NOT A

Department of Defense
Systems Engineering Plan (SEP)
Outline

Version 4.1 for Integrated Baseline Review

Paul Solomon draft

May 2023 May 18, 2025

Office of the Under Secretary of Defense for Research and Engineering

Washington, D.C.

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 should include a digital ecosystem implementation plan that addresses the DoD Digital Engineering Strategy goals and defines six key digital engineering ecosystem attributes: infrastructure, environment, data, security, collaboration, and innovation. Applied elements of these attributes (requirements, models, digital artifacts, network hardware/software tools, data accessibility, and compatibility, etc.) will be evident in the planning of the digital ecosystem implementation that results in the authoritative source of truth (ASoT) for the program (DoDI 5000.88, Para 3.4.a.(3).(m)).
- 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:
    - 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) and (2) 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 as a way 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.
- 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

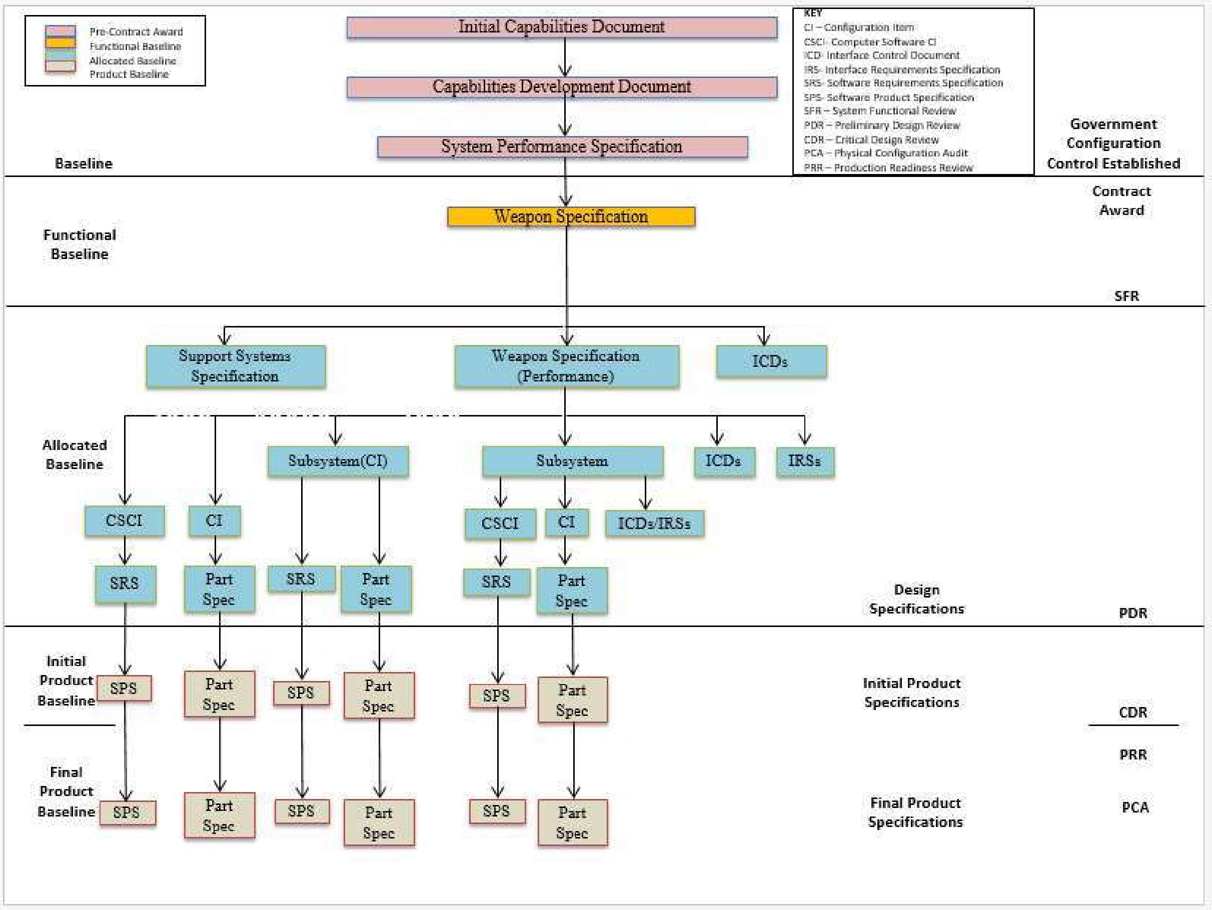
Describe how technical requirements are defined, derived, and refined from the Joint Capabilities Integration and Development System (JCIDS) or other applicable capability requirements documents down to configuration item (CI) build-to specifications and verification plans. (*See* SE Guidebook (2022), Requirements Analysis Process, for additional guidance).

