# Air Force Materiel Command Supplement to Department of Defense Systems Engineering Plan (SEP) Outline V4

# Version 1.0

**Date: 12 May 2023**

Approved By:

STEIPP.CHADWICK.M.1089149289

Digitally signed by STEIPP.CHADWICK.M.1089149289
Date: 2023.05.12 12:44:30 -04'00'

CHADWICK M. STEIPP, Col, USAF
Deputy Director, Engineering
and Technical Management

## Preface

The Office of the Deputy Director for Engineering for the Department of Defense published the Systems Engineering Plan (SEP) Outline Version 4 in September of 2021. Although the outline indicates required SEP content, the format is not prescribed. Each Service is allowed to use the OSD Outline as a template to create further SEP guidance with required content.

The Air Force Materiel Command has elected to create this supplement using Version 4.0 of the OSD SEP Outline as the basis to further refine Digital Engineering content that should be included in a Program-level Systems Engineering Plan. The original OSD SEP Outline content in this document is written in black text, Air Force specific supplemental guidance is **written in bold font and preceded by the words (Added)(AFMC).**

# [Program Name]

# SYSTEMS ENGINEERING PLAN (SEP)

**[DATE]**

**Publishing Organization**

Distribution Statements as Needed

Office of Primary Responsibility (OPR):

Name
Address
Email

# Contents

## Tables



## Figures



*Note: Additional tables and figures may be included at the Component or Program Manager's discretion.*

[MANDATORY APPROVAL PAGE CONTENT]

# PROGRAM NAME – ACAT LEVEL___

# [ACQUISITION PATHWAY]

# SYSTEMS ENGINEERING PLAN
# VERSION ___

# SUPPORTING _____DECISION
# AND
# SUPPORTING TRANSITION INTO_____PHASE

# [DATE]

**********

## SEP APPROVAL AUTHORITY APPROVAL

_____ _____

Approval Authority Name Date
Approval Authority Signature Block

SUBMITTED BY

| | | | |
|---|---|---|---|
| Name<br>Program Lead Systems Engineer | Date | Name<br>Program Manager | Date |

CONCURRENCE

| | | | |
|---|---|---|---|
| Name<br>Lead/Chief Systems Engineer<br>(System Center or Command) | Date | Name<br>Program Executive Officer or Equivalent | Date |

COMPONENT APPROVAL

| | |
|---|---|
| Name<br>Title, Office<br>Component SEP Approval Authority | Date |

***Expectation:*** *The following expectations apply to the Systems Engineering Plan (SEP) as a whole:*

- The Lead Systems Engineer/Chief Engineer (LSE/CE), under the direction of the Program Manager (PM), will prepare a SEP to manage the systems engineering (SE) activities starting at Milestone A (Department of Defense Instruction (DoDI) 5000.88, Engineering of Defense Systems). The SEP should be a "living," "go-to" technical planning document and should serve as the blueprint for the conduct, management, and control of the technical aspects of the government's program from concept to disposal.
- The SEP is a planning and management tool, specific to the program and tailored to meet program needs. Although the SEP Outline employs terminology mainly applicable to DoDI 5000.02, Operation of the Adaptive Acquisition Framework (e.g., DoDI 5000.85, Major Capability Acquisition), the principles and practices described herein should be applied, as appropriate, to all DoD programs.
- The SEP defines the methods for implementing all system requirements having technical content, technical staffing, and technical management.
- The SEP will include the engineering management approach to include technical baseline management; requirements traceability; linkage to the system architecture; configuration management (CM); risk, issue, and opportunity management; and technical trades and evaluation criteria (DoDI 5000.88, Para 3.4.a.(3).(b, d and l)).
- The SEP will describe a data management approach consistent with the DoD Data Strategy. The approach should support maximizing the technical coherency of data as it is shared across engineering disciplines (DoDI 5000.88, Para 3.4.a.(3).(s)). Additional approaches to data management should at a minimum describe:
    - **(Added)(AFMC) Determination if a classified repository is needed;**
    - **(Added)(AFMC) Development of an Intellectual Property Strategy to identify and manage the full spectrum of data rights and related issues (e.g., Intellectual Property rights, technical data and computer software deliverables, patented technologies, and appropriate license rights) from the inception of a program and throughout its life cycle. Separately address IP and licensing associated with establishment of digital engineering tools, database, etc., to be used through product life cycle. For technical data, computer software deliverables, and digital engineering tools, identify the license owner;**
    - The government's ownership in, or intellectual property (IP) license rights it has acquired to data it created or a contractor delivered to it, respectively;
    - Digital artifact generation for reporting and distribution purposes;
    - Expected data and method of delivery to the government, from all models, simulations, designs, reviews, audits, analysis, formal contract deliverables, and expected level of data rights (DoDI 5000.88, Para 3.4.a.(3).(j)); and;
    - Sufficient data to support system testing and assessment of the system.
- Upon approval by the Milestone Decision Authority (MDA), the SEP provides authority and empowers the LSE/CE to execute the program's technical plan.
- The SEP should be updated following a technical review, before milestones or the Development Request for Proposal (RFP) Release Decision Point, or as a result of SE planning changes.

- The SEP should be updated after contract award to reflect (1) the winning contractor(s)' technical approach reflected in the Systems Engineering Management Plan (SEMP) **(Added)(AFMC) (2) a summary of the contractor and government team structures and Integrated Digital Environment integration, and (3)** details not available before contract award. This post-award update should be completed within 120 days of contract award or no later than 30 days before the next technical review. The program should define and justify this update as either a minor or major update to influence related staffing and approval risk.

# 1 Introduction

The introduction should:

- Summarize the program (ensure the description aligns with the program Acquisition Strategy (AS)).
- Describe how the Program Management Office (PMO) has tailored the SEP to execute the AS.
- Describe the program's plan to align the Prime Contractor's SEMP with the PMO SEP.
- Summarize how and when the SEP is updated and the criteria for doing so.
- **(Added)(AFMC) Summarize how the program plans to implement Model Based Systems Engineering and Digital Engineering processes.**
- Identify the phase of the program, its entry and exit criteria, and approval and updating authority(ies).

# 2 Program Technical Definition

## 2.1 Requirements Development

Describe how technical requirements are defined, derived, and refined from the Joint Capabilities Integration and Development System (JCIDS) or other applicable capability requirements documents down to configuration item (CI) build-to specifications and verification plans. (*See* SE Guidebook (forthcoming), Requirements Analysis Process, for additional guidance). **(Added)(AFMC) This section should also describe the authoritative process for requirements modification (e.g., who has the authority to approve requirements changes for KPP's or KSA's).**

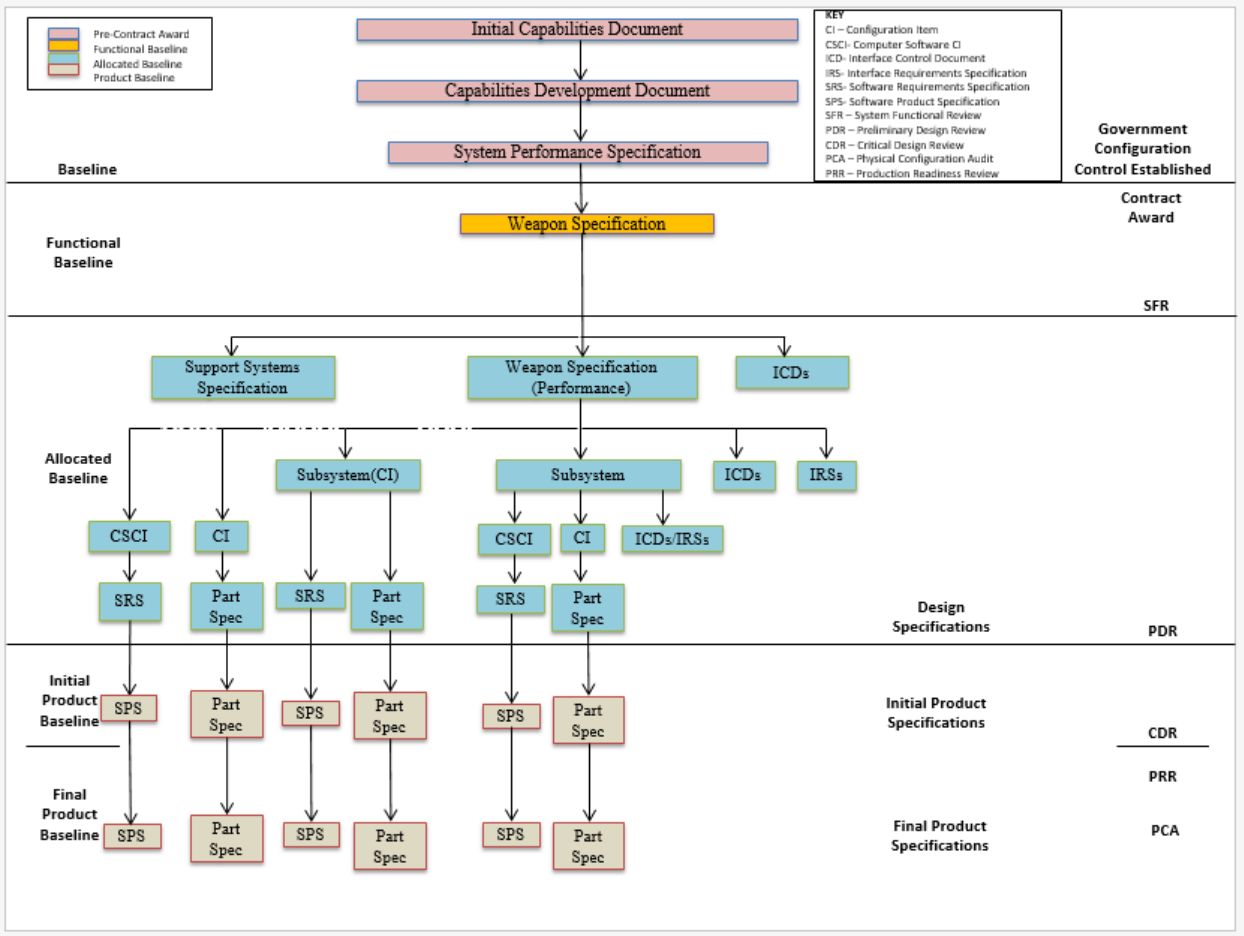
***Expectation:*** *Program should maximize traceability and the use of models as an integral part of the mission, concept, and technical baseline to trace measures of effectiveness, measures of performance, and all requirements throughout the life cycle from JCIDS (or equivalent requirements authoritative source(s)) into a verification matrix, equivalent artifact, or tool that provides contiguous requirements traceability digitally.* ***(Added)(AFMC) Program should describe automated tools used throughout the process of requirements analysis and tradespace analysis and define responsible Point of Contact for each level of requirement****. A decomposition/specification tree provides a summary of the requirements traceability and technical baselines. The requirements trace should not contain any orphan requirements. The requirements trace should identify those requirements that were identified in the JCIDS documents as expected to change over the life of the program due to evolution of the threat or technology so that they may be considered in the modular open systems approach (MOSA). Figure 2.1-1 shows a sample Requirements Decomposition/Specification Tree/Baseline (DoDI 5000.88, Para 3.4.a.(3).(l)).*

***Expectation:*** *Program requirements documents for all* ***(Added)(AFMC) National Security Systems (NSS)*** *will have program protection, cybersecurity, cyber survivability, and operational resilience requirements defined in the requirements source (see DoDI 5000.82, Acquisition of Information Technology (IT)). Cybersecurity requirements are usually related to the Risk Management Framework (DoDI 8510.01, Risk Management Framework for DoDEA Information Technology) and federal laws. Cyber survivability requirements are specified using the Joint Staff Cyber Survivability Endorsement Implementation Guide and are threshold requirements in addition to the System Survivability (SS) Key Performance Parameter (KPP), even if the program does not have an SS KPP. Operational resilience is a specified requirement in the DoDI 8500.01.* ***(Added)(AFMC) DAF Users are encouraged to utilize the guidance and best practices outlined in the DAF Systems Security Engineering (SSE) Cyber Guidebook (SSECG)****. Implied and derived cyber requirements (security, survivability, resilience) should be considered if the requirements source is lacking these cyber requirements, as all digital acquisitions are susceptible to some cyber threats. Traceability and models should trace the cyber requirements through decomposition as with all other requirements.*

***Expectation: (Added)(AFMC)Implied or derived requirements for certifications and integrity programs should be considered and match the identified certifications and integrity programs specified in Sections 2.6 and 2.7.***

***Expectation:*** *System safety engineering principles and analyses are part of all requirements development. Brief justification should be provided if system safety engineering principles and analyses are not part of a requirement.*

**CLASSIFICATION**



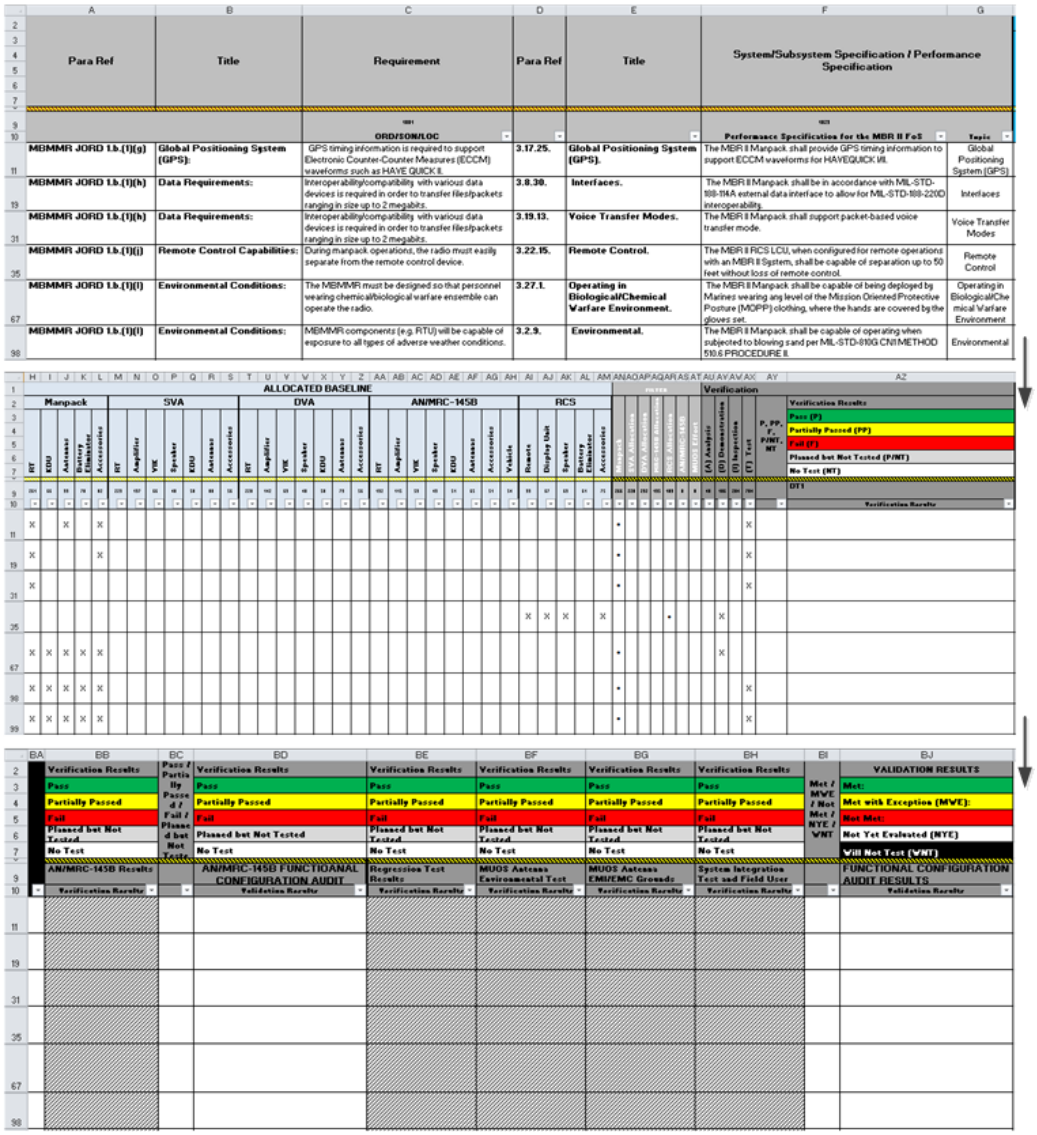

**Source: Name Year if applicable.** **CLASSIFICATION**

**Figure 2-1 Specification Tree Illustrating Requirements Decomposition and Technical Baselines (mandatory) (sample)**

***Expectation:*** *Program should trace all requirements from the highest level (JCIDS, **(Added)(AFMC) Certifications or integrity programs or equivalent requirements sources**) to the lowest level (e.g., component specification or user story). This traceability should be captured and maintained in digital requirements management tools or within model(s). The system Requirements Traceability Matrix (RTM) should be a model output that can be embedded in or attached to the SEP, or the SEP should contain a tool reference location. This matrix will grow as the system matures. The matrix should include the verification method for each of the identified requirements. Table 2.1-1 shows a sample RTM. If applicable, provide a link to a location where the current RTM is maintained that will meet the expectation for requirements traceability.*

***Expectation:*** *Program cyber requirements trace should also flow to the lowest level (e.g., component specification for passive sensing or user story for software automated resilience approaches). Use early and repeated or updated Mission-Based Cyber Risk Assessments (MBCRAs) supported by cyber test representatives (contractor and government) to inform cyber requirement flow down.* ***(Added)(AFMC) Requirements should trace to applicable certifications and integrity programs required by the program (reference Section 2.6 and 2.7 of this document). See (DAF) Systems Security Engineering Cyber Guidebook (SSECG), appendix C and D for requirements decomposition methodology.***

**Table 2.1-1 Requirements Traceability Matrix (mandatory) (sample)**



| Para Ref | Title | Requirement | Para Ref | Title | System/Subsystem Specification / Performance Specification | |
|---|---|---|---|---|---|---|
| | | ORD/SOW/LOC | | | Performance Specification for the MBR II FoS | Topic |
| MBMMR JORD t.b.(1)(g) | Global Positioning System (GPS): | GPS timing information is required to support Electronic Counter-Counter Measures (ECCM) waveforms such as HAVE QUICK II. | 3.17.25. | Global Positioning System (GPS). | The MBR II Manpack shall provide GPS timing information to support ECCM waveforms for HAVEQUICK I/II. | Global Positioning System (GPS) |
| MBMMR JORD t.b.(1)(h) | Data Requirements: | Interoperability/compatibility with various data devices is required in order to transfer files/packets ranging in size up to 2 megabits. | 3.8.30. | Interfaces. | The MBR II Manpack shall be in accordance with MIL-STD-188-184A external data interface to allow for MIL-STD-188-220D interoperability. | Interfaces |
| MBMMR JORD t.b.(1)(h) | Data Requirements: | Interoperability/compatibility with various data devices is required in order to transfer files/packets ranging in size up to 2 megabits. | 3.19.13. | Voice Transfer Modes. | The MBR II Manpack shall support packet-based voice transfer mode. | Voice Transfer Modes |
| MBMMR JORD t.b.(1)(j) | Remote Control Capabilities: | During manpack operations, the radio must easily separate from the remote control device. | 3.22.15. | Remote Control. | The MBR II RCS LCU, when configured for remote operations with an MBR II System, shall be capable of separation up to 50 feet without loss of remote control. | Remote Control |
| MBMMR JORD t.b.(1)(l) | Environmental Conditions: | The MBMMR must be designed so that personnel wearing chemical/biological warfare ensemble can operate the radio. | 3.27.1. | Operating in Biological/Chemical Warfare Environment. | The MBR II Manpack shall be capable of being deployed by Marines wearing ang level of the Mission Oriented Protective Posture (MOPP) clothing, where the hands are covered by the gloves set. | Operating in Biological/Chemical Warfare Environment |
| MBMMR JORD t.b.(1)(l) | Environmental Conditions: | MBMMR components (e.g. RTU) will be capable of exposure to all types of adverse weather conditions. | 3.2.9. | Environmental. | The MBR II Manpack shall be capable of operating when subjected to blowing sand per MIL-STD-810G CN1 METHOD 510.6 PROCEDURE II. | Environmental |

Source: Name Year if applicable. Classification: UNCLASSIFIED.

