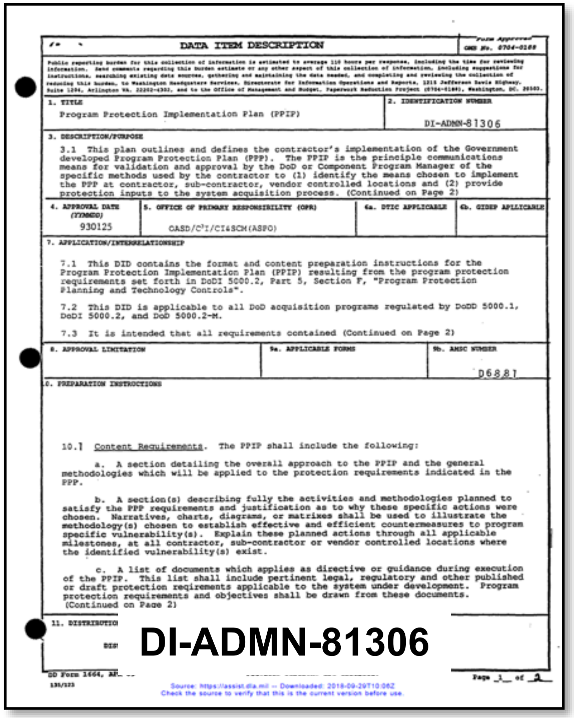
   3.5. A section describing an effective and efficient protection of CPI; which will include the following:

   3.5.1. The Contractor's Program Security / OPSEC Management structure, including relationships with the corporate hierarchy and program subcontractors and suppliers.
   3.5.2. An overview of all Contractor's activities, operations, tests, and other associated activities to be undertaken in performance of the contract; identifying those in rdware,

DI-MGMT-82144

Source: http://assist.dla.mil -- Downloaded: 2019-08-04T22:55Z
Check the source to verify that this is the current version before use.

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
Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of reducing this burden, to Washington Headquarters Services, 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 (0704-0188), Washington, DC 20503.

1. TITLE
Program Protection Implementation Plan (PPIP)

2. IDENTIFICATION NUMBER
DI-ADMN-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 principle 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 (YYMMDD)
930125

5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)
OASD/C³I/CI&SCM(ASPO)

6a. DTIC APPLICABLE

6b. GIDEP APLLICABLE

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 DoD 5000.2-M.

7.3 It is intended that all requirements contained (Continued on Page 2)

8. APPROVAL LIMITATION

9a. APPLICABLE FORMS

9b. AMSC NUMBER
D6881

10. PREPARATION INSTRUCTIONS

10.1 Content Requirements. The PPIP shall include the following:

a. 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.

b. A section(s) describing fully the activities and methodologies planned to satisfy the PPP requirements and justification as to why these specific actions were chosen. Narratives, charts, diagrams, or matrixes shall be used to illustrate the methodology(s) chosen to establish effective and efficient countermeasures to program specific vulnerability(s). Explain these planned actions through all applicable milestones, at all contractor, sub-contractor or vendor controlled locations where the identified vulnerability(s) exist.

c. 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 reqirements applicable to the system under development. Program protection requirements and objectives shall be drawn from these documents. (Continued on Page 2)