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. 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 acquisition programs with digital components and interoperability requirements 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. 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: *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


Pre-Contract Award
Functional Baseline
Allocated Baseline
Product Baseline
Initial Capabilities Document
Capabilities Development Document
System Performance Specification
KEY
CI – Configuration Item
CSCI- Computer Software CI
ICD- Interface Control Document
IRS- Interface Requirements Specification
SRS- Software Requirements Specification
SPS- Software Product Specification
SFR – System Functional Review
PDR – Preliminary Design Review
CDR – Critical Design Review
PCA – Physical Configuration Audit
PRR – Production Readiness Review
Government Configuration Control Established
Baseline
Weapon Specification
Contract Award
Functional Baseline
SFR
Support Systems Specification
Weapon Specification (Performance)
ICDs
Allocated Baseline
Subsystem(CI)
Subsystem
ICDs
IRSs
CSCI
CI
CSCI
CI
ICDs/IRSs
SRS
Part Spec
SRS
Part Spec
SRS
Part Spec
Design Specifications
PDR
Initial Product Baseline
SPS
Part Spec
SPS
Part Spec
SPS
Part Spec
Initial Product Specifications
CDR
PRR
Final Product Baseline
SPS
Part Spec
SPS
Part Spec
SPS
Part Spec
Final Product Specifications
PCA

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

Figure 2.1-1 Specification Tree Illustrating Requirements Decomposition and Technical Baselines (mandatory) (sample)

Expectation: *Program should trace all requirements from the highest level (JCIDS 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 and an indication whether each requirement is expected to change over the life of the program. 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.*

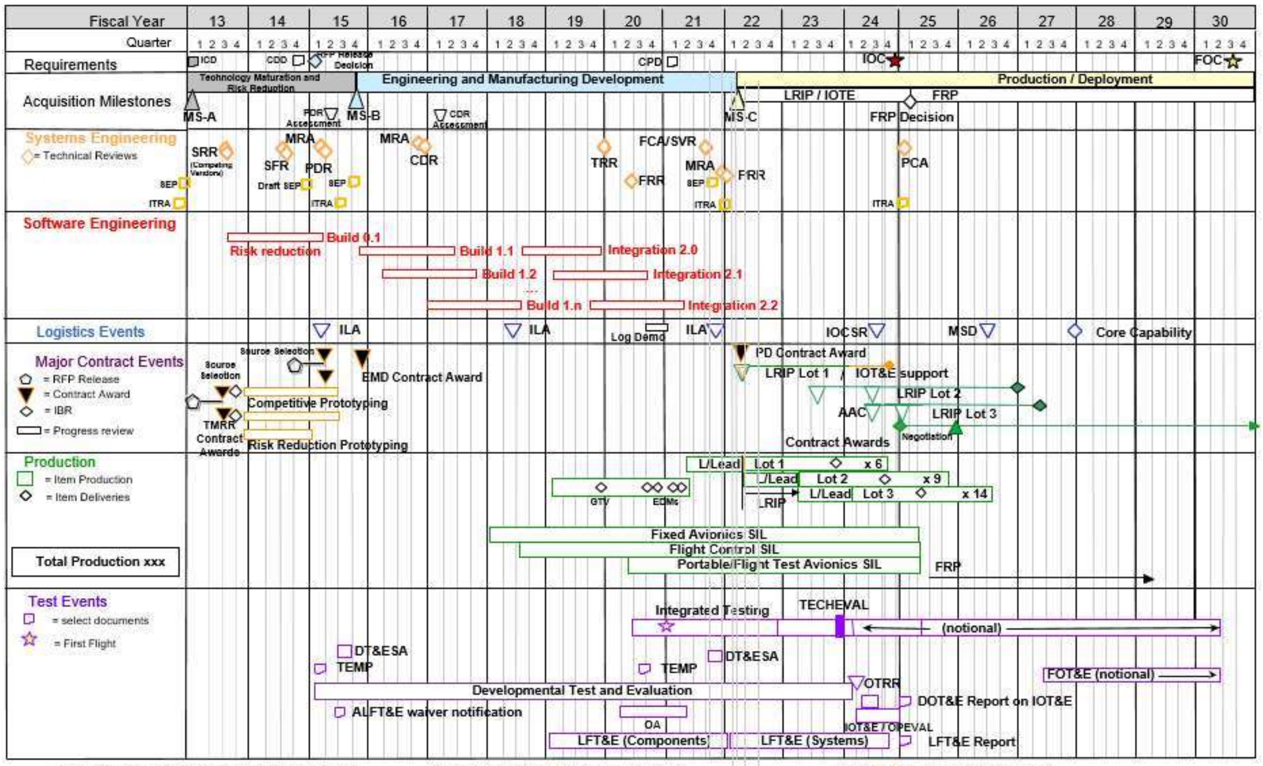
Expectation: *Program cyber requirements trace should also flow to the lowest level (e.g., component specification for passive sensing or user story for software automated resilience approaches). Use early and repeated or updated Mission-Based Cyber Risk Assessments (MBCRAs) supported by cyber test representatives (contractor and government) to inform cyber requirement flow down.*

