Reliability and Maintainability Engineering Contract Language for the Software Acquisition Pathway

April 2026

Office of Systems Engineering and Architecture

Office of the Under Secretary of War for
Research and Engineering

Washington, D.C.

Reliability and Maintainability Engineering Contract Language for the Software Acquisition Pathway

April 2026

Office of Systems Engineering and Architecture
Office of the Under Secretary of War for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301
https://www.cto.mil/sea
osd-sea@mail.mil | Attn: Specialty Engineering

Approved by
Executive Director, Systems Engineering and Architecture
Office of the Under Secretary of War for Research and Engineering

R&M Engineering Contract Language for the Software Acquisition Pathway
Change Record

Date	Version	Change
April 2026	Initial release.	N/A.

Contents

Figures

Tables

Preface

This guide provides sample language for Department of War (DoW) program offices to use to incorporate reliability and maintainability (R&M) engineering activities into contracts for the DoW Software Acquisition pathway. This guide provides recommendations for tailoring the Software Acquisition pathway activities and corresponding language to plan for the appropriate R&M for the type of program.

Software Acquisition is one of the six pathways introduced in DoD Instruction (DoDI) 5000.02, "Operation of the Adaptive Acquisition Framework" (AAF) (November 2020):

- Major Capability Acquisition (MCA)
- Urgent Capability Acquisition (UCA)
- Middle Tier of Acquisition (MTA)
- Software Acquisition
- Defense Business Systems (DBS)
- Acquisition of Services

Although this document focuses on acquiring software using the Software Acquisition pathway (DoDI 5000.87), it also discusses software acquired or developed using other AAF pathways. Programs may use a combination of AAF pathways to provide value not otherwise available through a single pathway.

Section 1 of this guide provides an overview of the AAF and Software Acquisition pathway. Section 2 provides the R&M guidance and sample language for Requests for Information (RFIs). Section 3 provides R&M tailoring guidance and sample contract language for Requests for Proposals (RFPs). This guide includes selected hyperlinks to major sources. Additional sources and links are available in the reference list at the end of the document.

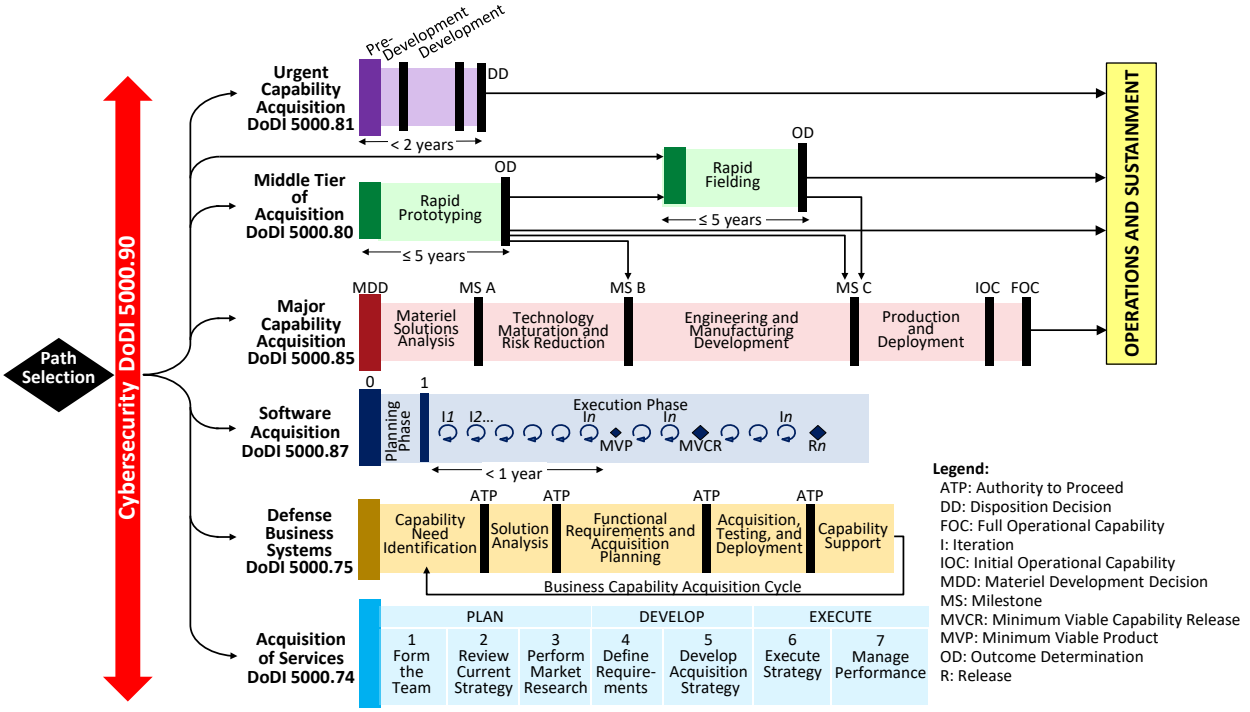
The sample contract language in this guide is provided for reference only. Acquirers should confirm all language with their respective legal authorities.

This guidance supplements the R&M Engineering Management Body of Knowledge (R&M BoK) available on the Systems Engineering and Architecture (SE&A) website R&M page. The R&M BoK was initiated before the DoW instituted the AAF and is organized according to a policy in place at the time for hardware-intensive programs. The BoK approach closely aligns with the current AAF MCA pathway. The R&M BoK and this guidance will be updated as needed to incorporate advanced R&M practices and current policy.

1 INTRODUCTION

1.1. Adaptive Acquisition Framework

The AAF pathways provide opportunities for Milestone Decision Authorities, Decision Authorities, and program managers (PMs) to develop acquisition strategies and employ acquisition processes that match the characteristics of the capability being acquired and deliver capability at the speed of relevance. See the Warfighting Acquisition University (WarU) AAF web page for a discussion of the AAF and guidance on selecting a pathway. The site provides detailed information on the pathways, policies, phases, and frequently asked questions. Figure 1-1 shows the six pathways of the AAF.