11. DISTRIBUTIO
DIS

DI-ADMN-81306

DD Form 1664, AP
135/123

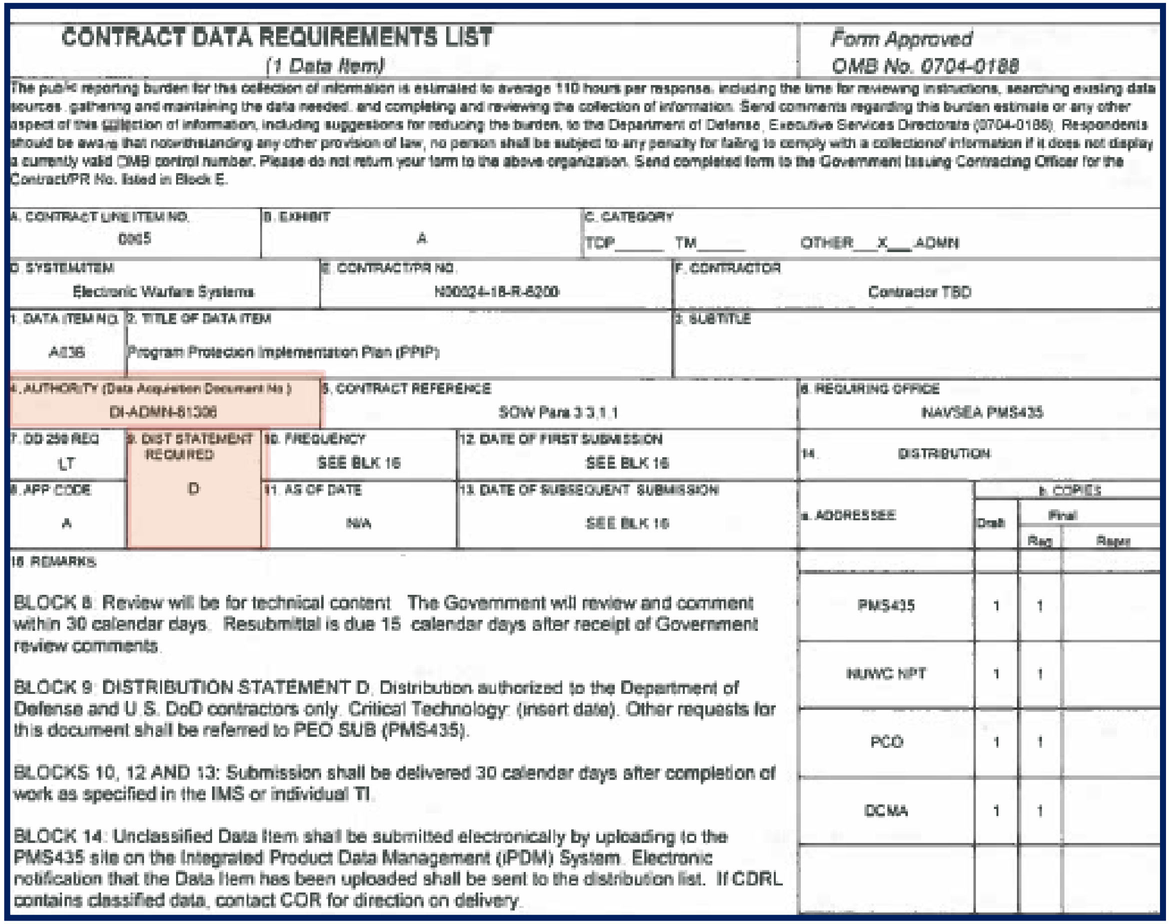
Page 1 of 2

Source: https://assist.dla.mil -- Downloaded: 2018-09-29T10:06Z
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…

Establishes content requirements for data deliverables

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 collectionof 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 TDP_____ TM_____ OTHER__X__ADMN
D. SYSTEM/ITEM Electronic Warfare Systems
E. CONTRACT/PR NO. N00024-18-R-6200
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-ADMN-81306
5. CONTRACT REFERENCE SOW Para 3.3.1.1
6. REQUIRING OFFICE NAVSEA PMS435
7. DD 250 REQ LT
8. APP CODE A
9. DIST STATEMENT REQUIRED D
10. FREQUENCY SEE BLK 16
11. AS OF DATE N/A
12. DATE OF FIRST SUBMISSION SEE BLK 16
13. DATE OF SUBSEQUENT SUBMISSION SEE BLK 16
14. DISTRIBUTION

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
PMS435	1	1	
NUWC NPT	1	1	
PCO	1	1	
DCMA	1	1	

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.