## 2.2 Architectures and Interface Control

Describe the architecture products, including the mandatory JCIDS architecture artifacts and any additional architecture views or diagrams, the program will develop. Explain how those mandatory architecture artifacts and additional architecture products are related to requirements definition or how they support other SE activities. (*See* SE Guidebook (forthcoming), Architecture Design Process, for additional guidance).

The LSE should have all interfaces (including temporary interfaces related to mission requirements) and dependencies clearly identified and accounted for in functional and physical architectures (including but not limited to mechanical, electrical, thermal, data, control,

procedural, and other interactions). (*See* SE Guidebook (forthcoming), Interface Management Process, for additional guidance). Include as appropriate the following:

- **(Added)(AFMC) List any Architecture Frameworks (e.g., the DoD Architecture Framework), tools and Reference Architectures used to develop architectural views and products.**
- List of the program's planned suite of architecture products with status of each.
- **(Added)(AFMC) Describe the storage locations, classification, or proprietary nature of architecture products (Cloud-based, on-premises, etc.) and how the products are accessed (via government office storage, or via access to contractor storage environments).**
- **(Added)(AFMC) (Links to the architecture products described in this Section of the SEP can replace the other bullets described in this Section as long as the links are accessible to all expected readers of the SEP).**
- Architecture diagrams and models (e.g., physical, functional, behavior model and software). (**Added)(AFMC) If digital twins are used, program office should define the type (e.g., Geometric, CAD/CAM to include manufacturing, Loads, Electrical Load).**
- All hardware-defined modular system interfaces that define shared boundaries between the major system platform and major system components, modular systems, or both, residing within that platform; or between those major system components, modular systems, or both, and between major system platforms (e.g., Interface Control Documents (ICDs), Interface Requirements Specification (IRS), Interface Design Description (IDD), and functional descriptions of software-defined interfaces conveying semantic meaning of interface elements (e.g., the function of a given interface field)).
- All software-defined modular system interfaces that define interface syntax and properties specifically governing how values are validly passed and received between major subsystems and components in machine-readable format and a machine-readable definition of the relationship among the delivered interface and existing common standards or interface repositories (e.g., Application Program Interfaces (API), Dynamic Link Libraries (DLL).
- The contractor's Software Architecture Description
- List of major external system (outside the authority/control of the program) interfaces (attach or embed separate ICD).
- List of modular system interfaces with the interface requirement specifications necessary for system operation, interface standards and standards profiles, and other documentation that fully describe the physical and functional interfaces needed to ensure compatibility between interfacing components, systems, and platforms.
- List and reference of all program Component-specific, joint, and coalition mission threads (JMT and CMT). (Department of Defense Acquisition Framework (DoDAF CV-6 (Capability to Operational Activities Mapping) provides list of JMTs).
- Consistent with the program's acquisition strategy and Life Cycle Sustainment Plan, the level(s) of indenture of the WBS (see section 3.1.3.1) and Software Architecture Description (see section 3.2.3.2) for specific modular systems and major system components into which functionality will be partitioned in discrete, cohesive, and self-contained units.

***Expectation:*** *Architectures are generated to describe and understand the system and how the subsystems join together, including internal and external interfaces (e.g., human-machine interactions, role-based access), to form the system and also to inform interoperability and cyber testing.*

### 2.3 Specialty Engineering

Provide a summary of the program approach for the integration of Specialty Engineering (SpENG) disciplines (e.g., Reliability and Maintainability, Manufacturing and Quality, Human Systems Integration (HSI), and System Safety) throughout systems engineering planning (e.g., requirements, schedule, staffing, Technical Performance Measures (TPMs), and technical reviews and activities) (DoDI 5000.88, Para 3.4.a.(3).(t)). Summarize critical elements of the SpENG sections in 3.2. Technical Tracking. **(Added)(AFMC) Describe the toolset and models used to support Specialty Engineering (HSI, R&M, Safety, etc.).**

### 2.4 Modeling Strategy

Define the modeling strategy to be used (model-supported, model-integrated, or model-centric). **(Added)(AFMC) The model strategy should follow the definitions outlined in the Acquisition Guidance and Key Digital Engineering Features spreadsheets found on the DAF Digital Guide (https://usaf.dps.mil/teams/afmcde/SitePages/Model-based-Contract-Language.aspx). The model-integrated term outlined by OSD is undefined, so the DAF will instead use the term model-collaborative which is outlined as part of the acquisition guidance contained within the Digital Guide site.**

| Model-Supported | Model-Collaborative | Model-Centric |
|---|---|---|
| **An acquisition approach where models may be used to support various engineering activities including the production of key documents for contractual purposes** | **An acquisition approach where models form part of the contractual artifacts, but only as secondary or complementary artifacts (with the capability to generate required documentation or model views).** | **An acquisition approach where models are primary artifacts (with the capability to generate required documentation or views).** |

Describe why the modeling strategy was chosen. Describe basic model components. **(Added)(AFMC) As part of the program's digital engineering approach, describe how models, simulations, the digital ecosystem, and digital artifacts will be used as part of an integrated approach to supporting Engineering activities and deliverables. The Air Force has been using the term Integrated Digital Environment in place of the OSD term digital ecosystem, so for the rest of this document the terms will be used synonymously.**

**(Added)(AFMC) Describe the Integrated Digital Environment (IDE). An IDE is a compilation of data, models, and tools for collaboration, analysis, and visualization across all functional domains. The IDE includes the methodology and specification for data, models, and tools arrangement with processes and procedures to exploit informational results. The IDE description should include information about the storage type for the IDE (Cloud-based, High Performance Computing Environment, or on-premises environment) as well as a mapping of the tools required to support the**

**modeling strategy. The IDE tool chain should maintain specifications and documentation in digital form that were historically contained in paper documents. The Program may also be working with a Contractor who manages a Contractor IDE. This section should define different levels of IDE (e.g., Government provided, Contractor hosted, or integrated Government and Contractor). Figure 2.4-1 shows a notional scenario that compares a Contractor IDE with the Program Office IDE including consideration for an IDE that spans multiple classification levels. Figure 2.4-2 shows a notional mapping of tools supporting various program functional areas.**

**(Added)(AFMC) Provide details for Integrated Digital Environment access controls. Describe roles and associated access permissions, e.g., reviewing officials who may require access only during milestone review activities, technical review team members who require only temporary access to the IDE when conducting independent reviews. Include for these types of events whether information will be pulled from the IDE and provided to outside officials or made available to outside officials via direct access to the IDE.**

**(Added)(AFMC) Identify tools to be used for modeling, design, build, test, automation, maintaining Authoritative Source of Truth (ASoT), cyber security and survivability. Describe access and license attributes: proprietary, COTS, needs on multiple classification levels, government owned, government purchased contractor maintained etc. Include Developer, licensing requirements, version(s), COTS v GOTS, date of first implementation, which org own/maintains, sunsetting date (if known); notate proprietary or outdated formats. Identify tools under development or not in a stable configuration.**

**(Added)(AFMC) Describe the storage locations of architecture products (Cloud-based, on-premises, etc.) and how the products are accessed (via government office storage, or via access to contractor storage environments). Describe the permissions/approvals and software licenses required for accessing and using these architecture products.**

**(Added)(AFMC) Identify the style guide that will be used for Model Based Systems Engineering (MBSE).**

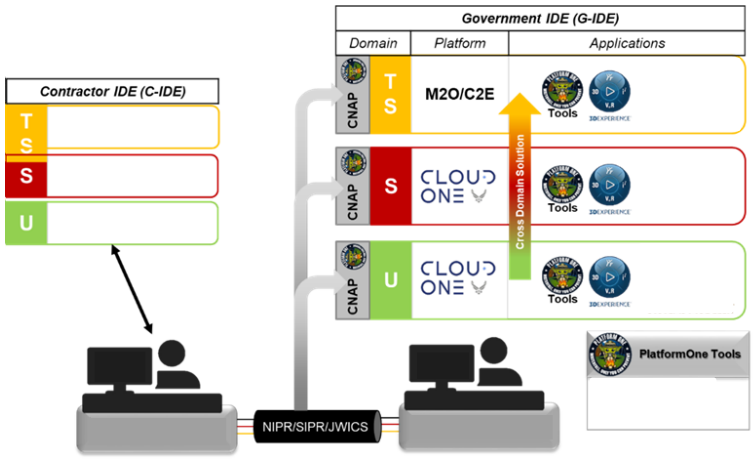



**Figure 2-2 (Added)(AFMC) Relationship Between Government and Contractor IDEs**

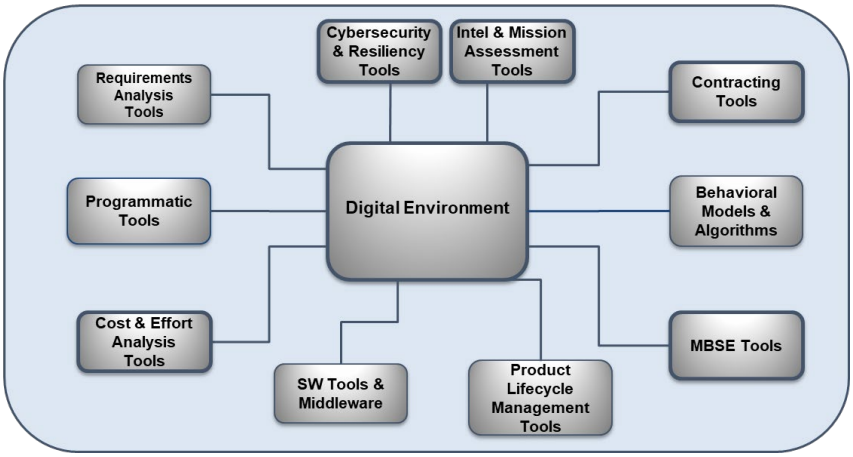



**Figure 2-3 (Added)(AFMC) An Exemplar IDE Showing Associated Tools**

## 2.5 Design Considerations

As shown in Table 2.5-1, identify the design considerations that are critical to achieving the program's technical requirements. Ensure the design and architectural factors from DoDI 5000.88 are addressed. If additional documentation is required, those documents may need to be embedded/attached in the SEP or located within the program's **(Added)(AFMC) IDE**. (*See* SE Guidebook (forthcoming), Design Considerations, for a partial list of design considerations.) Not all are equally relevant or critical to a given program, but all should be examined for relevance.

**Table 2.5-1 Design Considerations (mandatory) (sample)**

| Mapping Key Design Considerations into Contracts | | | | | |
|---|---|---|---|---|---|
| **Name (Reference)** | **Cognizant PMO Org** | **Certification** | **Documentation (embedded or reference attached)** | **Contractual Requirements (CDRL #)** | **Describe how the program captures, integrates, and uses technology, models, simulations and data to support life cycle activities within the program's (Added)(AFMC) IDE** |
| Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability | | | | | Describe how the design incorporates the CBRN survivability requirements and how progress toward these requirements is tracked and documented over the life cycle.<br>For additional information on CBRN Survivability, *see* https://www.dodtechipedia.mil/dodwiki/display/techipedia/Chemical%2C+Biological%2C+Radiological%2C+and+Nuclear+Survivability (Defense Technical Information Center (DTIC) account required). |
| Modular Open Systems Approach (MOSA) | | | List of applicable MOSA/Interface Standards and Reference Architectures \| | | Describe how the program uses MOSA in the system design to enable affordable change, evolutionary acquisition, and interoperability. Describe how the system design considers the evolution of requirements identified in the capability documents. Describe how the architectural design accommodates the requirements. Provide rationale if MOSA is not feasible or cost-effective. List known key interfaces (with identification of spec), |

| Mapping Key Design Considerations into Contracts | | | | | |
|---|---|---|---|---|---|
| **Name (Reference)** | **Cognizant PMO Org** | **Certification** | **Documentation (embedded or reference attached)** | **Contractual Requirements (CDRL #)** | **Describe how the program captures, integrates, and uses technology, models, simulations and data to support life cycle activities within the program's (Added)(AFMC) IDE** |
| | | | | | known/desired severable modules and modular system interfaces. Name MOSA-related controlling or guiding reference architectures and standards. |
| Digital Ecosystem<br>**(Added)(AFMC) AKA Integrated Digital Environment** | | | | | **(Added)(AFMC) Describe the Configuration Management techniques used in the IDE (If not defined in the Configuration Management Plan).**<br>Describe how the program uses the information in the IDE in the system's design of life cycle activities to establish system performance validation capability through models, simulations, or digital twin instantiations. Describe how the IDE will be maintained through the sustainment phase of the system to facilitate enhancements, updates, and changes.<br>Describe how the **(Added)(AFMC) IDE (e.g., software tools, plugins, environments)** or parts of it will be required to stay updated and maintained in order to support quick software updates and fast delivery to the field. Identify design products (e.g., digital threads, digital twin) and the program plans used to support development activities, manufacturing activities, operations, and sustainment activities. |
| **(Added)(AFMC) Product Life Cycle Management** | | | | | **Product Life Cycle Management is the process of managing the configuration of a product through an agile but disciplined approach that supports program offices' efforts to maintain operational safety,** |

| Mapping Key Design Considerations into Contracts | | | | | |
|---|---|---|---|---|---|
| **Name (Reference)** | **Cognizant PMO Org** | **Certification** | **Documentation (embedded or reference attached)** | **Contractual Requirements (CDRL #)** | **Describe how the program captures, integrates, and uses technology, models, simulations and data to support life cycle activities within the program's (Added)(AFMC) IDE** |
| | | | | | **suitability, and effectiveness (OSS&E) throughout the entire life cycle of the product. Describe what tools the program is using for Product Lifecycle Management (e.g., Teamcenter) and what capabilities (e.g., Hardware Bill of Materials, Software Bill of Materials, manufacturing Bill of Materials, Engineering Bill of Materials, as-maintained Bill of Materials, Engineering Technical Assistance Requests, Deficiency Reporting, Purchasing Requirement or Contract Data Management) the program is tracking in their PLM tool(s).**<br>***Keep in mind the SAF/AQ Product Life Cycle Management Enterprise Services Memorandum which requires a waiver if Teamcenter is not used.** |
| System Security Engineering | | | Program Protection Plan (PPP) | | Describe how the design addresses protection, survivability, and resilience of DoD warfighting capability from foreign intelligence collection; from hardware (HW), software (SW), and firmware (FW) vulnerabilities, cyberspace attacks, cyber events, and supply chain exploitation; and from battlefield loss throughout the system life cycle, balancing security requirements, designs, testing, sustainment activities, and risk management in the respective trade spaces. **(Added)(AFMC) Describe the tools used and security methodology (i.e., meta-data, tagging, digital forensics) associated with the program(s) IDE and countermeasures** |

| Mapping Key Design Considerations into Contracts | | | | | |
|---|---|---|---|---|---|
| **Name (Reference)** | **Cognizant PMO Org** | **Certification** | **Documentation (embedded or reference attached)** | **Contractual Requirements (CDRL #)** | **Describe how the program captures, integrates, and uses technology, models, simulations and data to support life cycle activities within the program's (Added)(AFMC) IDE** |
| | | | | | **applied to safeguard digital data relevant to design and cybersecurity resiliency.** |
| Diminishing Manufacturing Sources and Material Shortages (DMSMS) | | | DMSMS Management Contract Language | | Describe how the design seeks to exhibit DMSMS resiliency by both minimizing the occurrence of obsolescence and enabling quicker, lower cost resolutions when obsolescence does occur. Describe how the design is adapted to meet any contract requirement so the product will have no DMSMS issues for a specified period of time. Describe how the part selection process avoids items with projected near-term obsolescence. Describe how the program is conducting monitoring and surveillance to identify issues as early as possible as well as the processes the program uses to mitigate those issues by changing the design before production. **(Added)(AFMC) Describe how the use of tools in the IDE are leveraged for DMSMS activities and how those tools can/will be integrated into other government systems.** |
| Parts Management | | | Parts Management Contract language | | Describe how the program implements contracts for standardization and parts management to reduce the costly proliferation of parts and equipment; enhance reliability, availability and maintainability; and mitigate counterfeit and DMSMS occurrences in support of life cycle management and sustainability through integrated program planning and systems engineering throughout the acquisition life cycle. |

| Mapping Key Design Considerations into Contracts | | | | | |
|---|---|---|---|---|---|
| **Name (Reference)** | **Cognizant PMO Org** | **Certification** | **Documentation (embedded or reference attached)** | **Contractual Requirements (CDRL #)** | **Describe how the program captures, integrates, and uses technology, models, simulations and data to support life cycle activities within the program's (Added)(AFMC) IDE** |
| Intelligence | | | Life-Cycle Mission Data Plan (LMDP)<br>(MS A, Dev RFP Rel, B, & C)<br>(if program is Intelligence Mission Data (IMD) dependent)<br>Validated Online Lifecycle Threat (VOLT) Report | | Summarize the plans to identify IMD requirements and need dates. Describe how the program plans to address the risk of unavailable IMD. Also, describe how the design will address current and future threat capabilities, specifically highlighting what will be done to manage risk to system performance in the event of a Critical Intelligence Parameter (CIP) breach.<br>**(Added)(AFMC) (Expectation) Ensure that all projects, programs and studies are fully threat informed and able to accept agreed upon digital formats of threat data (both blue and red models, for example) in an integrated threat environment** |
| **(Added)(AFMC) Authoritative Data** | | | | | **Authoritative Data: Describe plans for developing configuration-controlled repositories to establish and maintain an authoritative source of truth for engineering data. Plan to make it accessible to the appropriate organizations. The authoritative source of truth will be the hub for all the models and data required for specific usages. List in the plan the models to be stored in this repository, which may include common reference models, model libraries, competency models, program office models, certification models, process models, knowledge models, and other models needed to** |

| Mapping Key Design Considerations into Contracts | | | | | |
|---|---|---|---|---|---|
| **Name (Reference)** | **Cognizant PMO Org** | **Certification** | **Documentation (embedded or reference attached)** | **Contractual Requirements (CDRL #)** | **Describe how the program captures, integrates, and uses technology, models, simulations and data to support life cycle activities within the program's (Added)(AFMC) IDE** |
| | | | | | **perform integrated engineering activities. Currently some Government-owned Repositories such as JEDMICS (or its follow on) are not cleared for classified data. Therefore, the Program Office must develop a plan on how it will maintain the Program's classified engineering data. The PM will develop a process to maintain classified data internally or may choose to contract with the Prime Contractor to store and maintain. The process should also consider the TEMP and how collected test data will use IDE pathways to update models for validation.** |