Source: DoDI 5000.02

Figure 1-1. DoW Adaptive Acquisition Framework

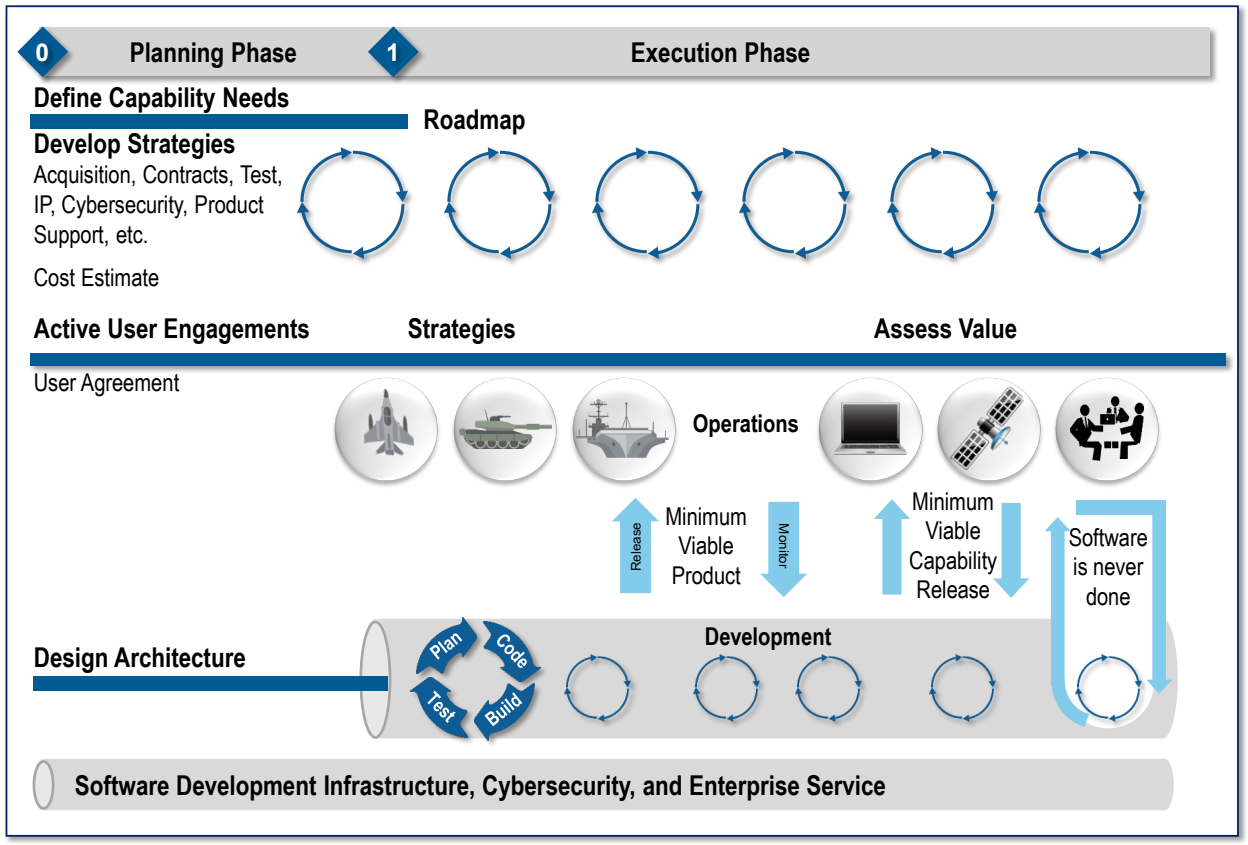
The DoW acquisition system is designed to allow the Department to acquire quality products that satisfy warfighter needs with measurable improvements to mission capability. The AAF is intended to shorten cycle times and enable programs to rapidly develop, acquire, and deliver capabilities to the warfighter.

1.2. Software Acquisition Pathway

Software is critical to national security, an integral part of DoW weapon systems, and vital to battlefield dominance. Software is an element in all advanced warfighting, cyber, physical, and

weapon systems and a driver of system performance, capability, security, functionality, complexity, and risk. Given the software-intensive nature of military systems, software R&M considerations are essential.

The Software Acquisition pathway (DoDI 5000.87) facilitates a rapid, iterative approach to software development by reducing costs, technological obsolescence, and acquisition risk. This pathway integrates modern software development practices such as Agile software development (see Agile Software Acquisition Guidebook (2020)), DevSecOps, and Lean practices. Programs use tightly coupled mission-focused government-industry software teams to employ automated tools for development, integration, testing, and certification so programs can deploy software capabilities iteratively to the operational environment. Figure 1-2 outlines the major activities and artifacts of the two phases of the Software Acquisition pathway that enable rapid and iterative software development and delivery.



Source: DoDI 5000.02.

Figure 1-2. Software Acquisition Pathway

The Software Acquisition pathway includes two paths: Applications and Embedded Software. With some exceptions, the guidance in this document applies to both paths equally.

- Applications Path: This path provides for rapid development and deployment of software running on commercial hardware, including modified hardware, and cloud computing platforms.
- Embedded Software Path: This path provides for the rapid development, deployment, and insertion of upgrades and improvements to software embedded in weapon systems and other military-unique hardware systems. The system in which the software is embedded could be acquired via other acquisition pathways (e.g., Major Capability Acquisition).