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
    - Long-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



ALFT&E: Alternative Life Fire Test & Evaluation
CDR: Critical Design Review
DT&ESA: DT&E Sufficiency Assessment
EDM: Engineering Development Model
EMD: Engineering & Manufacturing Development
FCA: Functional Configuration Audit
FOT&E: Follow-On Operational Test & Evaluation
FRP: Full Rate Production
FRR: Flight Readiness Review
GTV: Ground Test Vehicle

ILA: Independent Logistics Assessment
IOT&E: Initial Operation Test & Evaluation
ITRA: Independent Technical Risk Assessment
LFT&E: Live Fire Test & Evaluation
LRIP: Low-Rate Initial Production
MRA: Manufacturing Readiness Assessment
MSD: Material Support Data
OA: Operational Assessment
OPEVAL: Operational Evaluation
OTRR: Operational Test Readiness Review

PCA: Physical Configuration Audit
PDR: Preliminary Design Review
PRR: Production Readiness Review
SFR: System Functional Review
SIL: Systems Integration Lab
SRR: System Requirements Review
SVR: System Verification Review
TMRR: Technology Maturation and Risk Reduction
TECHEVAL: Technical Evaluation
TRR: Test Readiness Review

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

Figure 3.1-1 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 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 digital ecosystem.
- 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 digital ecosystem 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., 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
- Digital engineering implementation and how it interfaces with new starts and legacy programs. Include how the digital ecosystem will be implemented to track and highlight integration issues within the program and with other programs (SoS)
- ICDs and any interface control WGs (ICWGs)

- *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
- 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