***Expectation**: SEP demonstrates necessary design considerations as an integral part of the design decision process, including trade study criteria.*

## 2.6 Technical Certifications

Summarize in table format (Table 2.6-1) the system-level technical certifications obtained during the program's life cycle. Review the following references and add and delete certifications to/from table 2.6-1 as applicable to your program. (*See* **(Added) (AFMC) DAFPAM** 63-128, Attachment 14, AFI 63-101/20-101). **(Added)(AFMC) Keep derived certifications in mind (e.g., Air Force Flight Standards Agency Primary Flight Reference certification is not called out in DAFPAM 63-128, but is required for Airworthiness certification).**

**Table 2.6-1 Certification Requirements (mandatory) (Added)(AFMC) This is a sample table refer to DAFPAM 63-128 and AFI 63-101/20-101 for a more complete listing of Technical Certifications. Programs can add columns to the table for additional items (e.g., requirement traceability, coordination with approval authority, or others as needed)**

| Certification | PMO Team/POC | Activities to Obtain Certification[1] | Certification Authority | (Added)(AFMC) Source / Requirement Guidance | Expected Certification Date |
|---|---|---|---|---|---|
| Airworthiness | Airframe Integrated Product Team (IPT) | **(Added)(AFMC) Complete Airworthiness Determination Form**<br>**(Added) Receive approved Certification Basis**<br>**(Added) Receive approved Compliance Report**<br>**(Added) Obtain Military Flight Release or Military Type Certificate** | **(Added)(AFMC) Technical Airworthiness Authority or Delegated Authority** | **(Added)(AFMC) AFPD 62-6**<br>**(Added)(AFMC) MIL-HDBK 516** | XQ FYXX |
| Joint Interoperability Test Command (JITC) | Systems Engineering Integration and Test (SEIT) | Operational test demonstrates the system:<br>• Is able to support military operations<br>• Is able to be entered and managed on the network<br>• Effectively exchanges information | JITC system interoperability test certification memorandum<br>**(Added)(AFMC) Point to reference, JITC OPERATIONAL TEST AND EVALUATION GUIDEBOOK VERSION 3.0 for guidance on activities to obtain accreditation.** | **(Added)(AFMC) AFI 17-140**<br>**(Added)(AFMC) CJCSI 6212.01F** | XQ FYXX |
| **(Added)(AFMC) Authorization to Operate (ATO)** | | **(Added)(AFMC) Program provides security authorization documentation to Authorization Official and receives an ATO based upon an agreed set of security control measures** | **(Added)(AFMC) Approved Authorization Official** | **(Added)(AFMC) DoDD 4630.5**<br>**(Added)(AFMC) DoDI 4630.8** | |

| Certification | PMO Team/POC | Activities to Obtain Certification[1] | Certification Authority | (Added)(AFMC) Source / Requirement Guidance | Expected Certification Date |
|---|---|---|---|---|---|
| Joint Weapons Safety Working Group | | Any weapon or laser systems used by two or more DoD components must be reviewed by the JWSWG | | **(Added)(AFMC) DoDI 5000.69** | |
| Transportability | | | | | XQ FYXX |
| Insensitive Munitions (IM) | Manufacturing IPT | Reference Document: Program Executive Office (PEO) IM Strategic Plan | | **(Added)(AFMC) DoDD 5000.01**<br>**(Added)(AFMC) CJCSI 5123.01** | XQ FYXX |
| Etc. | | | | | XQ FYXX |

[1] *Note:* This entry should be specific, such as a specification compliance matrix; test, inspection, or analysis; or a combination. It can also reference a document such as the Test and Evaluation Master Plan (TEMP) for more information.

***Expectation:*** *Program should include the plans for required technical certification activities and timing in the program Integrated Master Plan (IMP) and the Integrated Master Schedule (IMS).* ***(Added)(AFMC) Program should trace the certification to the requirement source that drives the need for the certification whenever possible.***

## 2.7 (Added)(AFMC) Integrity Programs

**(Added)(AFMC) Summarize in table format (Table 2.7-1) the system-level integrity Programs. Review the following references and add and delete certifications to/from table 2.7-1 as applicable to your program.**

**Table 2.7-1 (Added)(AFMC) Integrity Programs (sample)**

| Integrity Program | Source Requirement |
|---|---|
| **Aircraft Structural Integrity Program (ASIP)** | **AFI 63-140; Mil-Std 1530** |
| **Mechanical Equipment Systems Integrity Program (MECSIP)** | **Mil Std-1798** |
| **Propulsion Systems Integrity Program (PSIP)** | **Mil-Std-3024** |
| **Avionics Integrity Program (AVIP)** | **Mil Std-1796** |
| **Rotorcraft Structural Integrity Program** | **Mil-Std-3063** |

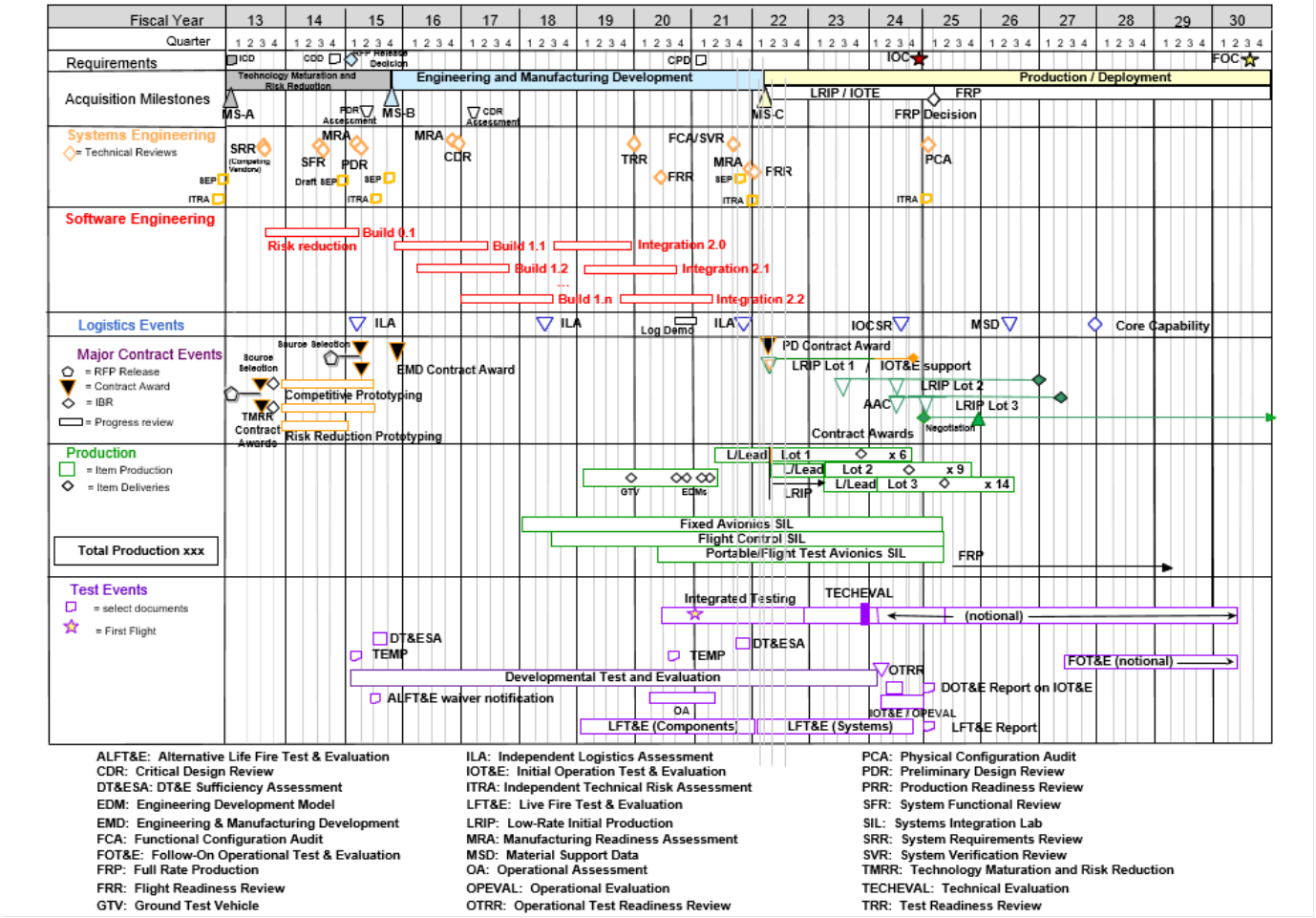
***(Added)(AFMC) Expectation: Program should trace the integrity program to the requirement source that drives the need for the integrity program whenever possible***

# 3 Program Technical Management

## 3.1 Technical Planning

### 3.1.1 Technical Schedule

- List scheduling/planning assumptions and describe schedule risk assessment methodology and frequency ((DoDI 5000.88, Para 3.4.a.(3).(e)).
- Describe how the IMP is maintained, where it is stored, and how to obtain access to it.
- Provide the current technical schedule derived from the IMP/IMS (Figure 3.1-1) for the program, including activities/tasks and event milestones such as:
    - SE technical reviews and audits
    - Program protection activities
    - Technology on/off-ramps
    - RFP release dates
    - SW builds/releases
    - Minimum Viable Product (MVP)/Minimum Viable Capability Release (MVCR)
    - Hardware/Software (HW/SW) Integration phases
    - Contract award (including bridge contracts)
    - Testing events/phases
    - System-level certifications
    - Technology Readiness Assessments (TRAs)
    - Manufacturing Readiness Assessments (MRAs)
    - Logistics/sustainment events
    - System Diminishing Manufacturing Sources and Material Shortages (DMSMS) health assessments
    - **(Added)(AFMC) Certification Requirements (i.e., ATO, SEEK EAGLE, Request for Frequency Allocation, etc.)**
    - 9Long-lead or advanced procurements
    - Technology development efforts to include prototyping
    - Production lot/phases
    - Need dates for government-furnished equipment (GFE) deliveries
    - HSI domain and management activities (e.g., HSI Plan, task analysis)
    - Production Readiness Reviews (PRRs)
    - Independent Technical Risk Assessments (ITRAs)
    - Developmental Test and Evaluation Sufficiency Assessments
    - Reliability growth testing
    - Key modeling activities
    - Model release dates
    - **(Added)(AFMC) Airworthiness activities (e.g., assessment, certification basis, compliance)**




Source: Name Year [if applicable]. Classification: UNCLASSIFIED.

**Figure 3-1 System Technical Schedule as of [Date] (mandatory) (sample)**

***Expectation:*** *Program should properly phase activities and key events (competitive and risk reduction prototyping, TRA, Preliminary Design Review (PDR), Critical Design Review (CDR), etc.) to ensure a strong basis for financial commitments. Program schedules are event driven and reflect adequate time for SE, integration, test, corrective actions, and contingencies. SEPs for approval should include a current schedule, no more than 3 months old.*

### 3.1.1.1 Schedule Management

- Provide a description of the program's IMP and IMS process, to include **(Added)(AFMC) what tools are used,** definitions, updated schedules, audits, baseline control, and the integration between program-level and contractor detailed schedules (DoDI 5000.88, Para 3.4.a.(3).(f)).
- Provide the program-level IMP as an attachment to the SEP.
- Discuss the relationship of the program's IMP to the contractor(s) IMS, how they are linked/interfaced, and what the primary data elements are.

- Identify who or what team (e.g., Integrated Product Team/Working Group (IPT/WG)) is responsible for developing the IMP, when it is required, and whether it is a part of the contract.
- Describe how identified technical risks are incorporated and tracked into the program's IMP, IMS, and **(Added)(AFMC) IDE, and are traced to requirements, certifications, integrity programs, and architecture**.
- If used, discuss how the program uses Earned Value Management (EVM) cost reporting to track/monitor the status of IMS execution and performance to plan.
- If EVM is not used, state how often and discuss how the IMS is tracked according to contract requirements and how performance is tracked to budget.
- Summarize the program's planned schedule risk analysis (SRA) products. Describe how each product will help determine the level of risk associated with various tasks, determine the readiness for technical reviews, and inform acquisition decisions. Identify who will perform SRAs, methodologies used, and periodicity.
- Discuss how often the program conducts Defense Contract Management Agency (DCMA) 14-point schedule health checks on the IMS (Earned Value Management System (EVMS) Program Analysis Pamphlet (PAP) (DCMA-EA PAM 200.1) October 2012: http://www.dcma.mil/LinkClick.aspx?fileticket=0CBjAarXWZA%3d&portalid=31).
- Describe the process to resolve/correct deficiencies identified by the DCMA health check.
- Describe the impact of schedule constraints and dependencies.
- Describe initiated, completed, or planned actions to mitigate schedule drivers.
- Describe the periodicity for performing critical path analysis, identifying items on the critical path with any risks and mitigations to meet schedule objectives.
- Describe how the PM will substantiate HW/SW schedule realism and the rigorous basis of estimate used to develop the detailed hardware/software activities.

***Expectation:*** *Program should regularly check IMS health and conduct SRAs to inform program decisions.*

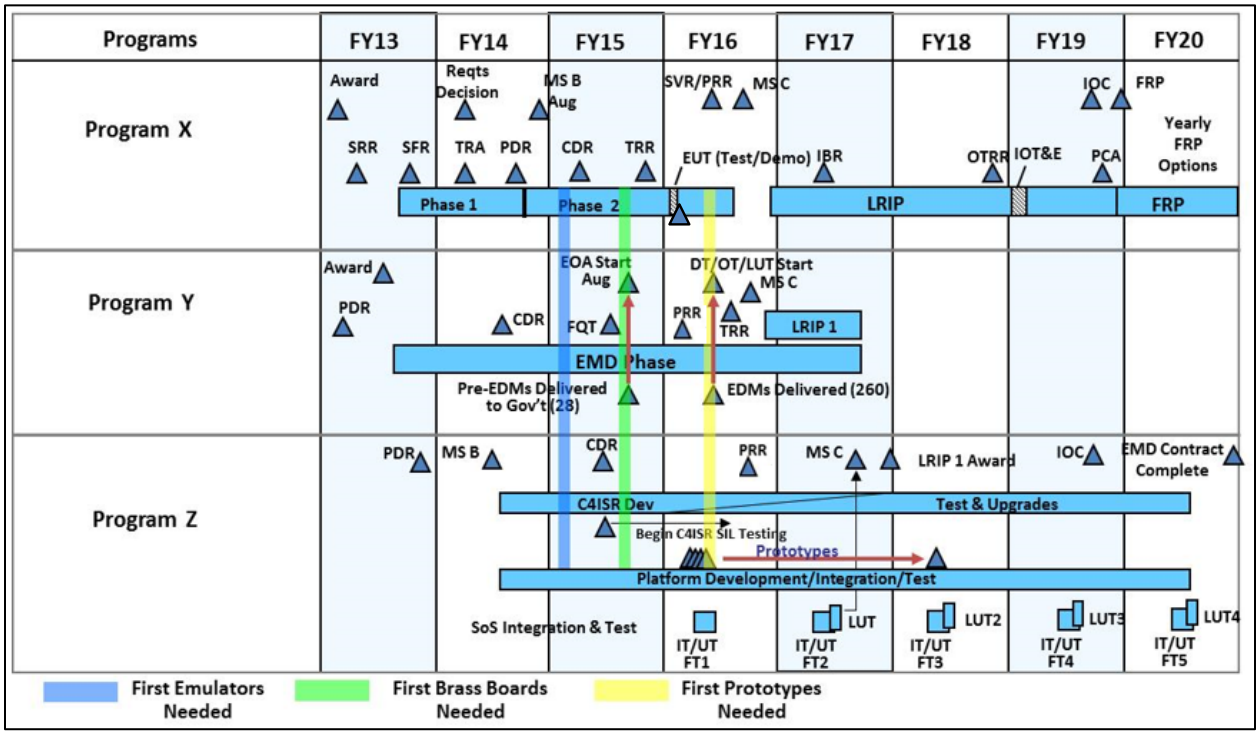
#### 3.1.1.2 Family of Systems/System of Systems Management

As part of the **(Added)(AFMC) IDE** implementation and within the ecosystem, describe the external organization integration plan. Identify the organization responsible for coordinating SE and ecosystem integration efforts associated with FoS/SoS and its authority to reallocate resources (funding and manpower). Describe methods used to document, facilitate, and manage interaction among SE team(s) and external-to-program government organizations (e.g., **(Added)(AFMC) partner Program Offices with shared interfaces,** OUSD(R&E) on technical tasks, activities, and responsibilities (e.g., requirements, technical baselines, and technical reviews). Address the following:

- Resolution of issues that cross PM, PEO, and Component lines **(Added)(AFMC) (e.g., planned development or sharing of digital twins, simulations, emulators, etc).**
- Digital engineering implementation and how it interfaces with new starts and legacy programs. Include how the **(Added)(AFMC) IDE** will be implemented to track and highlight integration issues within the program and with other programs (SoS)

- ICDs and any interface control WGs (ICWGs)
- "Triggers" that require a FoS/SoS member to inform the others if there is a cost, schedule, or performance deviation
- Description of who or what team (e.g., IPT/WG) is responsible for maintaining the alignment of the IMP and IMS across the interdependent programs
- Planned linkage between HW and SW upgrade programs within the FoS/SoS, to include modeling
- Any required GFE/government-furnished property/information (GFP/GFI) (e.g., test ranges, integration laboratories, and special equipment)
- Any major system components and modular system interfaces shared from or used by other programs (MOSA)

Include an SoS schedule (Figure 3.1-2) that shows FoS/SoS dependencies such as alignment of technical reviews, major milestones, test phases, GFE/GFP/GFI, etc.
*Note: If the system neither has nor will have any relationship with any external organization, the program may omit the content of 3.1.1.2 FoS/SoS Management and the associated Figure 3.1-2 SoS Schedule.*




Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3-2 System-of-Systems Schedule as of [Date] (mandatory) (sample)**

***Expectation:*** *Program should*

- *Manage the internal program schedule and synchronize it with external program schedules.*
- *Identify external interfaces and clearly define dependencies. This information should include interface control specifications or documents, which should be confirmed early on*

*and placed under strict configuration control. Compatibility with other interfacing systems and common architectures should be maintained throughout the development/design process.*

- *Identify any major system components, major system platforms, and modular system interfaces (MOSA) with dependencies clearly defined (DoDI 5000.88, Para 3.4.a.(3).(r)). This description should include all technical data and computer software (see Section 3.2.9) that will be delivered with appropriate IP rights.*
- *Develop Memorandums of Agreement with interfacing organizations that include:*
  - *Tripwires and notification to FoS/SoS members of any significant (nominally >10%) variance in cost, schedule, or performance*
  - *Mechanisms for FoS/SoS members to comment on proposed interface changes to include program's digital engineering implementation*
  - *Fast-track issue identification and resolution process*

### 3.1.2 Maturity Assessment Planning

Identify how the program will assess and document the technology maturity of all critical technologies and manufacturing processes consistent with the USD(R&E) guidance for technology readiness and Manufacturing Readiness Level (MRL) assessments. Identify the test results, including any early cyber testing and artifacts that have been conducted or are planned, that provide the documentation of the technology and manufacturing process maturity.