The overarching management principles that govern the DoW acquisition system are described in DoD Directive 5000.01, "The Defense Acquisition System," and in DoDI 5000.02. DoDI 5000.87 governs the operation of the Software Acquisition pathway. Software programs that meet the definition of a covered defense business system (DBS) should use the DBS pathway in accordance with DoDI 5000.75, "Business Systems Requirements and Acquisition," but may elect to incorporate the Software Acquisition pathway for custom-developed software.

Within the Execution phase, the Minimum Viable Product (MVP) is an early version of the software to deliver or field basic capabilities to users to evaluate and provide feedback. Insights from MVPs help shape scope, requirements, and design. The Minimum Viable Capability Release (MVCR) is the initial set of features suitable to be fielded to an operational environment that provide value to the warfighter or end user. The MVCR delivers initial warfighting capabilities to enhance some mission outcomes and is analogous to a minimum marketable product in industry.

Programs executing the Software Acquisition pathway are not subject to the standard requirements development and approval process (formerly the Joint Capabilities Integration and Development System (JCIDS)).[1] They will be handled as provided for by the Vice Chairman of the Joint Chiefs of Staff in consultation with the Under Secretary of War for Acquisition and Sustainment (USW(A&S)) and each Service Acquisition Executive. In addition, programs executing the Software Acquisition pathway will not be treated as Major Defense Acquisition Programs (MDAPs) even if exceeding thresholds in 10 USC 2430. See also the National Defense Authorization Act (NDAA) for Fiscal Year 2020, Section 800, "Authority for Continuous Integration and Delivery of Software Applications and Upgrades to Embedded Systems."

[1] An Office of the Secretary of Defense Memorandum of August 20, 2025, terminated the JCIDS process. The memo was reissued on November 7, 2025, under the name Office of the Secretary of War. Despite the termination, some programs have legacy JCIDS documentation (e.g., Capability Development Document (CDD)), which this guide acknowledges.

1.2.1. Planning Phase

As described in DoDI 5000.87,[2] the purpose of the Planning phase is to better understand the users' needs and to plan the approach to deliver software capabilities to meet those needs. The following five documents are required before advancing to the Execution phase:

- Capability Needs Statement (CNS)
- Acquisition Strategy (AS)
- Test and Evaluation (T&E) Strategy
- User Agreement
- Value Assessment

The Planning phase will be guided by a draft CNS developed by the operational community. The CNS is a high-level description of the mission deficiencies of, or needed enhancements to, existing operational capabilities, features, interoperability needs, legacy interfaces, and other attributes to respond to a threat environment. The CNS is intended to provide the program with enough information to define various software solutions. The sponsor will approve the CNS before the Execution phase starts.

The operational community should prioritize the required capabilities in the CNS to guide the software development. The operational community also should review the CNS periodically, at least as often as each value assessment, to determine whether updates are warranted. The system's key features are shaped by the CNS's results, ensuring it effectively addresses the gaps identified and meets the defined performance requirements.

Although programs using the Software Acquisition pathway are not subject to the standard requirements development and approval process (formerly JCIDS), the programs need to capture users' needs, priorities, and environment. The Military Service (sponsor) will oversee development of a draft CNS to support the initiation of a software acquisition using this pathway. The CNS should be clear and concise. Programs using the Embedded Software path will need to align the CNS with the requirements documents of the system(s) in which the software will be embedded.

The Acquisition Strategy describes the PM's plan to achieve program execution and programmatic goals across the entire program life cycle. It summarizes the overall approach to acquiring the capability (to include the program schedule, structure, risks, funding, and business strategy). It contains sufficient detail to allow senior leadership and the Milestone Decision Authority (MDA) to assess whether the strategy makes good business sense, effectively

[2] Section 1.2.1 and 1.2.2 descriptions of Software Acquisition pathway activities are taken or paraphrased from DoDI 5000.87, "Operation of the Software Acquisition Pathway."

implements laws and policies, and reflects management's priorities. Once approved by the MDA, the Acquisition Strategy provides a basis for more detailed planning. The Acquisition Strategy evolves over time and should continuously reflect the current status and desired goals of the program.

The T&E Strategy is an early T&E planning document that describes T&E activities starting with Technology Maturation and Risk Reduction (TMRR) and continuing through Engineering and Manufacturing Development (EMD) and Production and Deployment (P&D). The T&E Strategy describes how software being developed will be demonstrated in a relevant environment to support the program's transition into the EMD phase. Over time, the scope of the T&E Strategy will expand and evolve into the Test and Evaluation Master Plan (TEMP) due at Milestone B.

The User Agreement is a commitment between the sponsor and PM for continuous user involvement and assigned decision-making authority in the development and delivery of software capability releases.

The Value Assessment is an outcome-based assessment of mission improvements and efficiencies realized from the delivered software capabilities, and a determination of whether the outcomes have been worth the investment. The sponsor and user community perform an initial Value Assessment and update it at least annually, to inform Decision Authority and PM decisions.

The program office and related stakeholders will actively engage users throughout the software life cycle to understand their mission deficiencies, required enhancements to existing operational capabilities, cybersecurity requirements, features, interoperability needs, legacy interfaces, intelligence needs, threat intelligence, and other desired attributes.

During the Planning phase, the Decision Authority selects a PM and may establish a new program office or assign an existing program office to plan the software acquisition. The PM develops a constrained, tailored set of strategies to acquire, develop, and deliver the software capabilities, and will obtain the necessary resources (e.g., people, funding, technology) to effectively execute the strategies.

In mission-critical environments and safety-critical applications, software system safety is a foundational element of system safety and reliability engineering. Software system safety uses engineering principles to ensure software functions reliably and contributes an acceptable level of risk to the overall system, giving users confidence in the software's performance. While reliability intends to ensure consistent system performance over time, system safety and software system safety involve defining and conducting analysis to provide a sufficient level of confidence that a safety-critical or safety-related software function will perform as required.