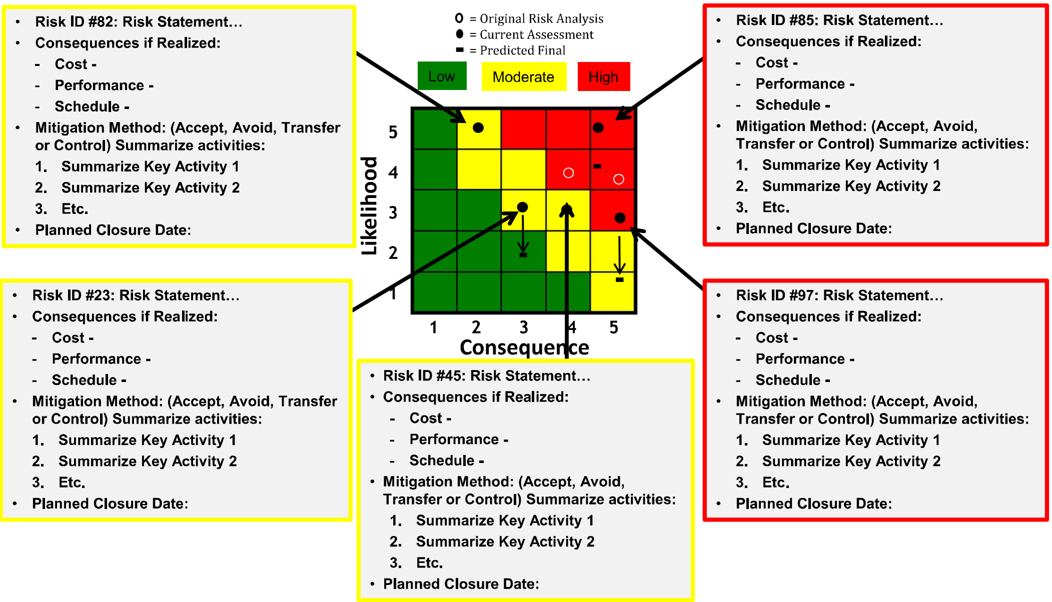
3.2 Technical Tracking

3.2.1 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 digital ecosystem 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, SpE, 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%



- Risk ID #82: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #85: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #23: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #97: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #45: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

Level	Cost	Schedule	Performance
5 Critical Impact	10% or greater increase over APB objective values for RDT&E, PAUC, or APUC Cost increase causes program to exceed affordability caps	Schedule slip will require a major schedule rebaselining 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] 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 Costs exceed life cycle ownership cost KSA	Schedule deviations will slip program to within 2 months of approved APB threshold schedule date Schedule slip puts funding at risk 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 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 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 Schedule slip impacts synchronization with interdependent programs by greater than 2 months	Unable to meet lower tier attributes, TPMs, or CTPs Design or supportability margins reduced 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 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 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.

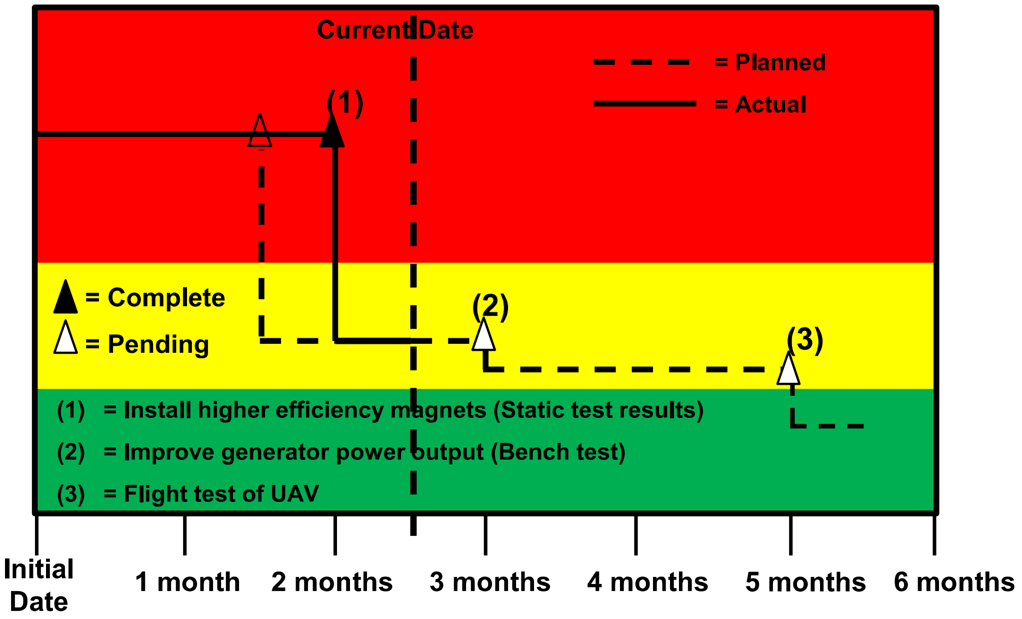
Figure 3.2-1 Risk Reporting Matrix as of [Date] (mandatory) (sample)

(*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 digital ecosystem at any time depicting the real-time status and should be accessible by all program personnel.*



Source: Name Year if applicable. Classification: UNCLASSIFIED.