***Expectation**: Programs will develop all critical technologies consistent with the USD(R&E) guidance for assessing technology readiness and MRL and document the maturity of those critical technologies and manufacturing processes. This documentation will be made available to support Office of the Secretary of Defense (OSD)- and Service-conducted reviews and assessments.*

### 3.1.3 Technical Structure and Organization

#### 3.1.3.1 Work Breakdown Structure

If a WBS exists, embed or attach it to the SEP. In addition, provide:

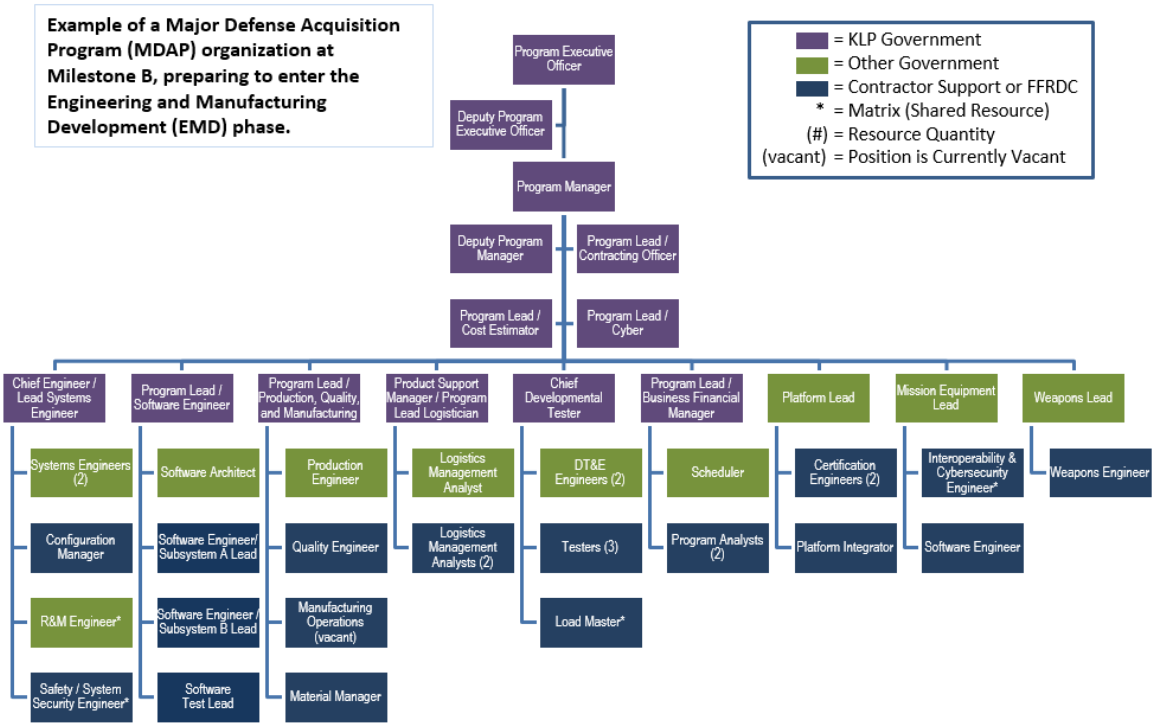
- WBS dictionary that is traceable from the IMS
- **(Added)(AFMC) Traceability of the WBS to other model data (e.g., drawings, specifications, requirements)**
- Explanation of the traceability between the system's technical requirements and the WBS
- (Optional) A digital ecosystem support IPT that is resourced or is part of the SEIT IPT or LSE/CE

#### 3.1.3.2 Government Program Office Organization

Provide the planned program office organizational structure (i.e., wiring diagram to illustrate hierarchy and identify any positions that are not filled) with an as-of date, and include the following elements (Figure 3.1-3):

- Organization to which the program office reports
- PM

- LSE/CE
- Functional Leads (e.g., test and evaluation (T&E), logistics, DMSMS, risk, production/quality, reliability, SW, **(Added)(AFMC) IDE**, system safety).




FFRDC: Federally Funded Research and Development Center; KLP: Key Leadership Position

Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3-3 Program Office Organization as of [Date] (mandatory) (sample)**

### 3.1.3.3 Program Office Technical Staffing Levels

Summarize the program's technical staffing plan, to include:

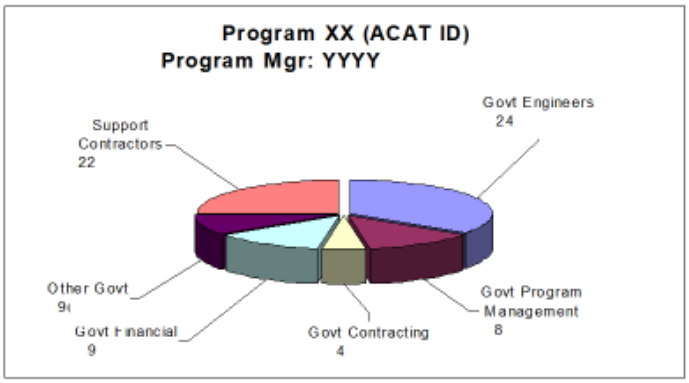
- Risks and increased demands on existing resources if staffing requirements are not met
- A figure (e.g., sand chart, Figure 3.1-4) to show the number of required PMO full-time equivalent (FTE) positions (e.g., organic, matrix support, and contractor support) over time, by key program events (e.g., milestones and technical reviews)
- Description of the basis of estimate for the staffing sand chart
- A figure to show the program's budget for SE and program management (SEPM) over time as a percentage of total program budget (Figure 3.1-5)
- Description of the adequacy of SW development staffing resources
    - Describe the key PMO and contractor SWE position experience and qualification requirements (e.g., quantity and experience level).
- Description of the adequacy of staffing resources for the **(Added)(AFMC) IDE**

- Describe the key **(Added)(AFMC) IDE** position experience to include the skill set, experience and qualification requirements applicable for MBSE, simulation, software engineering (SWE), and information technology positions (e.g., quantity and experience level).

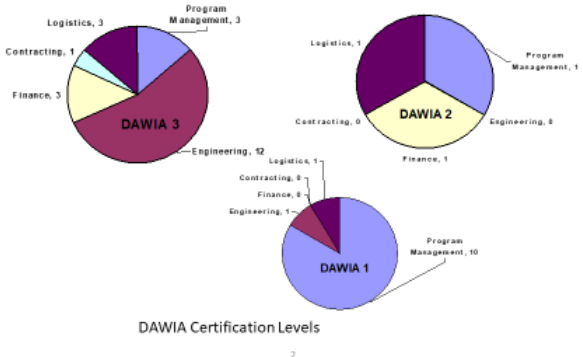
- For programs still under competition, the approaches used to manage flow of information in the competitive environment
- Description of the adequacy of cyber engineering development staffing resources
  - The key PMO and contractor cyber engineering position experience and qualification requirements (e.g., quantity and experience level), to include adversarial testing
- Description of the adequacy of system safety staffing resources

***Expectation:*** *Program should use a workload analysis tool to determine the adequate level of staffing, appropriate skill mix, and required amount of experience to properly staff, manage, and execute successfully.*

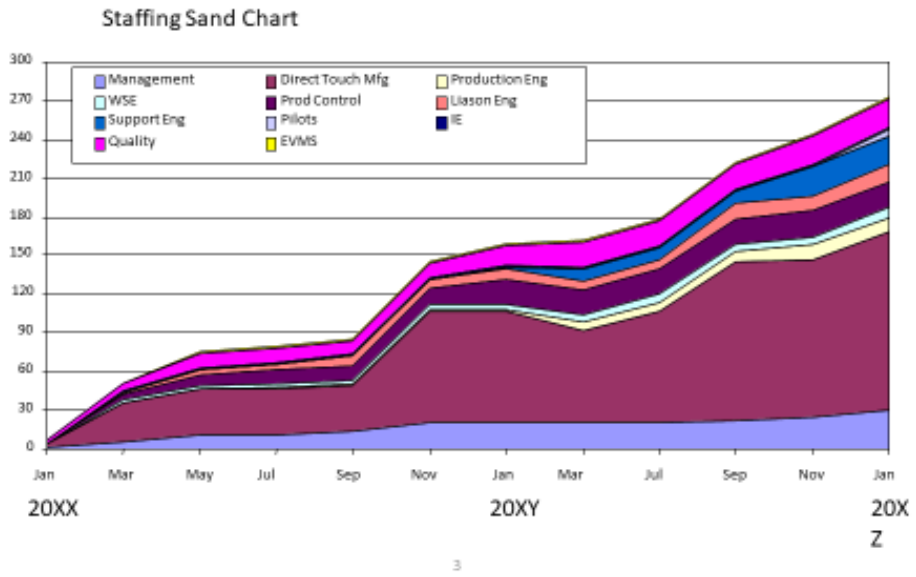
Technical Staffing- *Example*



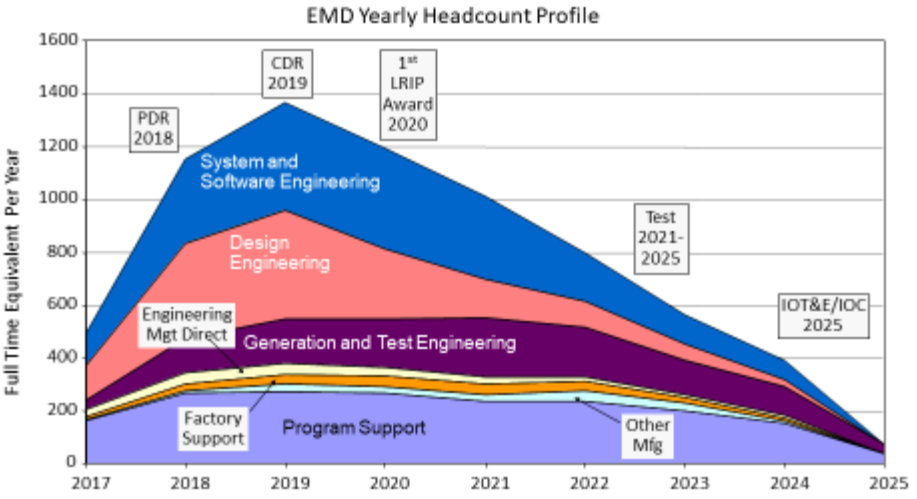

Technical Staffing- *Example*



Technical Staffing- *Example*

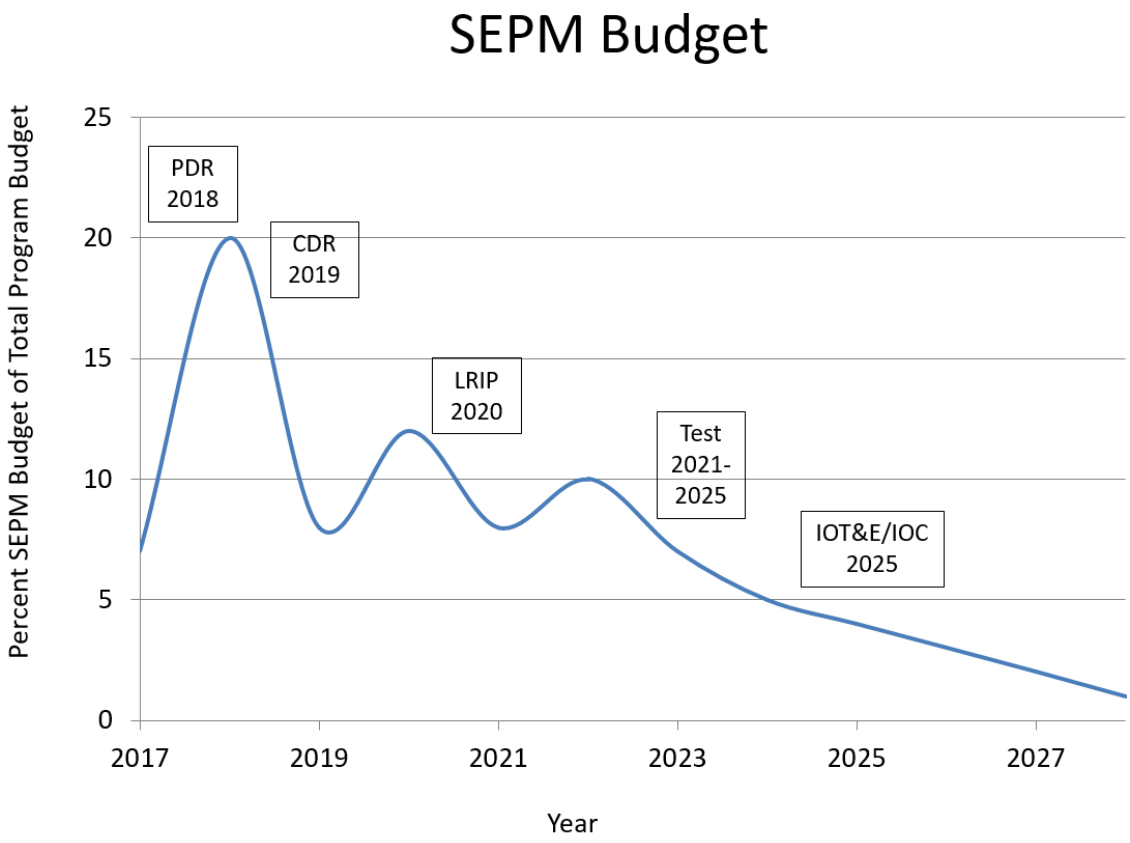



Contractor Team Staffing- *Example*




Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3-4 Program Technical Staffing (mandatory) (sample)**

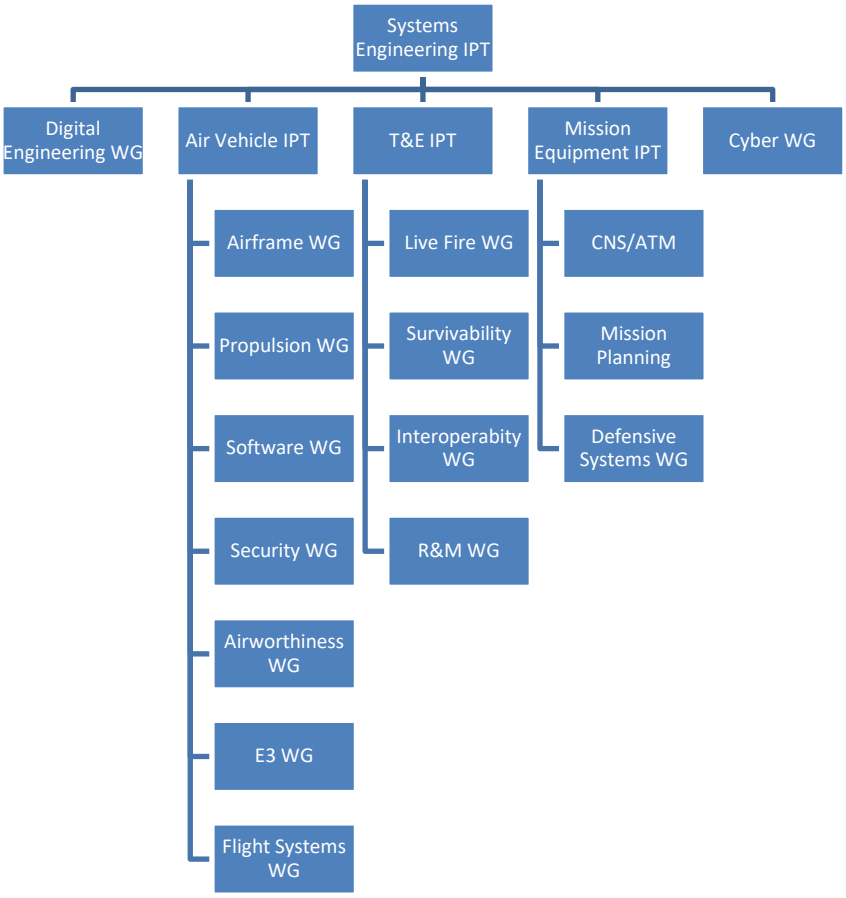



Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3-5 SEPM Budget (mandatory) (sample)**

### 3.1.3.4 Engineering Team Organization and Staffing

- **Integrated Product Team (IPT) Organization** – Provide diagrams that show the government and contractor (when available) IPTs and their associated working-level IPTs (WIPTs) and WGs that illustrate the hierarchy and relationship among them (Figure 3.1-6). Identify the government leadership for all teams.
- **IPT Details** – For government and contractor(s) (when available) IPTs and other key teams (e.g., Level 1 and 2 IPTs and WGs), include the following details either by attaching approved charters or in a table (Table 3.1-1, mandatory unless charters attached):
  - IPT name
  - Functional team membership (to include external program members, and representation from all SpENG disciplines (Section 2.3) and design consideration areas (Section 2.4))
  - IPT roles, responsibilities, and authorities
  - WBS tasks assigned to IPT
  - IPT products (e.g., updated baselines, risks, etc.)
  - IPT-specific TPMs and other metrics.




Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3-6 IPT/WG Hierarchy (mandatory) (sample)**

***Expectation:*** *Program should integrate SE activities with all appropriate functional and stakeholder organizations within the IDE. In addition, IPTs should include personnel responsible for each of the design consideration areas in Table 2.5-1. Note: Ensure the IPTs in Figure 3.1-6 match the IPTs in Table 3.1-1.*

**Table 3.1-1 Integrated Product Team Details (mandatory unless charters are submitted) (sample)**

| Team Name | Chair | Team Membership (Function or Organization) | Team Role, Responsibility, and Authority | Products and Metrics |
|---|---|---|---|---|
| SE IPT | Lead SE | • Program Office<br>  ○ Platform Lead<br>  ○ Mission Equipment Lead<br>  ○ Weapons Lead<br>  ○ Test Lead<br>  ○ Logistics Manager<br>  ○ DMSMS Lead<br>  ○ SW Lead<br>  ○ Production/Quality Manager<br>  ○ System Safety Lead<br>  ○ Interoperability Lead<br>  ○ R&M Lead<br>  ○ System Security Engineering Lead<br>  ○ Cyber Lead<br>  ○ **(Added)(AFMC) Configuration Management Lead**<br>  ○ **(Added)(AFMC) Information Protection or Acquisition Security / Program Protection Lead**<br>• PEO and PM<br>• Service Representative<br>• OSD SE<br>• Key Subcontractor or Suppliers<br>• External programs<br>• Intelligence Lead<br>• Environmental Lead<br>• DCMA Engineers | Role: IPT Purpose (e.g., Aircraft Design and Development)<br><br>Responsibilities: Integrate all technical efforts throughout the life cycle within an end-to-end IDE<br>• Manage and oversee design activities<br>• Oversee configuration management of requirements and their traceability<br>• System Safety<br>• Manage specialty engineering activities including the following disciplines: survivability/vulnerability, human systems, integration, electromagnetic environmental effects (E3), reliability and maintainability (including availability), system security, and environmental impacts to system/subsystem performance<br>• Evaluate and mitigate counterfeit and DMSMS risk in design, production, and sustainment<br>• Manage safety and certification requirements<br>• Ensure compliance with applicable international, federal, state, and local environment, safety, and occupational health (ESOH) laws, regulations, and treaties<br>• Manage system manufacturing assessments, weight, and facilities management (System Integration Laboratory) planning<br>• Perform functional allocations and translate the system definition into WBS<br>• Ensure compliance with all specialty engineering specification requirements<br>• Support the Program Protection IPT and Program Protection System Engineering<br>• Manage SEIT performance through IDE, EVMS, TPMs, and other metrics and risk assessments | Products:<br>SEP/SEP updates<br>WBS, IMP/IMS input<br>Specifications<br>IDE Architecture and Design Description<br><br>Metrics tracked by IPT:<br>• Cost<br>• Performance<br>• Schedule<br>• Engineering Infrastructure and Environment Utilization and Performance Metrics |

| Team Name | Chair | Team Membership (Function or Organization) | Team Role, Responsibility, and Authority | Products and Metrics |
|---|---|---|---|---|
| | | | • Identify and communicate SEIT issues to leadership<br>• Evaluate technical and performance content and cost/schedule impacts to support the Configuration Control Board (CCB) process<br>• Support test plan development and execution<br>• Support the T&E IPT in system verification requirements<br>• Support the Product Support IPT WGs and other Technical Interchange Meetings (TIMs)<br>• Develop and support the SEIT part of the incremental development and technology refresh processes<br>• Support Program Management Reviews (PMRs)<br>• Support program technical reviews and audits<br>• Perform SEIT trade studies to support affordability goals/caps<br>• Perform FAR mandatory engineering surveillance<br>• Ensure minimum essential data is acquired and managed.<br><br>Schedule and frequency of meetings<br><br>Date of signed IPT charter and signatory | |

| Team Name | Chair | Team Membership (Function or Organization) | Team Role, Responsibility, and Authority | Products and Metrics |
|---|---|---|---|---|
| XXX IPT | XXX Lead | • Program Office<br>○ Lead SE<br>○ **(Added)(AFMC) Digital Engineering Lead**<br>○ Mission Equipment Lead<br>○ Weapons Lead<br>○ Test Manager<br>○ Logistics Manager<br>○ DMSMS lead<br>○ SW Lead<br>○ R&M Lead<br>○ Production/Quality Manager<br>○ Safety Lead<br>○ System Security Lead<br>○ Interoperability Rep.<br>○ Key Subcontractor or Suppliers<br>○ **(Added)(AFMC) Information Protection or Acquisition Security / Program Protection Lead** | Role: IPT Purpose<br><br>Responsibilities: Integrate all technical efforts<br>• Team member responsibilities<br>• Cost, performance, schedule goals<br>• Scope, boundaries of IPT responsibilities<br><br>Schedule and frequency of meetings<br><br>Date of signed IPT charter and signatory | Products:<br>• Specification input<br>• SEP input<br>• TEMP input<br>• DMP input<br>• AS input<br><br>Metrics tracked by IPT:<br>• TPM 1<br>• TPM 2 |

CCB: DMP: Data Management Program; FAR: Federal Acquisition Regulation; IPT: Integrated Product Team; SEP: Systems Engineering Plan; TEMP: Test and Evaluation Master Plan; TPM: Technical Performance Measure; etc.....

## 3.2 Technical Tracking

### 3.2.1 (Added) (AFMC) Deficiency Reporting

**(Added)(AFMC) Summarize the program's process in which deficiency reports are tracked to resolution. Per AFI 63-101/20-101 paragraph 5.2.2.8.3 this process should be documented "in the Systems Engineering Plan no later than Milestone C."**

- **(Added)(AFMC) For deficiency reporting guidance refer to T.O. 00-35D-54, USAF Deficiency Reporting, Investigation, and Resolution (DRI&R).**

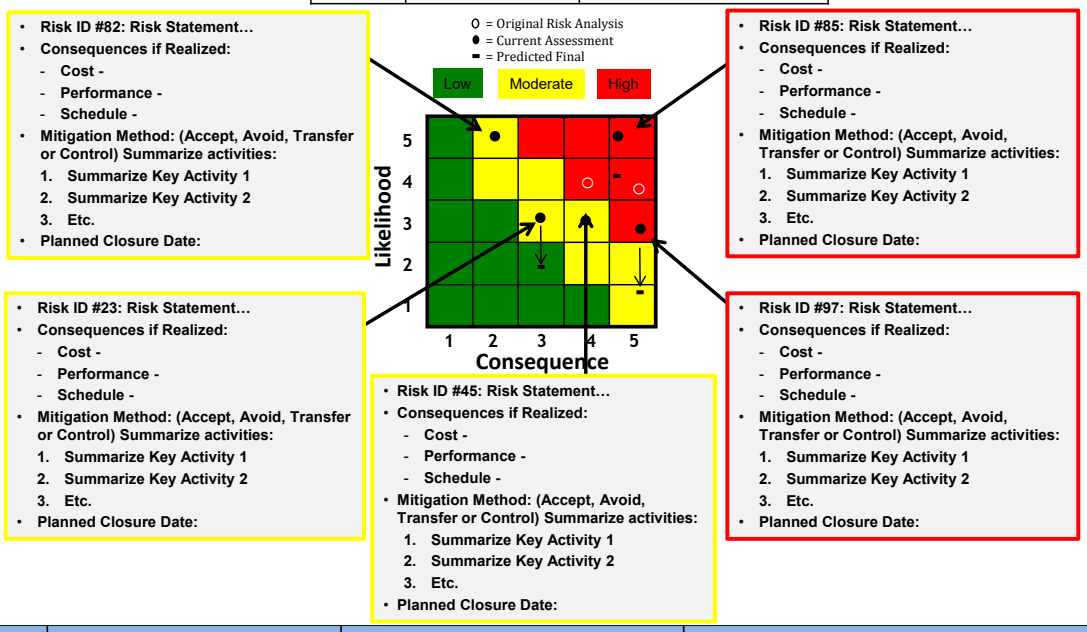
### 3.2.2 Technical Risk, Issue, and Opportunity Management

- **Technical Risk, Issue, and Opportunity (RIO) Management Process Diagrams**
  - Embed or attach to the SEP the latest (no more than 3 months old) RIO management document including an as-of date.
- **Risk Management Roles**
  - Determine roles, responsibilities, and authorities within the risk management process for the following:
    - Reporting/identifying risks or issues
    - Criteria used to determine whether a "risk" submitted for consideration becomes a risk or not (typically, criteria for likelihood and consequence)
    - Adding/modifying risks
    - Changing likelihood and consequence of a risk
    - Closing/retiring a risk or issue
  - If Risk Review Boards or Risk Management Boards are part of the process, identify the chair and participants and state how often they meet.
  - State how the process will be implemented using the IDE and digital artifacts, establishing the risk ASoT while maximizing automated reporting, seamless access, and accuracy of risk status.
- **Risk/Issue Management**
  - Risk Tools – Describe the risk management and tracking tools the program office and contractor(s) will use. If the program office and contractor(s) use different risk tools, describe how information will be transferred or integrated without loss. *Note: In general, the same tool should be used. If the contractor's tool is acceptable, the government may opt to use it but must have direct, networked access to the tool.*
  - Technical Risk and Mitigation Planning – Summarize the key engineering, integration, technology, SpENG, and unique SW risks and planned mitigation measures for each risk (DoDI 5000.88, Para 3.4.a.(3).(q)).
  - Risk Reporting – Provide a risk reporting matrix (Figure 3.2-1) or a list of the current system-level technical risks and issues with:
    - As-of date
    - Risk rating

- Risk statement and consequences, if realized
- Mitigation activities and expected closure date.

System Safety Risks can also be mapped on the risk cube and reporting matrix in Figure 3.2-1. However, the process for risk burn down shown in Figure 3.2-2 depends on the process to attain acceptance by the System Safety Risk Assessment Authority or mitigation through system safety design order of precedence.

| Level | Likelihood | Probability of Occurrence |
|---|---|---|
| 5 | Near Certainty | > 80% to ≤ 99% |
| 4 | Highly Likely | > 60% to ≤ 80% |
| 3 | Likely | > 40% to ≤ 60% |
| 2 | Low Likelihood | > 20% to ≤ 40% |
| 1 | Not Likely | > 1% to ≤ 20% |




| Level | Cost | Schedule | Performance |
|---|---|---|---|
| 5 Critical Impact | 10% or greater increase over APB objective values for RDT&E, PAUC, or APUC<br><br>Cost increase causes program to exceed affordability caps | Schedule slip will require a major schedule rebaselining<br><br>Precludes program from meeting its APB schedule threshold dates | Degradation precludes system from meeting a KPP or key technical/supportability threshold; will jeopardize program success [2]<br><br>Unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP) |
| 4 Significant Impact | 5% - <10% increase over APB objective values for RDT&E, PAUC, or APUC<br><br>Costs exceed life cycle ownership cost KSA | Schedule deviations will slip program to within 2 months of approved APB threshold schedule date<br><br>Schedule slip puts funding at risk<br><br>Fielding of capability to operational units delayed by more than 6 months[1] | Degradation impairs ability to meet a KSA.[2] Technical design or supportability margin exhausted in key areas<br><br>Significant performance impact affecting System-of System interdependencies. Work-arounds required to meet mission objectives |
| 3 Moderate Impact | 1% - <5% increase over APB objective values for RDT&E, PAUC, or APUC<br><br>Manageable with PEO or Service assistance | Can meet APB objective schedule dates, but other non-APB key events (e.g., SETRs or other Tier 1 Schedule events) may slip<br><br>Schedule slip impacts synchronization with interdependent programs by greater than 2 months | Unable to meet lower tier attributes, TPMs, or CTPs<br><br>Design or supportability margins reduced<br><br>Minor performance impact affecting System-of System interdependencies. Work-arounds required to achieve mission tasks |
| 2 Minor Impact | Costs that drive unit production cost (e.g., APUC) increase of <1% over budget<br><br>Cost increase, but can be managed internally | Some schedule slip, but can meet APB objective dates and non-APB key event dates | Reduced technical performance or supportability; can be tolerated with little impact on program objectives<br><br>Design margins reduced, within trade space [2] |
| 1 Minimal Impact | Minimal impact. Costs expected to meet approved funding levels | Minimal schedule impact | Minimal consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires |

Source: Name Year if applicable. Classification: UNCLASSIFIED.

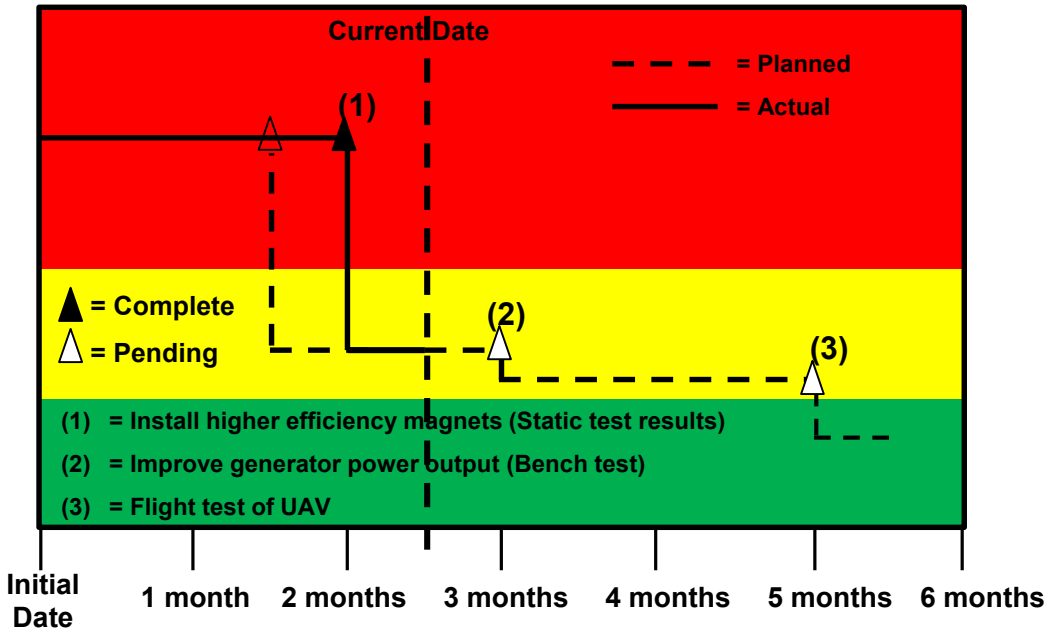
**Figure 3-7 Risk Reporting Matrix as of [Date] (mandatory) (sample)**

(*Note:* Include an as-of date – time-sensitive figure.)

- **Risk Burn-Down**
  - Describe the program's use of risk burn-down plan to show how the program should implement mitigation activities to control and retire risks. Also discuss how activities are

linked to TPMs and to the project schedule for critical tasks. For each high technical risk, provide the risk burn-down plan. (Figure 3.2-2 contains a sample risk burn-down plan.)

***Expectation:*** *Program should use hierarchical boards to address risks and integrates risk systems with contractors. The approach to identify risks is both top-down and bottom-up. Risks related to technology maturation, internal and external integration, modeling, and each design consideration indicated in Table 2.5-1 are considered in risk identification. SEPs submitted for approval contain a current, updated Risk Reporting Matrix and associated Risk Burn-Down plan for high technical risks. Reporting risk artifacts should be auto generated from within the IDE at any time depicting the real-time status and should be accessible by all program personnel.*




Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3-8 Risk Burn-Down Plan as of [Date] (mandatory for high risks; others optional) (sample)**

- **Opportunity Management** – Discuss the program's opportunity management plans to create, identify, model, analyze, plan, implement, and track initiatives (including technology investment planning and pollution prevention projects) that can yield improvements in the program's cost, schedule, or performance baseline through reallocation of resources.
  - If applicable, insert a chart or table that depicts the opportunities being pursued, and summarize the cost/benefit analysis and expected closure dates (Table 3.2-1).
  - Address opportunities that would mitigate system safety risks and improve return on investment.

**Table 3.2-1 Opportunity Register (if applicable) (sample)**

| Opportunity | | | Return on Investment | | | Owner | |
|---|---|---|---|---|---|---|---|

| | Likeli-hood | Cost to Implement | Monetary | | | Schedule | Performance | System Safety Impact | Program Priority | Management Strategy | | Expected Closure |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | RDT&E | Procurement | O&M | | | | | | | |
| Opportunity 1: Procure Smith rotor blades instead of Jones rotor blades. | Mod | $3.2M | | | $4M | 3-month margin | 4% greater lift | | #2 | Reevaluate; summarize the plan | Mr. Bill Moran | March 2017 |
| Opportunity 2: Summarize the opportunity activity. | Mod | $350K | $25K | | $375K | | | | #3 | Reject | Ms. Dana Turner | N/A |
| Opportunity 3: Summarize the opportunity activity. | High | $211K | | $0.04M | $3.6M | 4 months less long-lead time needed | | | #1 | Summarize the plan to realize the opportunity | Ms. Kim Johnson | January 2017 |

### 3.2.3 Technical Performance Measures

Summarize the program's strategy for selecting the set of measures for tracking and reporting the maturation of system development, design, and production. TPMs are carefully chosen, and their values collected over time for the purpose of seeing trends and forecasting program progress to plan. TPMs provide the ability for the PM, LSE, and senior decision makers to (1) gain quantifiable insight to technical progress, trends, and risks; (2) empirically forecast the impact on program cost, schedule, and performance; and (3) provide measurable feedback of changes made to program planning or execution to mitigate potentially unfavorable outcomes. TPMs are metrics that show how well a system is satisfying its requirements or meeting its goals. TPMs for cyber survivability and operational resilience should be defined. TPMs should not repeat Critical Risks, KPPs, Key System Attributes (KSAs), or Critical Technical Parameters (CTPs) but should trace to them. As the system matures, the program should add, update, or delete TPMs documented in the SEP.
(*See* SE Guidebook (forthcoming), Technical Assessment Process, for category definitions and additional guidance.) This section should include:

- An overview of the measurement planning and selection process, including the approach to monitor execution to the established plan, and identification of roles, responsibilities, and authorities for this process
- A set of TPMs covering a broad range of core categories, rationale for tracking, intermediate goals, and the plan to achieve them with as-of dates (Table 3.2-2.)
- SE leading indicators to provide insight into the system technical maturation relative to a baseline plan
- The maturation strategy, assumptions, reporting methodology, and maturation plans for each metric with each performance metric traced to system requirements and mission capability characteristics
- The program's process and documentation approach for adding or deleting TPMs and any changes to the TPM goals
- Whether any contractual provisions relate to meeting TPM goals or objectives
- Description of how models, simulations, the IDE, and digital artifacts will be used to support TPM tracking and reporting.

- Description of the traceability among KPPs; KSAs; key technical risks and identified TPMs; CTPs (listed in the TEMP); Critical Program Information (CPI); threats associated with the program's Critical Intelligence Parameters (CIPs) (identified by Service Intelligence); vulnerabilities (listed in the Program Protection Plan (PPP)); or other measures:
    - Identify how each KPP and KSA is covered by a TPM. If not, explain why a KPP or KSA is not covered by a TPM.
    - Identify how the achievement of each CTP is covered by a TPM. If not, explain why a CTP is not covered by a TPM.
    - Identify planned manufacturing measures, appropriate to the program phase, to track manufacturing readiness performance to plan.
    - Identify SW measures for SW technical performance, process, progress, and quality (e.g., Table 3.2-2, Appendix C – Agile and Development, Security and Operations (DevSecOps) Software Development Metrics).
    - Identify what threat information is being used and if a Validated Online Lifecycle Threat (VOLT) from Service intelligence was used. The VOLT should be used and reviewed by the engineering team and provided to the prime contractor. If a VOLT is not being used, explain why.
    - Indicate what CIPs have been defined for any threat-sensitive requirements per the JCIDS Manual. Identify how CIP breach(es) affect TPM(s).

Table 3.2-2 provides examples of TPMs in each of 15 core categories. The table includes examples of each, with intermediate goals as a best practice for effective technical management (DoDI 5000.88, Para 3.4.a.(3).(g)).