- Safety as a Pillar of Trust: A system may meet performance and reliability metrics like uptime and low fault rates, but if system failures can cause harm, safety verification should be integrated throughout the entire development life cycle—from initial planning through deployment—to ensure safety is built in rather than added as an afterthought.
- Regulatory and Standards Alignment: High-assurance systems, particularly those developed under MIL-STD-882E, "System Safety," require comprehensive attention to system safety, software system safety, and reliability from the start. This alignment ensures compliance, certifiability, and mission assurance.
- DevSecOps and Safety Assurance Synergy: Modern DevSecOps practices including automated testing, continuous integration, and real-time monitoring can assist the program to maintain robust safety assurance while enabling agility and delivery velocity. These capabilities support early detection of safety-significant defects and continuous risk awareness.

1.2.2. Execution Phase

As described in DoDI 5000.87, the purpose of the Execution phase is to rapidly and iteratively design, develop, integrate, test, deliver, and operate resilient and reliable software capabilities that meet the users' priority needs. Programs will assemble software architecture, infrastructure, services, pipelines, development and test platforms, and related resources from enterprise services and development contracts. Leveraging existing services from enterprises and development contracts will be preferred over acquiring new ones to the extent consistent with the program acquisition strategy and intellectual property (IP)[3] strategy.

Programs will maximize use of automated software testing and security accreditation, continuous integration and delivery of software capabilities, and frequent user feedback and engagement. Programs will consider life-cycle objectives and will actively manage technical debt. Programs will use modern, iterative software practices to continuously improve software quality (e.g., iteratively refactor design and code, reduce cybersecurity vulnerabilities, and create effective modular open systems approaches to support future capabilities). Programs using the Embedded Software path will align test and integration with the overarching system testing and delivery schedules.

The sponsor and program office will develop and maintain a product roadmap to plan regular and iterative deliveries of software capabilities. The product owner and program office also will develop and maintain program backlogs that identify detailed user needs in prioritized lists. The backlogs allow for dynamic reallocation of current and planned software releases. Issues, errors,

[3] Intellectual property (IP) is described broadly as a work or invention that (1) is the product of the human intellect and (2) is protected from certain unauthorized use.

threats, and defects[4] identified during development and operations, including software updates from third parties or suppliers, should be captured in the program's backlogs to address in future iterations and releases. Regular stakeholder feedback and inputs will shape the product roadmap and program backlogs.

The PM and the sponsor will use an iterative, human-centered design process to define the MVP, recognizing that an MVP's definition may evolve as user needs become better understood. Insights from MVPs help shape scope, requirements, and design.

If the MVP does not provide sufficient capability or performance to deploy into operation, the PM and sponsor will use an iterative, human-centered design process to define an MVCR. The MVCR delivers initial warfighting capabilities to enhance mission outcomes. The MVCR for Applications path programs should be deployed to an operational environment within one year after funds are first obligated to acquire or develop new software capability (DoDI 5000.87). If determined sufficient to be fielded for operational use, the MVP becomes the MVCR. Subsequent capability releases should be delivered at least annually. Software updates to address cybersecurity vulnerabilities are released in a timely manner, potentially including out-of-release cycle as needed, according to the program's risk-based life-cycle management approach.

Programs will continuously improve or refine software development processes, practices, tools, and program strategies to reflect them. They should employ small, empowered teams and scale larger efforts across multiple teams. This includes integrating and aligning efforts across government and software development organizations. Continuous user feedback and self-assessments help balance investments between short-term capability deliveries and longer-term enduring solutions.

Software development testing, government developmental testing, and operational testing will be integrated, streamlined, and automated to the maximum extent possible to accelerate delivery timelines based on risk strategies. Automated test scripts and test results will be made available to the test community so that critical verification functions (e.g., performance, reliability, system safety, and software system safety) and validation functions (e.g., effectiveness, suitability, and survivability) can be assessed iteratively and incrementally. Automated cyber testing and continuous monitoring of operational software should be designed and implemented to support a continuous authority to operate (cATO)[5] or an accelerated accreditation process to the maximum extent practicable; and will be augmented with additional testing where appropriate in accordance with cybersecurity policies and in coordination with the authorizing official.

[4] For the purposes of this document, defects are the result of errors that are manifest in the system requirements, software requirements, interfaces, architecture, detailed design, or code. A defect may result in one or more failures. It is also possible that a defect will never result in a fault if the operational profile is such that the code containing the defect is never executed.

[5] The core concept of cATO is to build software security into the software development methodology so that the authority to operate process (as with the testing process) is done alongside development. If done correctly, an authority to operate is nearly guaranteed once the software is release ready.

Software system safety testing should be executed to ensure the software behaves as intended, particularly under normal, degraded, and fault conditions. Software safety testing provides objective evidence that the software performs safely and predictably in its operational context, including when faults occur, and should determine that the software meets the requirements.

The PM will iteratively develop and verify technical training materials that are synchronized with software deliveries throughout the software development lifecycle. The PM will deliver training materials that ensure that receiving users and military units can be trained to the appropriate level of proficiency and readiness to successfully execute the individual and collective tasks necessary to accomplish the mission supported by the software. The PM will deliver technical operator and maintainer manuals. Digital delivery of software manuals and automated training will be allowed and preferred. Every effort should be made to include all updated software manuals and automated training with each new release of software capabilities.

Programs using the Software Acquisition pathway will demonstrate the viability and effectiveness of capabilities for operational use not later than one year after the date on which funds are first obligated to develop the new software capability. New capabilities will be delivered to operations at least annually to iteratively meet requirements, but more frequent updates and deliveries are encouraged where practical. For programs using the Embedded Software path, this annual update applies after initial operational acceptance of the system in which the software is embedded and should be aligned with the associated system's schedule. Before the operational acceptance of the system in which the software is embedded, software will be delivered to an operationally representative environment at least annually.