**Block 2. Identifies the Title of Data Deliverable –
Program Protection Implementation Plan**

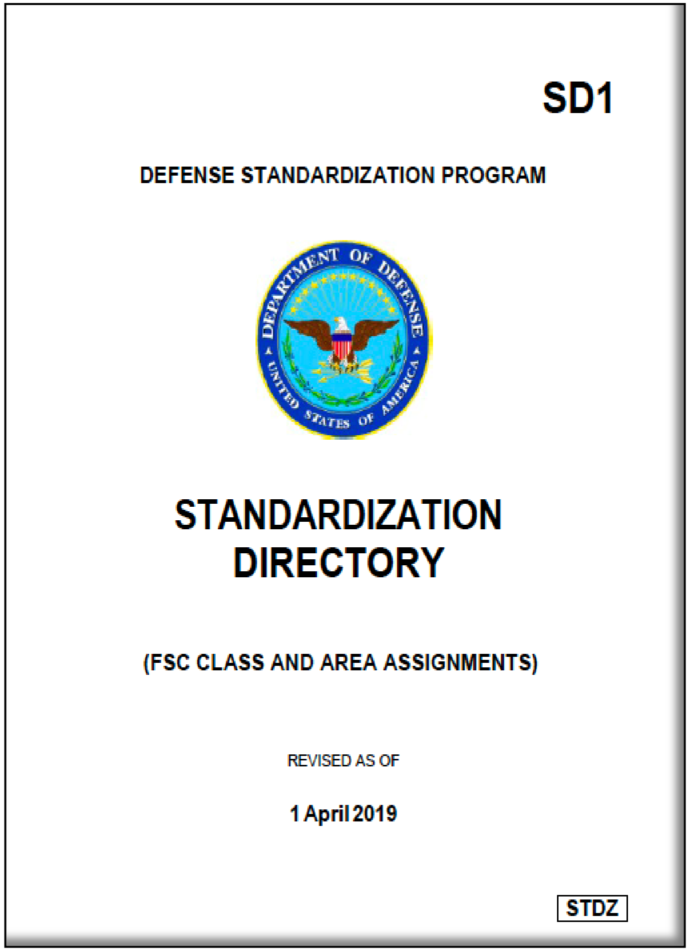
**Block 4. Identifies the Data Item Description –
DI-ADMIN-81360
Program Protection Implementation Plan**

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

Secure Cyber Resilience Engineering (SCRE) Standardization Area



SD1

DEFENSE STANDARDIZATION PROGRAM

STANDARDIZATION DIRECTORY

(FSC CLASS AND AREA ASSIGNMENTS)

REVISED AS OF

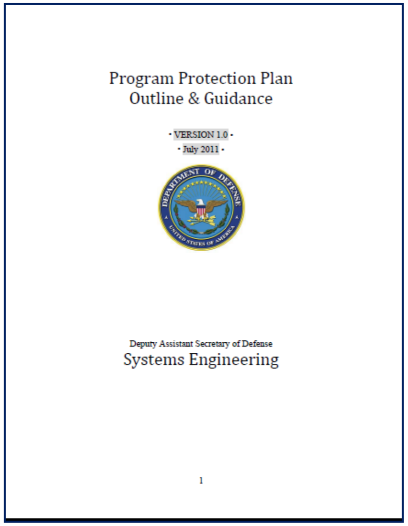
1 April 2019

STDZ

- **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.

Secure Cyber Resilient Engineering Standardization Area Established in March 2019

Program Protection Planning Update



Program Protection Plan
Outline & Guidance

· VERSION 1.0 ·
· July 2011 ·

Deputy Assistant Secretary of Defense
Systems Engineering

1

Modernize the PPP Outline and Guidance

- Policy Updates
- Acquisition Regulations
- Standards
- Lessons Learned

Concerted effort to enable consistent tailored implementation

- Scheduling virtual roadshows to provide training on implementation of DoDI 5000.83
- Updates to Defense Acquisition University (DAU) S&T managers and engineering education and training for technology and program protection will be informed by R&E-led Engineering Workforce Task Force

Collaboration with stakeholders is forthcoming

Summary

- DoDI 5000.83 establishes roles and responsibilities for the S&T manager and the engineering workforce
  - Updates to guidance, standards, education and training are pending to make more consistent implementation
- 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

Customer-Focused: Outcome-Based

Wrap-Up

Questions?

Backup

Backup

Distribution Statement A: Approved for public release. DOPSR case #20-S-2038 applies. Distribution is unlimited.

Alignment to National Defense Strategy

Technology and Program Protection

- Assigns responsibilities for S&T managers and engineers
- OUSD(R&E) monitors process, delegates responsibility to greatest extent practicable; approves acquisition categories (ACAT) 1D Program Protection Plans
- Links to Pathways, Engineering, Cybersecurity in the Acquisition System, Test and Evaluation, and Sustainment

Activities to Mitigate Adversary Threats

- Includes responsibilities for DoD-sponsored research, prior to Materiel Development Decision (MDD)
- Reinforces best practices for risk informed technical and engineering mitigations
- Implements technical information, hardware assurance, software assurance, anti tamper, and cyber resilient security engineering methods and level of assurance to achieve protection and cyber objectives
- Refreshed periodically throughout the program lifecycle

Technology Modernization Priorities

- Establishes TAPP for modernization priorities
- Establishes S&T Protection activities
- Enhanced protection for critical programs and technologies

Tailored Program Protection for Acquisition Pathways

- Enables tailoring to pathway focus areas
- Determine protection planning and implementation risks as part of the design and technical risk assessment process
- Ensure operator is informed of operational risks when system is fielded