**Table 3.2-1 Technical Performance Measures (mandatory) (sample)**

| Technical Performance Measure | TPM Category | Responsible IPT | Requirement Trace KPP(s),KSA(s), CTP(s) | TPM Goal | Plan / Actual | SRR Status | SFR Status | PDR Status | MS B Status | CDR Status | SVR/FCA Status | MS C Status | FRP Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mean Time Between Operational Mission Failure (MTBOMF) | Reliability, Maintainability, Availability | R&M | KSA (Reliability) | >45 | Plan | 36 | 36 | 37 | 38 | 40 | 45 | 47 | 50 |
| | | | | | Actual | 33 | 34 | 35 | 37 | | | | |
| Operating Weight (lb.) | System Performance | Air Vehicle | KPP (Effective Time on Station) | <99,000 | Plan | 98,999 | 98,999 | 98,000 | 95,000 | 85,540 | 85,540 | 85,540 | 85,650 |
| | | | | | Actual | 97,001 | 97,001 | 102,950 | 97,001 | | | | |
| Interface Definition - External ICDs Planned vs. Actual | Mission Integration Management | Configuration Management | Specification (% ICDs approved vs. planned) | 100% | Plan | 0 | 0 | 10 | 20 | 40 | 95 | 98 | 99 |
| | | | | | Actual | 0 | 0 | 15 | 20 | | | | |
| Time to perform mission-critical function | Mission (End to End) Performance | Mission Systems | KPP (Time to perform critical functions-sec) | <15s | Plan | 25 | 25 | 25 | 23 | 20 | 15 | 15 | 15 |
| | | | | | Actual | 25 | 25 | 25 | 25 | | | | |
| Risk-based supply chain, design, SWA, system function, component, part-level protection measures | System Security | Mission Systems | KSA (% IA detected and prevented) | >99.5% | Plan | 85 | 90 | 90 | 95 | 95 | 99.5 | 99.5 | 99.5 |
| | | | | | Actual | 80 | 81 | 86 | 92 | | | | |
| First pass yield (FPY) (%) | Manufacturing Quality | Manufacturing | Specification (% of 1st pass acceptance) | >=0.95 | Plan | | | | | | 0.95 | 0.96 | 0.97 |
| | | | | | Actual | | | | | | | | |
| Parts Delivery Performance | Manufacturing Management | Manufacturing | Specification (% of parts accepted) | >=98% | Plan | | | | | 95% | 97% | 98% | 99% |
| | | | | | Actual | | | | | | | | |
| Schedule Deviation | Schedule Management | System Engineering | Specification (% critical path variance) | <=5 | Plan | 5.3 | 5.3 | 5.3 | 5 | 5 | 5 | 5 | 5 |
| | | | | | Actual | 8 | 7 | 6.5 | 5.5 | | | | |
| | | | | | Plan | 5.5 | 5.5 | 5.5 | 5 | 5 | 5 | 5 | 5 |

| Technical Performance Measure | TPM Category | Responsible IPT | Requirement Trace KPP(s),KSA(s), CTP(s) | TPM Goal | Plan / Actual | SRR Status | SFR Status | PDR Status | MS B Status | CDR Status | SVR/FCA Status | MS C Status | FRP Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Government Staffing Deviation | Staffing and Personnel Management | System Engineering | Specification (% variance plan vs. filled) | <=5 | Actual | 6.5 | 6.5 | 7 | 5.2 | | | | |
| Average Production Unit Cost (APUC) | Resource Management | Cost | KSA (APUC) ($) | <150M | Plan | 170 | 170 | 170 | 167 | 160 | 155 | 150 | 150 |
| | | | | | Actual | 175 | 180 | 175 | 170 | | | | |
| Average % Requirements Change per Month | Requirements Management | System Engineering | KPP/CTP (Design Control and Stability) | 0% | Plan | 35 | 30 | 25 | 17 | 2 | 0 | 0 | 0 |
| | | | | | Actual | 33 | 29 | 26 | 24 | | | | |
| Software Size | Software Engineering | Software | Metric (e.g., SLOC, ESLOC, Story Points, Function Points) (% Estimating Uncertainty) | n/a | Plan | 500 FP | 500 FP | 500 FP | 500 FP | 500 FP | 500 FP | 500 FP | 500 FP |
| | | | | | Actual | 250 @ 70% | 350 @ 75% | 460 @ 80% | 480 @ 85% | | | | |
| Software Schedule / Duration | Software Schedule | Software | Metric (Project phase, e.g., Rqmts, High-level and Detailed Design, Code and Unit Test, Integration, System Test) (# months) (% Schedule Definition) | n/a | Plan | 70 | 70 | 80 | 90 | 95 | 100 | 100 | 100 |
| | | | | | Actual | 70 @ 70% | 70 @ 75% | 80 @ 80% | 95 @ 90% | | | | |
| Software Staffing | Software Resources | Software | Metric (Full-time Equivalent) | n/a | Plan | 70 | 90 | 100 | 110 | 110 | 80 | 70 | 50 |
| | | | | | Actual | 60 | 88 | 99 | 110 | | | | |
| Effort | Software Engineering | Software | Metric (Hours) (% Estimating Uncertainty) | n/a | Plan | 80 | 80 | 95 | 100 | 100 | 100 | 100 | 100 |
| | | | | | Actual | 75 @ 65% | 70 @ 75% | 90 @ 80% | 105 @ 90% | 110 @ 95% | | | |
| Software Defects | Software Quality | Software | Metric (Open critical Priority 1 and 2 defects, optionally by CSCI) | 0 | Plan | n/a | n/a | n/a | 20 | 10 | 0 | 0 | 0 |
| | | | | | Actual | n/a | n/a | n/a | 21 | 15 | 6 | 2 | 0 |
| Phase Containment | Software Quality | Software | Metric (Phase Defect originated vs Phase Defect found; %) | T: 0.8 O: 1.0 | Plan | 0.8 | 0.8 | 0.8 | 0.8 | 0.8 | 0.8 | 0.8 | 0.8 |
| | | | | | Actual | 37% | 45% | 65% | 85% | 77% | 95% | 100% | 100% |
| | | | | | Plan | 15 | 15 | 10 | 10 | 5 | 5 | 5 | 5 |

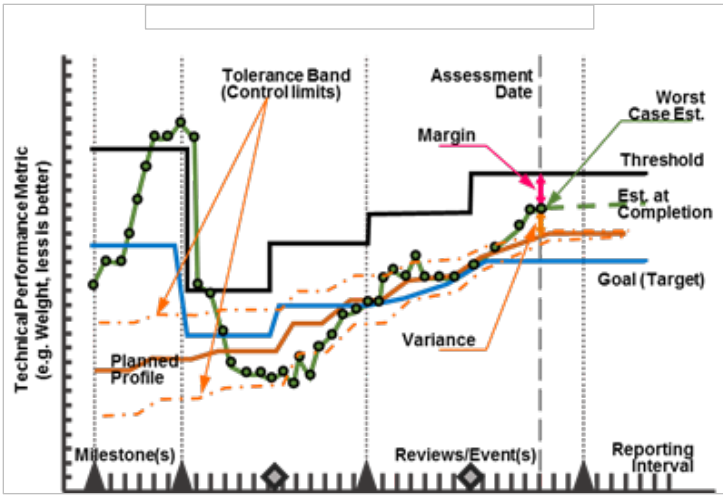
| Technical Performance Measure | TPM Category | Responsible IPT | Requirement Trace KPP(s),KSA(s), CTP(s) | TPM Goal | Plan / Actual | SRR Status | SFR Status | PDR Status | MS B Status | CDR Status | SVR/FCA Status | MS C Status | FRP Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Risk Management | Risk Management | System Engineering | KSA/Specification (% of risks that become issues) | <10% | Actual | 12 | 14 | 12 | 15 | | | | |
| Requirements Verification - % verified | Test Management | System Engineering | CTP (% verified requirements) | 99.99% | Plan | 0 | 0 | 10 | 20 | 40 | 95 | 98 | 99 |
| | | | | | Actual | 0 | 0 | 15 | 20 | | | | |
| Operational Resilience | System Performance | CyWG | Specification – verify system performance related TPMs with cyber effects as informed by MBCRA | 100 | | | | | | | | | |
| Cyber Survivability | Cyber Survivability | CyWG | KPP (as per 10 Cyber Survivability Attributes) | 100 | | | | | | | | | |

CyWG: Cyber Working Group

Source: Name Year if applicable. Classification: UNCLASSIFIED
Legend (Defined by program as example below.)
Green: Meets or exceeds plan value with positive consequence
Yellow: Within 5% of meeting plan value at milestones before MS C with negative; consequence
Red: Greater than 5% of meeting plan value with negative consequence and any failure to meet plan at MS C and beyond

***Expectation:*** *Program should use measures to report progress and keep stakeholders informed. These measures form the basis to assess current program status for milestone decisions, technical reviews and audits, risk management boards, contract incentives, and actions. Reporting measurement artifacts should be auto generated from within the IDE at any time depicting the real-time status and should be accessible by all program personnel.*

Figure 3.2-3 depicts the characteristics of a properly defined and monitored TPM to provide early detection or prediction of problems that require management action.

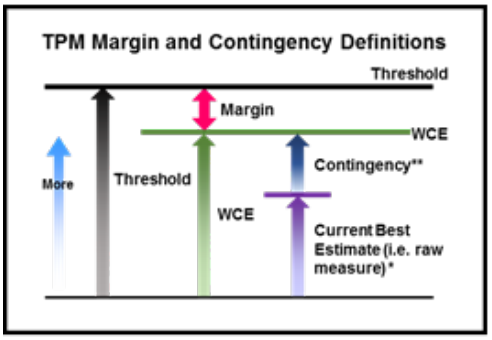



| | |
|---|---|
| **Worst Case Estimate** | (WCE) Measured or estimated progress to be compared with planned progress. WCE accounts for contingency (see below) |
| **Estimate at Completion** | Forecasted WCE value of a TPM at designated completion |
| **Planned profile** | Time phased expected values (based on prior experience) |
| **Tolerance Band** | Management control limits representing projected level of error or control within the process |
| **Goal (Target)** | Desired objective profile values; Usually set to allow design trade space between Goal and Threshold |
| **Threshold** | Limiting acceptable profile values, usually the required or specified values |
| **Variance** | Difference between the Planned Profile and WCE |
| **Margin** | Difference between the WCE and Threshold value |

Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3-9 Technical Performance Measure or Metric Graph (recommended) (sample)**

Figure 3.2-4 depicts the relationship among Contingency, Current Best Estimate, Worst Case Estimate, Threshold, and Margin, as well as example criteria for how contingency changes as the system/testing matures.




* Current Best Estimate value is the raw estimate of the metric determined either by prediction, analysis, direct measurement, and/or bottoms-up estimation without consideration for error.
** Contingency accounts for the uncertainty in estimation and immaturity of the item being measured.

**Example guidelines to allocate Contingency to each estimated measure to account for uncertainty**

| Basis for Current Best Estimate Value | | | Contingency |
|---|---|---|---|
| **Maturity of item/process being measured** | **Estimating Technique** | **Estimating Technique (alternate)** | **Uncertainty to be included in the WCE** |
| Paper Design | Analysis, legacy similarity | Guess | 15% |
| Roll-up of Component-level items | Extrapolated tests, Bottom-up models | Analysis | 10% |
| Integrated model / prototype | Integration lab demo | Modeling | 7% |
| Test article | Representative test | Demo | 4% |
| Final article | End-to-end test in real environment (e.g., OT&E) | Test | 0% |

For a data collection point determine the worst case (largest contingency) associated with the applicable item maturity or estimating technique. Apply that contingency percentage to the current best estimate to arrive at the WCE for that collection interval. An example is highlighted: A representative test is done with a roll-up of components. This results in a worst case Contingency of 10%, resulting in: WCE = CBE +10%

Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3-10 TPM Contingency Definitions**

### 3.2.4 Reliability and Maintainability Engineering

#### 3.2.4.1 Reliability and Maintainability Requirements and Engineering Activities

Describe how the program implements and contracts for a comprehensive Reliability and Maintainability (R&M) engineering program to include phased activities (listed in Table 3.2-3), and how R&M integrates with the SE processes. **(Added)(AFMC) Describe how reliability requirements are traced to certifications and integrity programs.** Describe how the JCIDS R&M thresholds were translated into contract specification requirements (listed in Table 3.2-4). (*See* https://ac.cto.mil/rme/)

**Table 3.2-3 Planning and Timing for R&M Activities (mandatory) (sample)**

| Activity | Planning and Timing |
|---|---|
| R&M Allocations | ***Expectation:*** *R&M requirements assigned to individual items to attain desired system-level performance. Preliminary allocations by System Functional Review (SFR) with final by PDR.* |
| R&M Block Diagrams | ***Expectation:*** *Block diagrams and math models to reflect the equipment/system configuration. Preliminary by SFR with final by PDR.* |
| R&M Predictions | ***Expectation:*** *Predictions to provide an evaluation of the proposed design or for comparison of alternative designs. Preliminary by PDR with final by CDR.* |
| Failure Definition and Scoring Criteria | ***Expectation:*** *Failure definitions and scoring criteria to make assessments of R&M contract requirements.* |
| Failure Mode, Effects, and Criticality Analysis (FMECA) | ***Expectation:*** *Analyses to assess the severity of the effects of component/subsystem failures on performance. Preliminary by PDR with final by CDR.* |
| Maintainability and Built-In Test Demonstrations | ***Expectation:*** *Assessment of the quantitative and qualitative maintainability and built-in test characteristics of the design.* |
| Reliability Growth Testing at the System and Subsystem Level | ***Expectation:*** *Reliability testing of development systems to identify failure modes, which if uncorrected could cause the equipment to exhibit unacceptable levels of reliability performance during operational usage. At the system level, assessments of development test data provide measures of effectiveness for the R&M engineering program and are used to track progress on reliability growth planning curves. At the subsystem level ALT and HALT (qualitative to eliminate failure modes) may be used.* |
| Failure Reporting, Analysis, and Corrective Action System (FRACAS) | ***Expectation:*** *Engineering activity during development, production, and sustainment to provide management visibility and control to improve R&M of HW and associated SW. Requires timely and disciplined use of failure data to generate and implement effective corrective actions to prevent a recurring failure.* |

**Table 3.2-4 R&M Requirements (mandatory) (sample)**

| Reliability and Maintainability Requirements | | |
|---|---|---|
| Parameter | JCIDS Threshold | Contract Specification Requirement |
| Reliability (e.g., MTBF) | | |
| Maintainability (e.g., MTTR) | | |

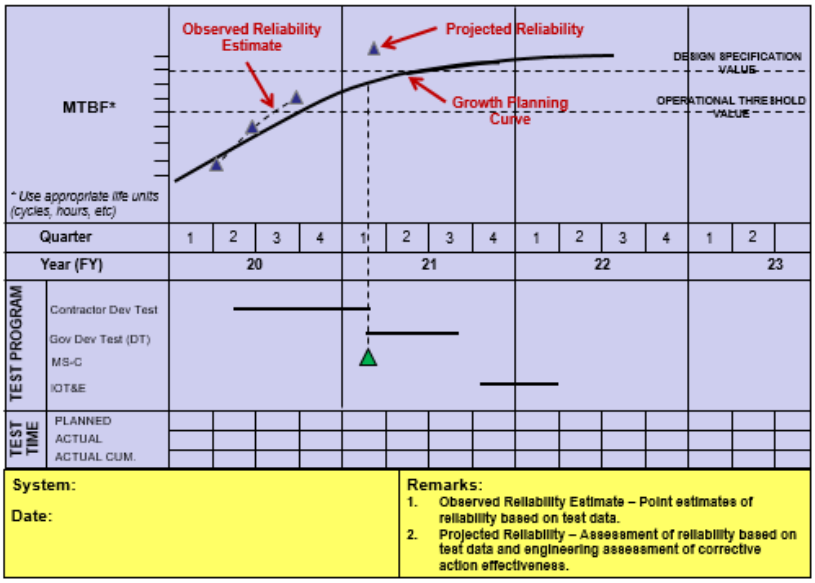
***Expectation:*** *(1) R&M activities and requirements are consistent with the level of design knowledge that makes up each technical baseline (see SE Guidebook (forthcoming), Reliability and Maintainability Engineering, and the Engineering of Defense Systems Guidebook for R&M guidance by acquisition phase). (2) For Major Defense Acquisition Programs (MDAPs), document the trades among reliability, downtime (includes maintainability), operational availability (AO), and Operations and Support (O&S) cost in the RAM-C Rationale Report and attach the report to the SEP (see https://ac.cto.mil/rme/ for annotated outline guidance and training). (3) In accordance with Section 2443 of Title 10, U.S.C., for ACAT I (MDAPs) and II (Major Systems) weapon system designs, include in the contract and in the process for source selection clearly defined and measurable R&M requirements and engineering activities. Consider including incentive fees and penalties (as appropriate) in all Engineering and Manufacturing Development and production solicitations and contracts to promote achieving*

*R&M design specification requirements. (4) Space programs should address Mission Assurance (MA) planning in accordance with the Mission Assurance Guide (see Aerospace Corporation TOR-2007(8546)-6018 REV. B, section 10.6.3, Risk Management (http://aerospace.wpengine.netdna-cdn.com/wp-content/uploads/2015/05/Mission-Assurance-Guide-TOR-20078546-6018-REV-B.pdf)).*

#### 3.2.4.2 Reliability Growth Planning

Summarize the program reliability growth strategy along with assumptions, planning factors, and planned assessment tools and methods. Provide a Reliability Growth Curve (RGC), Figure 3.2-5 using as reference Mil-HDBK-189C (DoDI 5000.88, Para 3.4.a.(3).(i)).