To iteratively deliver software to meet the users' priority needs, programs will require government and contractor software teams to use modern iterative software development methodologies (e.g., Agile, or Lean), modern tools and techniques (e.g., DevSecOps), and human-centered design processes. These modern approaches will also instrument software such that critical monitoring functions related to the health, security, and operational effectiveness of the software can be automated to the maximum extent practicable.

Software development is conducted in collaboration with end users, representing key user groups, to ensure software deliveries:

- Address their priority needs.
- Maximize mission impact.
- Undergo regular assessment of software performance and risk.

Leveraging existing enterprise services, if available, is preferred over creating unique software services for individual programs. These existing services may be procured from the DoW, the

DoW Components, other government agencies, or commercial providers, and they may leverage category management solutions and enterprise software agreements.

With adversaries intent on stealing IP or taking down networks, cybersecurity is a huge concern. Consequently, cybersecurity and program protection will be addressed from program inception throughout the program's life cycle in accordance with applicable cybersecurity policies and issuances. A risk-based management approach will be an integral part of the program's strategies, processes, designs, infrastructure, development, test, integration, delivery, and operations. Software assurance, cybersecurity, and T&E are integral parts of this approach to continually assess and measure cybersecurity preparedness and responsiveness, identify and address risks, and execute mitigation actions.

IP will be addressed from program inception throughout the program's life cycle in accordance with DoDI 5010.44, "Intellectual Property (IP) Acquisition and Licensing," and other applicable DoDIs. IP considerations will be integrated with, and support, all other program strategies to ensure return on government investment and enhance competitive options for development, integration, test, deployment, modernization, approaches for modular open systems, and product support of software-intensive systems.

Software development testing, government developmental testing, software system safety assessment, security certification, and operational test and evaluation should be integrated, streamlined, and automated to the extent practicable to accelerate delivery timelines based on early and iterative risk assessments. Maximum sharing, reciprocity, availability, and reuse of results and artifacts among the various testing and certification organizations is encouraged.

Programs using the Software Acquisition pathway will report a set of data to the Office of the USW(A&S) on a semi-annual basis as defined in the AAF Software Acquisition pathway guidance on WarU. Data reported under this pathway will be used to monitor the effectiveness of the pathway and will not be used for program oversight. The Decision Authority documents the decision and rationale for a program to use the Software Acquisition pathway in an Acquisition Decision Memorandum.

Existing acquisition programs may elect to update their Acquisition Strategy to transition to the Software Acquisition pathway or to use Software Acquisition in addition to their current pathway. The PM and applicable stakeholders should identify, and the Decision Authority approve, a transition approach to tailor processes, reviews, and documentation to effectively deliver software capabilities.

Value assessments should be performed at least annually after the software is fielded to determine if the mission improvements or efficiencies realized from the delivered software are timely and worth the current and future investments from the end user perspective. More frequent value assessments are encouraged if practical.

2 REQUESTS FOR INFORMATION FOR THE SOFTWARE ACQUISITION PATHWAY

This section provides discussion, R&M guidance, and sample language for an RFI.

In accordance with DoDI 5000.88, in all defense acquisition programs, the Lead Systems Engineer (LSE),[6] working for the PM, will integrate R&M engineering into the overall engineering process and the digital representation of the system being developed. The LSE will plan and execute a comprehensive R&M program using an appropriate strategy consisting of engineering activities, products, and digital artifacts. The specific activities required depend on whether the acquisition is using the Applications or Embedded Software path. The activities can include:

- R&M allocations, System Reliability Model (SRM), and predictions
- Developing system architecture
- Failure Definition and Scoring Criteria (FDSC)
- Software Failure Modes and Effects Analysis (SwFMEA)
- Fault Tree Analysis (FTA)
- Maintainability and built-in test (BIT) demonstrations
- Reliability testing at the system and subsystem level
- A Failure Reporting, Analysis, and Corrective Action System (FRACAS) maintained through the life cycle

The RFI is the initial opportunity to ensure that R&M engineering activities are integrated into the overall engineering process.

2.1. Purpose

Before developing an RFP, the Government acquisition team may issue one or more RFIs. The purpose of an RFI is to serve as a solicitation document used for market research, to obtain general information from suppliers about their products, services, and capabilities. An RFI is seldom the final stage but is commonly used in combination with an RFP or similar solicitation.

[6] The R&M engineer is responsible to the LSE for developing the R&M engineering program, overseeing the implementation of the R&M engineering activities, and coordinating with the LSE in evaluating risk areas and progress in meeting the R&M specifications.

2.2. RFI Sample Language

Table 2-1 shows sample language for an RFI. The information gained from an RFI will help the program office determine the potential of each alternative system to fulfill the operational mission. The intent is to have the contractors describe their design approach and, if they make R&M projections for that approach, to state how these projections were determined. It also provides an opportunity for each contractor to submit supplemental data to substantiate their R&M projections. The R&M projections should be for the anticipated field configuration. Contractor format is acceptable, and modeling results in lieu of formal presentations and reports are acceptable. The responses to the RFI will help the acquiring organization to develop the RFP for a Software Acquisition pathway program.