Figure 3.2-2 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	Likelihood	Cost to Implement	Return on Investment						Program Priority	Management Strategy	Owner	Expected Closure
			Monetary			Schedule	Performance	System Safety Impact				
			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

3.2.2 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 (2022), 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 digital ecosystem, 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)).

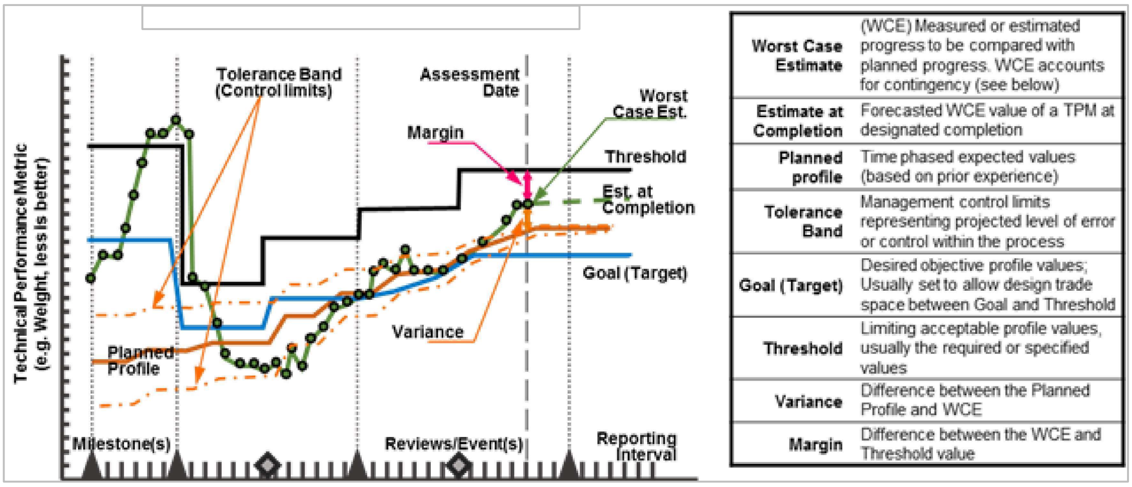
Requirements Verification - % verified	Test Management	System Engineering	CTP (% verified requirements)	99.99%	Plan	0	0	10	20	40	95	98	99
					Actual	0	0	15	20				
Operational Resilience	System Performance	CyWG	Specification – verify system performance related TPMs with cyber effects as informed by MBCRA	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 digital ecosystem 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 3.2-3 Technical Performance Measure or Metric Graph (recommended) (sample)

3.2.7 Corrosion Prevention and Control

Describe the program approach to reduce, control, or mitigate corrosion in sustainment. Ensure that corrosion prevention and control (CPC) requirements are included in the design and verified as part of test and acceptance programs established pursuant to DoDI 5000.67 (DoDI 5000.88, Para 3.7.c.). See the Corrosion Planning and Control Guidebook (2022) for more details on what to include in the SEP across the program life cycle.

The program approach to CPC should include, but not be limited to, the following:

- Engage corrosion expertise relevant to the system and its operating environment throughout the life cycle.
- Examine legacy systems for possible corrosion-design improvements.
- Document alternative material and process assessments that offer increased corrosion protection.
- Include CPC as a consideration in trade studies involving cost, useful service life, and effectiveness.
- Incorporate CPC requirements, plans, specification, standards, and criteria into relevant contractual documentation for all equipment and facilities.
- Include CPC in integrated product support element development and evaluation, including facilities.
- Identify planning, resourcing, and acquisition of corrosion-related features for longevity, lowest total ownership cost, and sustained system effectiveness.
- Retain access to CPC resources throughout the life cycle.

Expectation: *Programs should fully consider corrosion prevention and mitigation as early as possible in the acquisition life cycle and should implement appropriate strategies to minimize the life cycle impact.*

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 (2022)– *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 Development 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, digital ecosystem integration): 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.