***Expectation:*** *RGCs are used to plan, illustrate, and report progress as part of Defense Acquisition Executive Summary reviews. Growth curves are stated in a series of intermediate goals and tracked through fully integrated, system-level T&E events until the system achieves the reliability threshold. Growth planning curves are consistent with and align to test events and the IMS. If a single curve is not adequate to describe overall system reliability, provide curves for critical subsystems with the rationale for selecting them.*




Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3.2-5 Reliability Growth Curve (mandatory) (sample)**

### 3.2.5 Manufacturing and Quality Engineering

#### 3.2.5.1 Manufacturing and Quality Requirements and Engineering Activities

Describe the program approach for implementing and contracting for comprehensive manufacturing and quality (M&Q) programs, and how M&Q integrates with the SE processes, to include planning and timing for key activities (listed in Table 3.2-5). (*See* https://ac.cto.mil/maq/)

**Table 3.2-5 Planning and Timing for M&Q Activities and Requirements (mandatory) (sample)**

| Activity or Requirement | Planning and Timing |
|---|---|
| Manufacturing Management | ***Expectation:*** *Updates at each Milestone (example references may include MIL-HDBK-896, "Manufacturing Management Program Guide," SAE Standard AS6500, "Manufacturing Management Program," and* |

| Activity or Requirement | Planning and Timing |
|---|---|
| | *FAA certified production system IAW 14 CFR Part 21, Certification Procedures for Products and Parts).* |
| Industrial Capabilities Assessment | ***Expectation:** Updates at each Milestone (10 USC 2440).* |
| Technical Reviews and Audits | ***Expectation:** Manufacturing inputs for each review and audit (SE Guidebook (forthcoming)).* |
| Producibility Analysis | ***Expectation:** Describe approach (e.g., MIIL-HDBK-727 or NAVSO P-3678 best practices).* |
| Production Readiness Reviews (PRRs) | ***Expectation:** PRR at system, subsystem, and component levels for prime and subcontractor (SE Guidebook (forthcoming)).* |
| Supplier Qualifications | ***Expectation:** Description of approach (e.g., risk assessment, First Article Test/Inspection, audits, counterfeit parts mitigation).* |
| Statistical Process Control (SPC) | ***Expectation:** Applicable manufacturing processes are under SPC.* |
| Quality Management and Assurance | ***Expectation:** Updates for each phase of the program (example references may include applicable standards such as ISO 9100 and SAE AS9100 Quality Management Systems).* |
| Contractor Oversight | ***Expectation:** Description of DCMA role to include quality oversight delegated to DCMA.* |
| **(Added)(AFMC) Key and Critical Characteristics** | ***(Added)(AFMC) Expectation: Description of approach requiring the contractor and design-responsible suppliers to identify (including callouts on manufacturing drawings) and manage Key and Critical Characteristics throughout the design and production phases. (example references may include MIL-HDBK-896, SAE Standard AS6500)*** |

### 3.2.5.2 Manufacturing Maturity

Describe the program approach to (1) assess manufacturing readiness as the program prepares to enter technical reviews and program milestones; and (2) Manufacturing Maturation Plans for MRL threads that are assessed below the target MRL criteria (refer to the DoD Manufacturing Readiness Level Deskbook *www.dodmrl.com*).
Results are summarized as reflected in Table 3.2-6 structure.

**Table 3.2-6 Summary of MRA Results (mandatory) (sample)**

| Component, Subsystem, System Assessed | Assessment Description (Describe process, thread, or risk area from MRL Criteria) | Assessed MRLs | | | |
|---|---|---|---|---|---|
| | | PDR Entry (Target MRL ≥ 6 | CDR Entry (Target MRL ≥ 7) | LRIP (Target MRL ≥ 8) | FRP (Target MRL ≥ 9) |
| | | | | | |
| | | | | | |

### 3.2.6 Human Systems Integration

Describe the program approach for implementing and contracting for a comprehensive HSI program and how HSI integrates with SE processes **(Added)(AFMC) (e.g., how tools training is used early to identify HSI concerns)**, to include planning and timing for key activities (listed in table 3.2-7): (1) Defining the role of the human in the Concept of Operations (CONOPS); (2) Incorporating effective human-system interfaces; (3) Achieving required levels of human performance; (4) Making economical demands upon resources, skills, and training; (5) Managing program products to accommodate the characteristics of the user population that will operate, maintain, train with, and support the system; and (6) Managing the risk of loss, injury, or damage to personnel or equipment (*see* HSI Guidebook and DoDD 5000.01, *The Defense*

*Acquisition System*). Describe how HSI thresholds were translated into contract specification requirements (listed in table3.2-8). (See: https://ac.cto.mil/hsi/)

**Table 3.2-7 Planning and Timing for HSI Activities and Requirements (sample)**

| Activity or Requirement | Planning and Timing |
|---|---|
| HSI Plan | ***Expectation (Milestones and Full-Rate Production (FRP)):*** *HSI program is implemented early in the acquisition process. Program and system human-centered design considerations and readiness risks are addressed through trade-off analyses for human factors engineering, personnel, habitability, manpower, training, safety and occupational health, and force protection and survivability. Program describes the approach in the HSI Plan (e.g., 5000.PR).* |
| Human Engineering Design Approach Document (HEDAD)-Operator / HEDAD-Maintainer | ***Expectation (Milestones and FRP):*** *Human limitations are accounted for through human factors engineering (example references may include MIL-STD-1472 and MIL-STD-46855 when addressing HFE-related requirements and concerns).* |
| Task analysis / User workflow | ***Expectation:*** *The level of interaction and severity of interactions by the human component (e.g., human error) with the system (e.g., hardware, software) are defined and determined when conducting failure definitions and FRACAS activities.* |
| Usability evaluations | ***Expectation:*** *User assessments of prototype design models or physical systems emphasize system operation and sustainment. Program applies user feedback early and iteratively to improve usability, maintainability, and supportability in the design. UCD approaches are formulated and leveraged.* |
| M&S activities for human performance / Workload analyses | ***Expectation:*** *User needs are identified, communicated, and visualized under defined operational conditions, expected mission threads, and use cases. Software is evaluated for identified HSI and domain-level impacts to ensure software is user-friendly, requires minimal training, and informs other trade-off analyses. Workload and other human-related issues are addressed, tested, and mitigated as early in the life cycle as possible.* |

**Table 3.2-8 HSI Requirements (mandatory) (sample)**

| HSI Requirements | | |
|---|---|---|
| Parameter | Threshold | Contract Specification Requirement |
| HSI (e.g., human performance) | | |
| HSI Domain (e.g., manpower, training) | | |

### 3.2.7 System Safety

Document a strategy for the System Safety engineering program, addressing hardware and software, to include autonomous and artificial intelligence (AI) capabilities and functions, in accordance with MIL-STD-882 and applicable guidance. Document the ESOH risk and compliance requirements management planning by attaching the Programmatic Environmental Safety and Health Evaluation (PESHE), National Environmental Policy Act (NEPA), and Executive Order (E.O.) 12114 compliance schedule, in accordance with Section 4321 of Title 42, U.S.C.; activities captured in table 3.2-9. (See: https://ac.cto.mil/sse/)

***Expectation:*** *Program addresses risks associated with system-level hazards, system-of-system level hazards, hardware, software, environmental and occupational health related hazards, including autonomous and AI capabilities and functions, using MIL-STD-882E and applicable guidance. Software System Safety assessments are conducted using the Joint Software System Safety Engineering Handbook and the Joint Services – Software Safety Authorities (JS-SSA) Software System Safety Implementation Process and Tasks Supporting MIL-STD-882E. Program provides the procedure/process details on how they will support weapon, test, and flight system safety as appropriate and applicable.*

**Table 3.2-9 Planning and Timing for System Safety Engineering Activities and Requirements (mandatory) (sample)**

| Activity or Requirement | Planning and Timing |
|---|---|
| System Safety Program Plan (SSPP) | ***Expectation:*** *The System Safety methodology for the identification, classification, and mitigation of safety hazards as part of the overall SE process is documented. The approach for meeting requirements is documented. The SSPP is documented as early as possible and updated as needed.* |
| Hazardous Materials Management Plan (HMMP) | ***Expectation:*** *Contractor roles, responsibilities, and procedures needed to accomplish hazardous material (HAZMAT) management and tracking are defined. The HMMP is documented as early as possible and updated as needed.* |
| Functional Hazard Analysis (FHA) | ***Expectation:*** *The system functions and the safety consequences of functional failure or malfunction, i.e., hazards, are identified and classified. The FHA is part of PDR objective evidence.* |
| Preliminary Hazard Analysis (PHA) | ***Expectation:*** *Hazards are identified, initial risks are assessed, and potential mitigation measures are identified early. The PHA is part of PDR objective evidence.* |
| System of Systems (SoS) Hazard Analysis | ***Expectation:*** *Any unique SoS hazards are identified. The analysis begins at PDR and is final by the FRP decision review.* |
| Operating and Support Hazard Analysis (O&SHA) | ***Expectation:*** *Hazards introduced by operational and support activities and procedures are identified and assessed, and the adequacy of operational and support procedures, facilities, processes, and equipment used to mitigate risks associated with identified hazards are evaluated. The O&SHA begins at SRR and is final by FRP decision review.* |
| Environmental Hazard Analysis (EHA) | ***Expectation:*** *Hazards to the environment throughout all life-cycle phases and modes are identified; hazards in the Hazard Tracking System (HTS) are documented; hazards using the System Safety process described in MIL-STD-882E Section 4 are managed; and system-specific data to support National Environmental Policy Act (NEPA) and Executive Order (EO) 12114 requirements are provided. The EHA begins pre-PDR and is final by FRP decision review.* |
| Hazard Tracking System (HTS) | ***Expectation:*** *A closed loop HTS is implemented and maintained; as various hazard analyses are performed, the hazards are recorded and updated. The HTS begins as early as possible and is maintained for the life of the program.* |
| Safety Assessment Report (SAR) | ***Expectation:*** *Program conducts and documents an assessment to identify the status of safety hazards, associated risks, mitigation measures, and formal risk acceptance decisions in advance of testing, demonstration, or fielding.* |

*Note:* Table 3.2-9 is not a comprehensive list of all mandatory safety activities. All analyses, program plans, and management plans are identified tasks in MIL-STD-882. The tasks identified can be selectively applied to allow a tailored System Safety effort as specified in MIL-

STD-882E. Individual tasks should be specifically called out in contractual requirements as CDRLs with related Data Item Deliverables (DIDs).

### 3.2.8 Software Engineering

#### 3.2.8.1 Software Engineering Overview

Provide a brief, one paragraph summary of the scope and overall software effort. If a program has a government–provided Software Development Plan (SDP) document or content, provide a link or attach it to the SEP. To avoid duplication for areas where SEP topics may overlap with other documents (e.g., PPP, Cybersecurity Strategy (CSS), SDP (contractor)), provide a brief overview and a link to the document that provides additional coverage. Topics not explicitly covered by other documents and referenced, should be covered in the SEP (e.g., not covered in the SDP) (DoDI 5000.88, Para 3.4.a.(3).(c)).

For additional sources of information *see also:*

- The Software Engineering for Continuous Delivery of Warfighting Capability Guide (link TBD). The guide is part of a series on the topic of Continuous Delivery from the perspective of SWE for those leading and participating in the DoD transformation to continuous delivery. The planned series consists of 7 parts each addressing a different aspect of transformation; Part I – Policy and Guidance; Part II – Software Metrics and Use; Part III – Contracting for Software Engineering; Part IV – Observed Challenges and Best Practices; Part V – Technology Modernization; Part VI – Artificial Intelligence and Machine Leaning; Part VII – Workforce Competencies.
- Engineering of Defense Systems Guidebook (forthcoming)– *see* Software sections for additional Adaptive Acquisition Framework and Software Acquisition Pathway guidance.
- DoD Chief Information Officer's DoD Enterprise DevSecOps Reference Design (https://dodcio.defense.gov) for guidance on how specific collections of technologies form a secure and effective software factory.

***Expectation:*** *(Example) "Program XYZ is under contract to be developed by five companies. ABC (Contractor #1) is developing 15 Computer Software Configuration Items (CSCI), and DEF (Contractor #2) is developing 10 CSCIs. ABC and DEF are the largest efforts (>= 80%) from a software development effort perspective, comprising over 45% and 35% of the total XYZ software development staffing." The software scope will be summarized as illustrated in Table 3.2-10.*

**Table 3.2-10 Software Development Scope (mandatory) (sample)**

Scope: Program XYZ

| | | |
|---|---|---|
| **Size:** ~ 1,300 Function Points | **Peak Staff:** 150 FTE (ABC: 95, DEF 55) | **No. SW Suppliers:** 4 |
| **Methodology:** Mixed (i.e., agile & waterfall) | **Duration:** 66 months | **No. CSCIs:** 30 |
| **SW Dev Cost (BY$M):** $100.5M (est.) | **No. Builds:** 7 major builds | |

#### 3.2.8.2 Software Planning Phase

Address the following planning aspects for software engineering activities:

- Describe the software development methodology used (e.g., Agile, DevSecOps, Continuous Integration/Continuous Delivery (CI/CD), Waterfall, Hybrid); tools used to support

development activities (e.g., Integrated Digital Environment (IDE)); environments used in development, test, and deployment (e.g., operating systems for development and target environments); tools used to build and deploy software (e.g., software pipeline tools, IA as, PaaS, and SaaS); and degree of build/test/release automation.

- Describe the process, approach, and tools to perform software development estimation for the planning and execution phases.
- Describe the capability roadmap (i.e., full life cycle) to include the current build process, the expected build times, and the build cycle frequency.
- Describe the program's SW sustainment strategy, the rationale behind that strategy, and how the strategy is to be implemented, including SW transition planning and the intervals for management review.
- Identify and describe the software metrics used to monitor and manage the software activities (at both the team and program levels), including delivered end-to-end performance improvements, new capabilities, and value to the user. (see Appendix C – Agile and DevSecOps Software Development Metrics).
- Describe the integration, test, and release strategy (including Continuous Authority to Operate (cATO) process) to enable early and continuous integration to validate mission effectiveness early and throughout the software life cycle (DoDI 5000.88, Para 3.4.a.(3).(o)).
- Describe the process of identifying, managing, and mitigating software unique program risks.
- Describe the handling of critical SW requirements to address (1) flight clearance, (2) safety assurance, (3) cybersecurity, (4) program protection/software assurance, and (5) assurance of other critical requirements (e.g., nuclear surety). To avoid duplication and overlap with other documents providing more detailed topic coverage, provide a brief overview and a link to the document.
- Address reusable SW products (e.g., commercial off-the-shelf (COTS), government off-the-shelf (GOTS)). Describe (1) the approach for identifying, evaluating, and incorporating reusable SW products, including the scope of the search for such products and the criteria to be used for their evaluation and (2) the approach for identifying, evaluating, and reporting opportunities to develop reusable SW products.
- Identify software development deliverables and artifacts. Identify what IP rights licenses the Government will acquire to those deliverables and the access to software development artifacts. Specifically, describe the approach to provide authorized representatives with access to developer and subcontractor facilities to review SW products and activities.

***Expectation:*** *Program will plan for the integration of software "procurement" and "sustainment" activities. Software functionality will be developed, delivered, and sustained continuously across its life cycle; therefore, it must be constantly maintained to retain capability and to, for example, address future security threats and a potential increase in functionality. Software system safety should also be addressed.*

#### 3.2.8.3 Software Execution Phase

Address the following execution aspects for software engineering activities:

- SW development environment (e.g., software factory): establishing, controlling, and maintaining a software development environment, to include (1) SW engineering

environment, (2) SW test environment, (3) SW development library, (4) SW development files, (5) non-deliverable SW, and (6) SW assurance considerations, including tool selection

- SW requirements analysis: requirements decomposition process, including the steps needed to ensure that SW requirements are stable, traceable, prioritized and allocated to iterations; how deferred requirements will be managed
- SW design approach: (1) global design decisions, (2) architectural design, and (3) detailed design, with each area addressing: (4) SW Safety/Airworthiness, (5) Cybersecurity, and (6) Reliability/dependability (e.g., Site Reliability Engineering), (7) MOSA considerations, and (8) Software Assurance
- How the architecture and design strategy underpins SW sustainability
- SW integration and test approach, including (1) mapping of dependencies and performing frequent end-to-end integration and test, (2) preparing for integration and test, (3) performing integration and test, (4) recording and analysis of integration and test results, and (5) regression test of revisions
- Deployment, specifying the approach for (1) preparing the executable SW, (2) preparing version descriptions for user sites, (3) preparing user manuals, and (4) target environment installation and version compatibility at user sites
- SW configuration management, specifically the approach to manage and control the software configuration items
- SW quality assurance, specifically the approach for evaluations, measures to ensure quality control independence from the development team, and required records
- Managing technical debt, specifically the (1) problem/change reporting process, (2) process for maintaining the system backlog, and (3) role of the Government in the Problem Reporting and Deficiency Reporting processes
- How defects are tracked and resolved
- Software system safety efforts to be executed

#### 3.2.8.4 Software Obsolescence

Describe the approach to address software obsolescence, from a Diminishing Manufacturing Sources and Material Shortages (DMSMS) perspective. For each aspect below, describe the plans and processes to address:

- Functional changes resulting from hardware or software modifications (e.g., interfaces, deprecated data/functional constructs)
- Embedded COTS, GOTS, Military Off the Shelf
- Vendor end-of-life support (e.g., Windows XP, Windows Vista, Windows 7, Red Hat Enterprise Linux (prior to current 8.x))
- Infrastructure (e.g., software factory, digital twin)
- Changes resulting from published Information Assurance Vulnerability Alert (IAV-A) and Information Assurance Vulnerability Bulletin (IAV-B) security notices
- Configurable data items (e.g., anti-virus table updates, static configuration data tables, build scripts)

- The level of regression testing required at all levels (e.g., unit, CSC, CSCI, subsystem, system) to support continuous ATO impacts due to the changes in COTS, GOTS, or developmental software, including safety considerations and nuclear surety

***Expectation:*** *Program should understand the communication process among the software engineers, systems engineers, and the system safety experts in resolving DMSMS issues due to software obsolescence. These relationships must be understood and planned for to develop the best resolution.*

### 3.2.9 Technology Insertion and Refresh

List all technology insertion and refresh projects, approved or tentative, and describe briefly:

- Planning/execution status (e.g., nascent, total drawings 50% complete, and critical drawings 35% complete)
- Rationale (e.g., late-developing technology enables cost-effective achievement of user objective requirement(s), response to upgraded adversary capabilities, cost-effective improvement in R&M)
- Whether the project is covered in current acquisition program baseline; if not, state plan to fund project
- How DMSMS has been taken into account in the timing and scope of the project
- Any special provisions (that would not otherwise be included) in the present system design that enable/facilitate the project
- All identified risks related to technology insertion and refresh, including cyber risks to mission, with status of mitigation plans; embed or attach to the SEP
- The impact of the technology insertion and refresh on the ability to detect, respond, and recover from relevant cyber threats as may be elaborated in a Mission Based Cyber Risk Assessment (MBCRA). For emerging technology, which IPT(s) is (are) responsible for tracking and evaluation; include present maturity status
- If the technology is newly matured, the nature of the demonstration or embed or attach the test/demonstration reports
- The relationship of MOSA with the technology insertion and refresh projects
- Describe what, if any, modification will be needed to the program protection plan or additional protections plan due the technology insertion and refresh.