Table 2-1. Sample RFI Language

(1) Provide an overview of your software reliability (R(t)) program.
(2) Describe the planning and implementation of reliable software activities as well as coordination with reliability, test, design, systems, hardware, software, firmware, and field-programmable software and hardware engineering.
(3) Describe how you assess a software system and identify software failures/defects.
(4) Describe how you predict, allocate, and assess reliability of software, firmware, field-programmable gate array (FPGA) code, commercial off-the-shelf (COTS),[7] commercial items (CI), government off-the-shelf (GOTS), government-furnished software (GFS), and free and open source software (FOSS).
(5) Describe the environmental and usage conditions and mission profile(s) for the system-level reliability and maintainability (R&M) predictions and compare/contrast with usage conditions and mission profile(s) for this program. Provide system-level R&M predictions, using fielded performance for applicable R&M measures: (a) Reliability measures (mission and logistics) (b) Maintainability measures (to repair mission failures and logistics failures) (c) Direct maintenance corrective and preventive maintenance measures (d) Built-in test (percentage of faults detected, percentage of faults isolated, False Alarm Rate) (e) Operational availability

The IEEE 1633-2016 definition of software reliability is (1) the probability that software will not cause the failure of a system for a specified time under specified conditions, or (2) the ability of a program to perform a required function under stated conditions for a stated period. See also section 3.2.4, “Differences between Hardware and Software Reliability.”

[7] A commercial off-the-shelf (COTS) item is a commercial item sold in the exact form in substantial quantities. A single change or a new design will result in the item being a commercial item (CI). A CI is not sold in substantial quantities and, compared with COTS, would require additional analyses (e.g., parts count or stress analysis) to confirm its reliability characteristics. See the Federal Acquisition Regulation (FAR), Part 2.101 Definitions, for more information on commercial products in general and COTS specifically.

3 REQUEST FOR PROPOSAL FOR THE SOFTWARE ACQUISITION PATHWAY

This section discusses RFPs.[8] It provides R&M guidance and sample language and assists the R&M engineer to identify the engineering activities that should be placed on contract.

3.1. Purpose and Structure of the RFP

The RFP is a solicitation used in negotiated acquisition to communicate Government requirements to the prospective contractors and to solicit proposals.[9] At a minimum, the Federal Acquisition Regulation (FAR) requires that solicitations describe the Government's requirement, anticipated terms and conditions that will apply to the contract, information required in the Offeror's proposal, and (for competitive acquisitions) the criteria that will be used to evaluate the proposal and their relative importance. Official information is provided in FAR Subpart 15.2, Solicitation and Receipt of Proposals and Information; DFARS Part 215, Contracting by Negotiation; and the DoD Source Selection Procedures.

The process for developing an RFP consists of six steps:

Step 1: Conduct market research (see FAR Part 10)

Step 2: Determine the functional and non-functional requirements for the system (See FAR Part 1, Market Research).

Step 3: [Optional] Write a draft RFP.

Step 4: [Optional] Share the draft RFP with industry to obtain feedback.

Step 5: Finalize the RFP.

Step 6: Release to potential Offerors.

FAR 15.204, Contract Format, specifies a Uniform Contract Format (UCF) for a Government RFP, with the following sections:

Section A – Solicitation/Contract Form (SF-33)

Section B – Supplies and Services and Prices/Costs

Section C – Description/Specifications/Statement of Work

[8] See also FAR 15.203, Requests for Proposals, and MIL-HDBK-245E for details on preparing an RFP.

[9] A draft RFP may be used to solicit comments and ideas from interested parties. These inputs would then be used to revise the final RFP.

Section D – Packaging and Marking

Section E – Inspection and Acceptance

Section F – Deliveries or Performance

Section G – Contract Administration Data

Section H – Special Contract Requirements

Section I – Contract Clauses

Section J – List of Attachments

Section K – Representations, Certifications, and Other Statements of Offerors

Section L – Instructions, Conditions, and Notices to Offerors

Section M – Evaluation Factors for Award (unnecessary for sole-source acquisitions)

Section C includes the system specification and the contract Statement of Work (SOW). The specification includes quantitative technical requirements. The SOW lists tasks and deliverable data. The deliverable data is required by way of the DoW Contract Data Requirements List (CDRL) and appropriate list(s) of Data Item Descriptions (DIDs) and/or Negotiated Data Deliverables (NDDs).

The DoW maintains a catalog of standardized DIDs that cover a range of data items used in various DoW programs. Using standardized DIDs promotes interoperability and data sharing across the DoW. The guidance is to use the DIDs if possible and to define NDDs in those cases where the DIDs do not exist to meet the need. Once an NDD is created, it should be submitted as a DID to add integrity and sustainability to the new data definition.

One of the primary purposes of the specification and SOW is to ensure the contractor and the Government agree on all the terms for the acquisition program, so the specification and SOW need to clearly define all requirements to allow a reasonable and accurate response by the contractor.

Although the UCF indicates that the specifications and SOW belong in Section C of the RFP and contract, the usual and accepted practice is to attach them to the RFP or contract (the list of attachments is in Section J of the UCF) and reference the attachments in Section C. The following paragraphs suggest language for a requiring organization to use to incorporate R&M engineering activity requirements into the specification and the SOW, to result in a clear RFP and therefore a strong and effective contract. This guidance document focuses on Sections C, J, L, and M. The other sections are of less or no concern to the R&M engineer and are properly the focus of contracting specialists.

3.2. Contract Section C – Guidance for the Specification

The system specification includes quantitative system R&M requirements, which should be written in clear, conventional language. The specification should identify the associated system and should identify specific subsystems, equipment, and software to be included in the design and performance definitions.

The specification should list all system components or subsystems to be supplied as Government-furnished equipment (GFE) and should describe GFE R&M characteristics. The specification should provide this information for any special item, whether existing or in development, that is an integral part of the system concept.

Table 3-1 provides a list of the specification requirements and verification provisions. These requirements contain technical content for the design and quantitative R&M performance requirements placed in Section 3 of the specification and the verification criteria included in Section 4 of the specification.