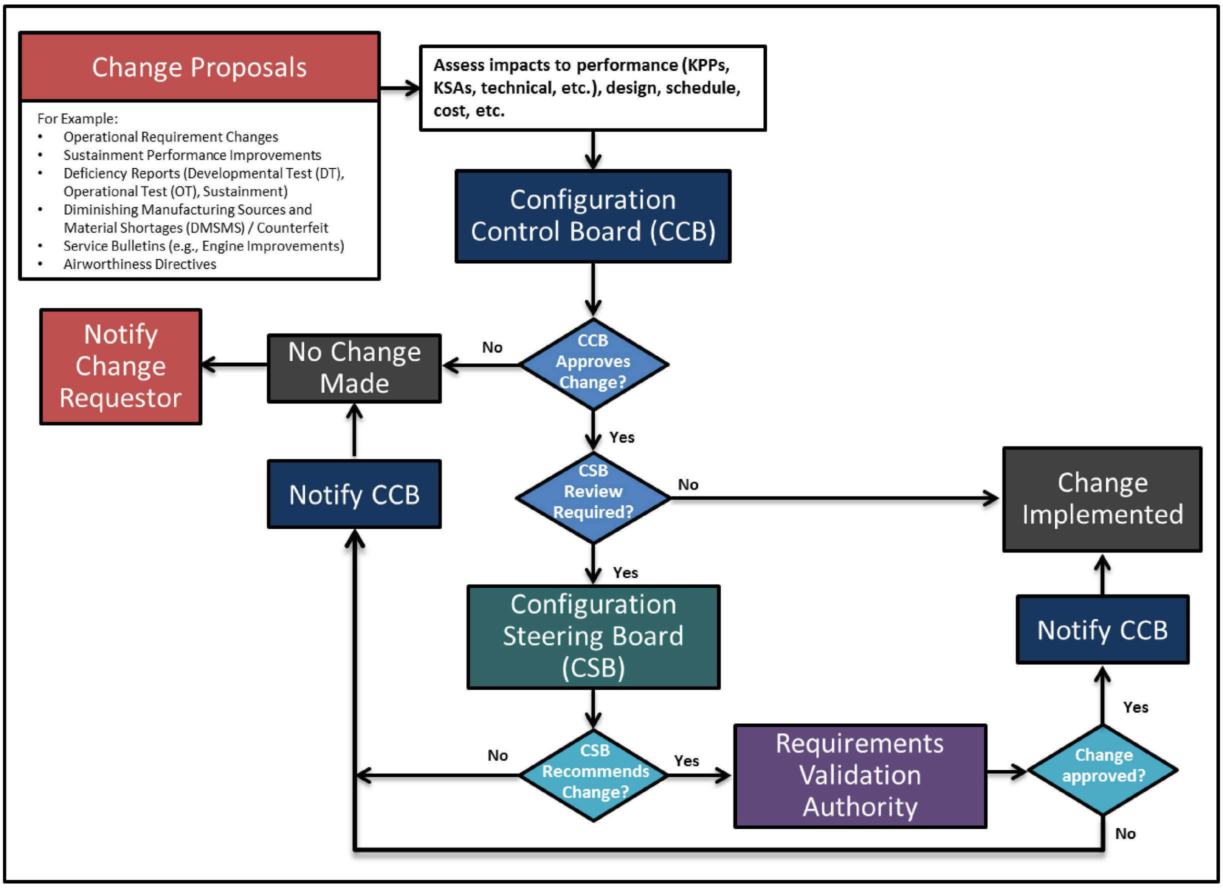
3.2.10 Configuration and Change Management

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

- **Technical Baseline Artifacts** – List and describe baseline artifacts. Describe how the program will track and manage baselines within its digital ecosystem. 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 (2022) Configuration Management Process, for additional guidance)

Expectation: *Program should own all baselines (concept, 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.