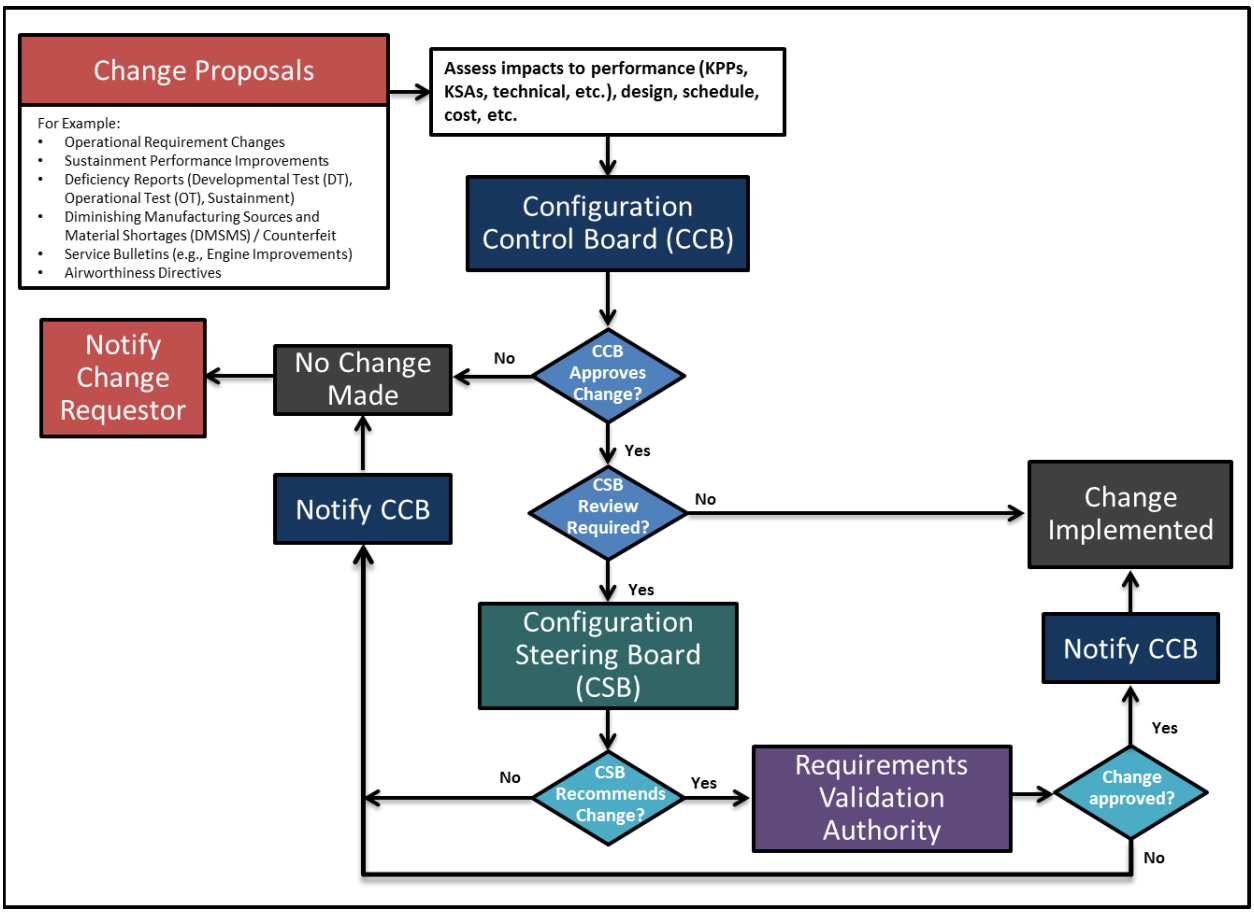
### 3.2.10 Configuration and Change Management

If a configuration management plan is available, then embed, attach, or cite the IDE reference. Otherwise, provide the following:

- **Technical Baseline Artifacts** – List and describe baseline artifacts. Describe how the program will track and manage baselines within its IDE. At a minimum, describe the artifacts of the concept, functional, allocated, and product baselines and when each technical baseline has been or will be established and verified. If practicable, the PM will establish and manage the technical baseline as a digital authoritative source of truth. (*See* SE Guidebook (forthcoming) Configuration Management Process, for additional guidance)

***Expectation:*** *Program should own all baselines (functional, allocated, and product); as such the program should understand which artifacts make up each technical baseline and manage changes appropriately.*

- **Configuration Management/Control (and Change) Process Description** – Provide a process diagram (Figure 3.2-6) detailing how the program maintains configuration control of its baselines. Describe the approach the program office takes to identify, document, audit, and control the functional and physical characteristics of the system design; track any changes; and provide an audit trail of program design decisions and design modifications.




Source: Name Year if applicable. Classification: UNCLASSIFIED.

**Figure 3.2-6 Configuration Management Process (mandatory) (sample)**

- **Roles, Responsibilities, and Authorities** – Summarize the roles, responsibilities, and authorities within the Configuration Management (CM) process. If this includes one or more configuration boards, describe the hierarchy of these boards, their frequency, who (by position) chairs them, who participates, and who (by position) has final authority in each. Describe how the program's IDE tools will support the CM process if used. Identify who has configuration control and when. **(Added)(AFMC) If a Configuration Control Board Charter is available, then embed, attach, or cite the IDE reference.**
- **Configuration Change Process** – Outline the program processes used to change the technical baseline/configuration and specifically address:

- How changes to a technical baseline are identified, evaluated, approved/disapproved, recorded, incorporated, and verified
- **(Added)(AFMC) How data, models, and analyses in digital engineering tools are configuration managed**
- **(Added)(AFMC) How changes are communicated to stakeholders**
- How product information is captured, maintained, and traced back to requirements
- How requirements for in-service configuration/design changes are determined and managed/controlled
- How internal and external interfaces are managed and controlled
- The process by which the program and external programs review configuration changes for possible impacts on each other's programs
- How the IP strategy affects and influences the planned configuration control processes, and embed or attach that strategy to the SEP.

- **Classification of Change** – Define the classification of change (Class 1, Class 2, etc.) applicable to the program and approval authority. Identify by position who in the CM process is responsible for determining the classification of a change and who (by position) verifies/confirms/approves it.

***Expectation:*** *Program controls the conceptual, functional, allocated, and product baselines and should be represented in a digital model, managed within the ecosystem. The Digital Engineering implementation facilitates the management of program baselines.*

### 3.2.11 Technical Data Management

The Technical Data Management process provides a framework to acquire, manage, maintain, use, and ensure access to the technical data and computer software required to manage and support a system throughout the acquisition life cycle (DoDI 5000.88, Para 3.4.a.(3).(h)). (*See* SE Guidebook (forthcoming), Technical Data Management Process, for additional guidance.)

***(Added)(AFMC) Expectation: Programs should identify the contractual language to obtain the data and models to design, develop, verify, validate, produce, maintain, sustain, operate, and modify the weapon system through the lifecycle and utilize the Digital Guide and Acquisition and Sustainment Data Package Contracting Language and Data Item Descriptions as reference materials whenever possible) (https://usaf.dps.mil/teams/afmcde/SitePages/Home.aspx). In addition, the program should identify the data and model delivery and how the program will access and store the data and models (e.g., Integrated Digital Environment and Product Lifecycle Management). If a data management plan is available, then embed, attach, or cite the IDE reference.***

The PM and Systems Engineer should ensure that data rights are identified early and appropriate contract provisions are put in place (IAW DFARS 252.227-7013, 252.277-7014, 252.227-7015 and 252.227-7017). The SEP should address how the digital engineering implementation will support the following activities and products:

- Data requirements
- Use of COTS software and open source software

- Technical data and software needed, when, for what purpose(s) and by what organization(s) to support data rights decisions
- How data will be received, verified, and accepted
- How data will be stored, maintained, and controlled
- How data will be used and exchanged
- How data will be protected

The SEP identifies the models, simulations, tools, workflows, and engineering environments the program plans to use as part of the respective planned activity. Address what data are needed for this activity, in what tool the data are written, and what other tools will need to consume the data. Planning should include an access control model that supports the ability of all participants in this activity to be able to use and share the data.

***Expectation:*** *Programs should address the technical planning required to implement the data strategy documented in the AS. Programs should acquire the appropriate rights to the interface technical data to allow for system evolution and interoperability in accordance with the program's IP strategy.*

### 3.2.12 System Security Engineering

Describe how the program implements comprehensive system security engineering/program protection to include hardware and software assurance, and how it integrates with the SE processes.

***Expectation:*** *To maintain technology dominance, the PM will prepare a PPP in accordance with DoDI 5000.83, Technology and Program Protection to Maintain Technological Advantage. The PPP will serve as a technical planning tool to guide system security engineering activities, which include software and hardware assurance for the program.*

### 3.2.13 Technical Reviews, Audits and Activities

Summarize key planned systems engineering, integration, and verification activities for all future acquisition phases, including updated risk reduction and mitigation strategies and technical and manufacturing maturity.

- Technical Review and Audit Planning – The LSE/CE should be responsible for the overall conduct of technical reviews. The Configuration Manager should be responsible for the overall conduct of configuration audits (DoDI 5000.88, Para 3.4.a.(3).(k)).
    - If useful, add a diagram of the process with the objective time frames for each activity before, during, and after the technical review and audit.
    - Technical reviews and audits should be conducted when the system under review is sufficiently mature and ready to proceed to the next phase.
    - Entry and exit criteria should include maturity metrics, such as required certifications obtained, percentages of total and critical drawings released, percentage of interfaces defined, etc.
- Technical Activities – The LSE/CE, or Technical Lead as delegated, will be responsible for other technical activities planned within the program’s life cycle that will be used to inform key decisions, derive mitigations and contingencies, or provide maturity status (current or

predictive) of requirement feasibility for the system, subsystem, or individual item or product(s).

- Software Development – The SEP should describe how software will be incorporated into the program level Technical Review and Audit process. Specifically, for system-level technical reviews, audits, and technical baselines, describe how SWE activities (i.e., when Agile, DevSecOps, Continuous Integration/Continuous Delivery methods are used) will be integrated into the program-level SE processes and acquisition documents/models.
- For each planned technical review and audit, the SEP should include a technical review and audit table (Table 3.2-11). (*See* SE Guidebook (forthcoming), Technical Reviews and Audits Overview, for additional guidance). Include all required technical reviews as listed in the DoDI 5000.88. If the PM is not planning on conducting a required technical review, provide a short paragraph that identifies the review and the reasoning for waiving the review.

**Table 3.2-11 Technical Review and Audit Details (mandatory) (sample)**

| XXX Details Area | XXX Review Details<br>*(Fill out tailored criteria for this acquisition phase, etc.)* |
|---|---|
| **Chairperson** | Identify the Technical Review Chair. |
| **PMO Participants** | Identify Positions/functions/IPTs within the program offices which are anticipated to participate (Engineering Leads; Risk, Logistics, and Configuration Managers; DCMA Rep., and Contracting Officer, etc.). |
| **Anticipated Stakeholder Participant Organizations** | Identify representatives (stakeholders) from Service SE and Test, OUSD(R&E) external dependent programs, the User, and participants with sufficient objectivity with respect to satisfying the preestablished review criteria. For ACAT ID programs, ensure that OUSD(R&E) receives invitations to attend sub-system level reviews as well as the system level reviews (particularly PDR and CDR) to allow for their independent Post-PDR and Post-CDR assessment.<br>Independent Review Team (IRT) (for MDAPs) |
| **Purpose (of the review)** | Describe the main purpose of the review and any specific SE goals. |
| **Entry Criteria** | Identify tailored Entry Criteria established for conducting an event-driven review. (Criteria should be objective and measurable/observable.) |
| **Exit Criteria** | Identify tailored Exit Criteria. (Criteria should be objective and measurable/observable.) |
| **Products/Artifacts (from the review)** | List expected products from the technical review (for example):<br>• Established system allocated baseline<br>• Updated risk assessment for Engineering, Manufacturing, and Development<br>• What artifacts constitute the baseline<br>• Assessment of SW development progress<br>• Updated Cost Analysis Requirements Document (CARD) or CARD-like document based on system allocated baseline<br>• Updated program schedule including system and SW critical path drivers<br>• Approved Life-Cycle Sustainment Plan updating program sustainment development efforts and schedules. |

| | |
|---|---|
| | • Updated list of list of Key Risks, Issues, and Opportunities and accepted Mitigation Plans/Strategies where appropriate. |

***Expectation:*** *Program plans and conducts event-driven technical reviews and audits. Program should use a standard process for conducting technical reviews and audits. If a technical review and audit guide and charter are available, the SEP will reference and provide. For ACAT IB/IC programs, the PDR and CDR planning table will include Component participants who will conduct the independent PDR Assessment and CDR Assessment.*

**For Appendices B, C, D, and E a link to the applicable documents is acceptable.**

## Appendix A – Acronyms

*Provide a list of all acronyms used in the SEP.* Example List:

| | |
|---|---|
| FMECA | Failure Mode, Effects, and Criticality Analysis |
| FRACAS | Failure Reporting, Analysis, and Corrective Action System |
| JCIDS | Joint Capabilities Integration and Development System |
| MRA | Manufacturing Readiness Assessment |
| OUSD | Office of the Under Secretary of Defense |
| SEP | Systems Engineering Plan |

## Appendix B – Item Unique Identification Implementation Plan

Attach a copy of the plan or a link to plan document(s).

## Appendix C – Agile and Development Security and Operations Software Development Metrics

Describe how the program uses SW metrics to monitor progress to plan. Discuss how often metrics are updated and reported, at what levels within the PM and SWE Teams, and how data-driven decisions are supported at every level (e.g., IPT Lead, Chief SE, PM, PEO, SAE).

Include a list of the metrics and describe how they will be tailored and used as part of the SW measurement program to assess SW development progress across the development and sustainment life cycle. Briefly describe how the metrics and measurement data will be provided or accessed, for example SW Dashboards/SW Metrics reports, and/or direct real-time access to contractor metrics and data.

When implementing the Software Acquisition Pathway (i.e., DoDI 5000.87), refer to the DAU website (https://aaf.dau.edu/aaf/software/) for the recommended set of metrics.

**Agile Software Development Metrics**

For programs employing Agile development and continuous integration methods, include the following **minimum set** of metrics, in addition to the TPM SW metrics identified in Table 3.2-2. Agile measures should be reported and aggregated where applicable.

- Sprint Management
  1. Sprint Velocity. *Report number of story points per sprint; planned and actual.*
  2. Average Cycle Time. *Report average time between starting and completing tasks, in time-series.*
  3. Burn-down (Hours or Story Points). *Report hours or story points remaining, in time-series.*
  4. *Discuss what went well and what can be improved for the completed sprint*

- Development and Continuous Integration
  1. Build Automation. *Report % steps automated.*
  2. Average Builds per Day/Week. *Report by Pass, Fail.*
  3. Average Duration per Build. *Report Minimum, Average, Maximum in hours.*
  4. Unit Test Coverage. *Report percent automated, percent coverage.*
  5. Static Code Analysis Coverage. *Report percent automated, percent coverage. For weakness/vulnerability identification, report percentage findings, burn-down and/or Pass/Fail should be included to support program planning.*
  6. Functional Thread Test Coverage. *Report percent automated, percent coverage.*
  7. System Test Coverage. *Report percent automated, percent coverage.*

**DevSecOps or CI/CD Metrics**

In addition to the Agile metrics identified above, for programs employing DevSecOps or CI/CD methodologies to SW development, test, and deployment, include the following **supplemental minimum set** of metrics,.

- Environment Management
  1. Number of Active Environments*; e.g., Development, System Integration Lab (SIL) (staging), Production/Operations.*
  2. Environment Availability. *Report uptime for active environments (not including Creating, Recovering, and Maintenance); e.g., # hours/day, #days/week*.
- Environment Automation
  1. Time to (Create, Activate, Recover) Environment. *Report in minutes/hours, % automated by environment (development, SIL (staging), Production/Operations)*.
  2. Automated Environment Controls/Features Monitored and Audited. *Report % by Phase*.
- DoD Enterprise's Software Modernization Initiatives and Policy Changes

  The following four metrics, often referred to as the DORA 4 (DevOps Research and Assessment), are widely used in industry to baseline and improve pipeline delivery performance.

  1. Deployment Frequency – frequency of software deployment to field/production.
  2. Lead Time - time from code commit to fielding/product deployment
  3. Mean Time to Recover (MTTR) – time to recover from a failure in the field/production
  4. Change Failure Rate - percentage of deployments causing a failure

***Expectation:*** *Program uses measures to report progress and keep stakeholders informed. These measures form the basis to assess current SWE status for SW maturity, Milestone decisions, technical reviews, and risk management boards and actions.*

## Appendix D – Concept of Operations Description

Programs will provide the draft or approved Concept of Operations (CONOPS) as an attachment or provide a high-level description of the CONOPS that includes mission scenarios,

design reference missions, and operational functions of the system and the relation to the design approach (DoDI 5000.88, Para 3.4.a.(3).(n)).

## References

*Note: Provide a list of documents used in the SEP. Include complete references to correspond with text citations. Include citations and references for illustrations reprinted from another source. Illustrations with no source information are assumed to be original to the SEP.*

*Example List:*

Air Force Guidance Memorandum, AFPAM 63-128, Attachment 14, AFI 63-101/20-101, para 5.1.5. September 16, 2016. Available at: https://www.netcents.af.mil/Portals/30/documents/AFI%20%2063_101_20_101_16%20Sept%202016.pdf?ver=2016-09-27-123456-923

Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability https://www.dodtechipedia.mil/dodwiki/display/techipedia/Chemical%2C+Biological%2C+Radiological%2C+and+Nuclear+Survivability.

DCMA-EA PAM 200.1. Earned Value Management System (EVMS) Program Analysis Pamphlet (PAP). Fort Belvoir: Defense Contract Management Agency, October 2012. http://www.dcma.mil/LinkClick.aspx?fileticket=0CBjAarXWZA%3d&portalid=31

DoD Directive 5000.01, “The Defense Acquisition System,” September 9, 2020.

DoD Instruction 5000.02. Operation of the Adaptive Acquisition Framework. Under Secretary of Defense for Acquisition and Sustainment, January 23, 2020. Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf

DoD Instruction 5000.82, “Acquisition of Information Technology (IT),” April 21, 2020.

DoD Instruction 5000.83. Technology and Program Protection to Maintain Technological Advantage, Publishing Office, July 20, 2020.
DoD Instruction 5000.85, “Major Capability Acquisition”, August 6, 2020.

DoD Instruction 5000.87, “Operation of the Software Acquisition Pathway,” October 2, 2020. Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF?

DoD Instruction 5000.88, “Engineering of Defense Systems,” November 18, 2020.

DoD Instruction 8582.01, “Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information,” Dec 9, 2019.

DoDEA Administrative Instruction 8510.01, “Risk Management Framework for DoDEA Information Technology,” October 29, 2019.

Engineering of Defense Systems Guidebook. Washington, D.C.: Office of the Deputy Director for Engineering, Forthcoming.

Human Systems Integration (HSI) Guidebook. Washington, D.C.: Office of the Deputy Director for Engineering, Forthcoming.

Mission Assurance Guide. TOR-2007(8546)-6018 REV. B, section 10.6.3 Risk Management. El Segundo, CA: Aerospace Corporation, June 1, 2012. Available at: https://safe.menlosecurity.com/doc/docview/viewer/docN0F9D572D9978558133f6f1e89d56d206a2a8e1dbbf34cbb78677356ae0291045ccb6b4945f40

Systems Engineering Guidebook. Washington, D.C.: Office of the Deputy Director for Engineering, Forthcoming.

**(Added)(AFMC) Development of an Intellectual Property Strategy: Research Notes to Support Department of Defense Programs. Special Report CMU/SEI-2014-SR-036. Pittsburgh, PA: Carnegie-Mellon University, Software Engineering Institute, September 1, 2014. Available at: https://apps.dtic.mil/sti/pdfs/ADA623591.pdf.**

**(Added)(AFMC) Department of the Air Force Systems Security Engineering (SSE) Cyber Guidebook (SSECG). https://crows-af.us/home.**

Program Name Systems Engineering Plan
Contact Info
Distribution Statement