Table 3-1. Specification Outline

Specification Section	Content
Section 2 – Applicable Documents	List documents referenced in sections 3 and 4 of the specification
Section 3 - Requirements	Quantitative R&M performance requirements
	Mission profile
	Definitions for Reliability (i.e., failures), Maintainability (i.e., bug fixes, failure recovery)
	Qualitative design requirements
Section 4 - Verification Provisions	Responsibility for test
	Classification of tests
	Rules for conduct of tests/demonstrations
	Description of R&M tests/demonstrations

The requiring organization can avoid creating unrealistic or ambiguous requirements or requirements that conflict with information in referenced documents (i.e., handbooks, standards) or in the specification itself[10] by validating and assessing the feasibility of requirements.

The specification generally is not used to task contractors to perform work tasks, or for specifying requirements for deliverable data that are addressed in the SOW and contract deliverables. MIL-STD-961E provides additional information on the format and content of a specification.

3.2.1. Quantitative R&M Performance Requirements

As is true for all acquisition programs, a software specification should define the level of performance, operating conditions, mission profile, use environment, failure definitions, and design constraints in quantitative terms. For the Software Acquisition pathway, the operational R&M requirements are included in the CNS. For software developed using the MCA, MTA, or UCA pathways, the requirements are provided in the Capability Development Document (CDD), stated in Service-unique terms.

In any case, R&M threshold should be validated via the Reliability, Availability, Maintainability, and Cost (RAM-C) analysis and RAM-C Rationale Report and then translated to design-controllable R&M requirements for inclusion in the specification.

The R&M engineer converts (translates) the requirements into quantitative contractual specifications. At a minimum, the specification should include the following contractual R&M requirements:

- *Mission Reliability.* The measure of the ability of an item to perform its required function for the duration of a specified mission profile, defined as the probability that the system will not fail to complete the mission, considering all possible redundant modes of operation. Includes all design-controllable failures that would prevent the system from performing its mission(s).
- *Logistics Reliability*. The measure of the ability of an item to operate without placing a demand on the logistics support structure for repair or adjustment, including all failures to the system and maintenance demand because of system operations. Includes all design-controllable failures that place a demand on the logistics system.
- *Maintainability* – Includes maintenance burden, corrective and preventive maintenance support, and direct maintenance support.

[10] The contract is the only legal document committing a contractor to deliver items, data, and services in accordance with specified requirements under agreed-upon terms and conditions. With its other requirements, the contract should include the R&M requirements, terms, and conditions that the requiring organization initially outlined in the RFP. 10 U.S.C. 4328, Weapon System Design: Sustainment Factors, addresses PM responsibilities for emphasizing R&M requirements, activities, and source selection criteria early during weapon systems design.

- *Built-In Test* – Includes fault detection, fault isolation, and false alarm rates. BIT can be implemented using software, which often involves specialized diagnostic routines that are part of the system under test.

Maintainability requirements derived from the operational thresholds should be compatible with the derived reliability requirements. The reliability, maintainability, maintenance concept, and logistic support analysis for the system should be adjusted during the system requirements analysis process to be compatible with the existing design constraints and program limitations. The relationship among reliability, maintainability, product support, and operations and support (O&S) cost must be acknowledged early in the formative stages of system design. The data from analyses conducted for these areas should be coordinated throughout the product life cycle.

The requiring activity should include the following details in the specification.

- *Design Requirements* – The translation of the R&M thresholds from the CNS, Initial Capabilities Document (ICD), draft CDD, or CDD[11] to the quantitative specification measures that the contractor can influence through the design or manufacture of the system.
- *Operational Mode Summary/Mission Profile (OMS/MP)* – A document describing how a system or training device will be used in wartime or peacetime at the time it is fielded, with focus on the future. The OMS/MP is also typically used for setting the Reliability, Availability, and Maintainability (RAM) goals in an early phase of weapon system development. An OMS/MP projects the anticipated variety of ways the software will be used for each moment of time to include both peacetime and wartime. It also includes the percentage of time the system will be exposed to each type of environmental condition and terrain. The Combat Developer produces the OMS/MP following development of the system Concept of Operations (CONOPS)[12] and uses the OMS/MP to determine the maintenance activities that will be conducted at each level.

[11] An ICD, rather than a CDD is used on the Software Acquisition pathway. A CDD is used when the software development it is supporting an MCA pathway program.

[12] A CONOPS is a verbal or graphic statement of a commander's assumptions or intent regarding an operation or series of operations. The CONOPS is frequently embodied in campaign plans and operation plans, particularly when these plans cover simultaneous and successive operations. The CONOPS presents an overall picture of the operation with the intent of providing additional clarity of purpose.

- *Mission Profile* – A description of environmental and use duty cycles throughout the mission period for which reliability is specified. The mission profile describes the time sequence of operational events required to accomplish mission objectives and is related to the time the software is operating with sub-conditions such as standby, alert time, recovery, and secure or deactivation time. The mission profile should define all the significant objectives and constraints that affect each special mission. A mission constraint is a limit or rule that a variable cannot be permitted to exceed under any condition.
- *Use Conditions* – A description that should include anticipated installation interfaces, interference characteristics of adjacent or associated systems, interactions with support systems, and the environments with which the system is to be compatible during its life cycle. The description should include packaging, handling, storage, transportation, maintenance, test, and checkout as well as operational conditions.
- *Definition of Failure* – The definition of failure for the software in relation to its important performance parameters needs to be clear and understood by all parties. Clearly state the definition of failure for the software in relation to its important performance parameters.
- *Test Requirements* – The R&M demonstration and test requirements and the acceptance criteria by which the system will be evaluated for conformance to the requirements.
- *Clarifying Notes* – Notes and R&M evaluation criteria (i.e., failure definitions and scoring criteria) intended to eliminate ambiguity or misunderstanding in specified requirements.

3.2.2. Value Engineering

Value engineering (VE) is a systematic technique that analyzes the functions of systems, equipment, facilities, services, and supplies to ensure they achieve their essential functions at the lowest life cycle cost (LCC) consistent with required performance, reliability, quality, and safety. DoDI 4245.14, "DoD Value Engineering Program," implements Section 1711 of Title 41, United States Code, and Office of Management and Budget (OMB) Circular No. A-131 by establishing policy, assigning responsibilities, and defining authorities for the effective administration of the DoW VE Program.