Change Proposals
For Example:
• Operational Requirement Changes
• Sustainment Performance Improvements
• Deficiency Reports (Developmental Test (DT), Operational Test (OT), Sustainment)
• Diminishing Manufacturing Sources and Material Shortages (DMSMS) / Counterfeit
• Service Bulletins (e.g., Engine Improvements)
• Airworthiness Directives
Assess impacts to performance (KPPs, KSAs, technical, etc.), design, schedule, cost, etc.
Configuration Control Board (CCB)
CCB Approves Change?
No
Yes
No Change Made
Notify Change Requestor
Notify CCB
CSB Review Required?
No
Yes
Change Implemented
Configuration Steering Board (CSB)
Notify CCB
Yes
CSB Recommends Change?
No
Yes
Requirements Validation Authority
Change approved?
No

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 digital ecosystem tools will support the CM process if used. Identify who has configuration control and when.
- **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
  - 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 (2022), Technical Data Management Process, for additional guidance.)

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 (2022), 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 *(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

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)).

Appendix E – Digital Engineering Implementation Plan

The program will include the Digital Engineering Implementation Plan as an appendix to the SEP. The implementation plan will serve, at a minimum, as a summary of the program's digital engineering implementation strategy goals, objectives, and overarching approach for such implementation. In addition, the SEP should include details to ensure the Digital Engineering Implementation Plan is integrated into the overall system engineering plan (DoDI 5000.88, Para 3.4.a.(3).(m)).

The Digital Engineering Implementation Plan should identify who is responsible for the digital engineering activities the program will conduct as part of its systems engineering activities. The program should monitor, control, and report on the implementation plan. The implementation plan should assign digital engineering roles and responsibility. The program's plan should include resources for planning for digital engineering, modeling, and simulation efforts.

This plan should capture the program's approach to establishing, evolving, maintaining, communicating, controlling, and using models within a continuous end-to-end digital engineering ecosystem. The plan should describe how relevant digital model(s), simulations, and digital artifacts will support the program efforts and how program participants, OSD, Joint Staff stakeholders, and other interdependent programs, throughout the life of the program, will have access to the plan. The plan should include planning for any training required for implementation and use of modeling tools and modeling actions. The program should consider an approach that supports incremental delivery of a continuum of models, simulations, and artifacts needed to support program events, milestones, and decisions.

The digital engineering tool chain should maintain specifications and documentation in digital form that were historically contained in paper documents. Information contained in specifications and documents will be available in the digital ecosystem and can be used to publish necessary documentation as required.

Programs should document the digital engineering implementation architecture and digital tool chain in this appendix or in the main body of the SEP. The documentation should include a list of the automated tools used and their purpose - including tools to perform modeling and simulation, to design, build and test the system, to maintain an ASoT, and to ensure system security and survivability. These attributes identify the capabilities needed to perform engineering activities and the capabilities needed to collaborate and enable ASoT information exchange that results in a continuous integrated end-to-end digital ecosystem.

The appendix should include plans for how the digital engineering implementation will support the program organization. Topics include but are not limited to:

Modeling Methodologies: Describe how each of the following will be provided and used and who is responsible for providing it.

- Definition of and or identification of methods, processes, and tools for implementing modeling methodologies for the integrated modeling environment.

- Definition of modeling standards, guidelines, and templates that will be needed to support digital engineering desired capabilities.

Configuration Control Baseline: Describe plans for the development of a robust, executable process for managing models throughout the program life cycle. The plans will also include the roles and responsibilities required to accomplish configuration management tasks. The plans may also include the necessary naming, marking, tagging necessary to make the models discoverable, accessible, reusable, and trusted.

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 perform integrated engineering activities.

Collaboration: Describe the plan for establishing the needed infrastructure and environment for programs and projects to conduct reviews and audits, hold technical meetings, perform analysis, and collaboratively develop models. The collaboration environment should also be planned to ensure internal and external stakeholders (e.g. OSD, Joint Staff, and interdependent programs) have the necessary access and availability of technical data and acquisition artifacts needed for both short-term decisions and long-term system life cycle management in a digital ecosystem.

Model Use: Include the scope of the program's complete modeling, simulation, and analysis efforts that are essential to performing engineering and system safety activities. Identify each model and what it will be used for to support the program. In addition, identify the model owner that is authorized to make changes and support others in its proper use. Establish and capture the model and data within this plan along with appropriate metadata required for model assurance and reuse purposes.

In the main body of the SEP, include details about how digital engineering implementation will support the integrated systems engineering and system safety activities.