The Government can incorporate VE principles into annual value assessments by requiring the contractor to address the questions below. The goal is to enable a thorough evaluation of mission improvements, efficiencies, and the overall return on investment for the delivered software capabilities:

- Can some other architecture perform the same function more effectively or at less cost with equal effectiveness?
- Is there a more effective hardware or software mix?
- Are user requirements too restrictive or excessive?
- Can a commercial product or a custom product or modifications to existing products provide better value?
- Are any test procedures, operations, or steps unnecessary?
- Are there alternatives (products, requirements, procedures, or methods)?
- Is there a more efficient way to accomplish a function or process?
- What is the most efficient pace for developing and fielding new capability?
- Are there opportunities to add value associated with hardware development of procurement?

A contractor VE program will assist the Government in value assessments and can be voluntary or required by contract; however, the requiring organization should validate and assess the feasibility of requiring contractors to have a VE program.

3.2.2.1 Value Management

The following language may be included in a contract to establish a Value Management Program that defines VE actions:

> The contractor shall establish and maintain a Value Management Program in order to apply value engineering/value analysis techniques to continuously review and analyze systems, projects, equipment, facilities, services, and supplies for the purpose of achieving the essential functions at the lowest life cycle cost consistent with required levels of performance, reliability, quality, or safety. Specifically, a contractor Value Management Program shall assist the Government in value assessments and may be voluntary or required by contract; however, the requiring organization shall validate and assess the feasibility of requiring contractors to have such program. Value improvement solutions shall be considered for formal submission of Value Engineering Change Proposals (VECPs) to reduce Government contract costs. The contractor may use SD-24 and FAR 52.248 as additional guidance for value management and VECPs.

3.2.2.2 Value Engineering Change Proposals

FAR Part 48 prescribes policies and procedures for using and administering value engineering techniques in contracts. FAR Part 52.248-1 encourages contractors to propose changes in the form of VECPs that can reduce the life cycle costs of projects while maintaining performance and quality standards. Contractors should consider proposing VECPs to (1) incorporate another more cost-effective architecture, (2) introduce commercial off-the-shelf (COTS) or custom

products to provide better value, or (3) modify established procedures and methods to reduce program costs while maintaining essential functions and requirements.

Regarding FAR VE guidance:

- *Contract Thresholds:* The requirement to include the 52.248-1 in contracts is based on the simplified acquisition threshold. FAR 52.248-1 may also be included in contracts of lesser value. Refence FAR 48.2 for exceptions to clause inclusion.
- *Contract Types:* The VE clause may be used in contract types such as incentive, fixed price, and cost reimbursement.
- *VE Approach:* The contracting officer includes either the standard VE incentive clause or a VE program requirements clause to inform the contractor of government agency expectations. The incentive clause allows the contractor to voluntarily submit VECPs. The program requirements clause is a modification to the incentive clause in which the government specifies a contractor VE program, but that may or may not result in viable VECPs.
- *VECP Requirement:* The VECP must generate net acquisitions savings to the Government and must change the instant contract to implement. See FAR 52.248-1 (b) (2) for restrictions to the type of change. Net acquisition savings are shared with the contractor that submitted the VECP.

3.2.3. Verification Provisions

Every specification requirement should have associated with it some means of verifying that the requirement has been met. Verification is the activity of checking that the design or production of an item (e.g., component, equipment, or system) meets the mandatory functions for or attributes of the item. Following are four fundamental methods of verification and hypothetical examples of each.

1. *Demonstration* – The performance of operations at the system or system element level where visual observations are the primary means of verification. Demonstration is used when quantitative assurance is not required for the verification of the requirements.
    - Aircraft: Start the aircraft and ensure the radar system is operating normally.
    - Software: Enter the required fields on a screen and select the button to return a specific report. Ensure that the report is returned with the type of data needed.
2. *Inspection (Examination)* – Visual inspection of equipment and evaluation of drawings and other pertinent design data and processes. The inspection should be used to verify conformance with characteristics such as physical, material, part, and product marking and workmanship.

- Aircraft: Visually inspect to ensure there are no obvious problems with flight controls.
- Software: Visually examine that requested screens appear correctly.

3. *Analysis* – The use of recognized analytic techniques (including computer models) to interpret or explain the behavior/performance of the system element. Analysis of test data or review and analysis of design data should be used as appropriate to verify requirements.
   - Aircraft jet engine: Complete a series of tests running the engine at specific throttle settings for a set length of time, while monitoring thrust. Use this information to model the engine's thrust versus rpm curve.
   - Software: Sample and correlate measured data and observed test results with calculated expected values to establish conformance with requirements.
4. *Test* – An activity designed to provide data on functional features and equipment operation under fully controlled and traceable conditions. The data are subsequently used to evaluate quantitative characteristics.
   - Aircraft: Advance the throttle and monitor engine gas temperature and fuel flow.
   - Software: Enter the values of an equation and exercise the software to produce the result. Check to ensure the result is correct.

Of these methods, testing is the most precise and controlled form of verification. An item is tested to confirm that it behaves precisely as specified under a set of carefully specified test conditions and using different sets of test conditions. Testing often is used to verify performance requirements, beginning with components, and progressing to higher levels of design, eventually reaching the system level. System-level testing is possible only near the end of a development program, however, and testing an entire system, such as an aircraft or ship, is extremely expensive. Using the other methods of verification throughout the development process is essential and reduces the risk of failing to meet system performance requirements.

3.2.4. Differences Between Hardware and Software Reliability

The ANSI/IEEE Standard Glossary of Software Engineering Terminology, STD-729-1991 defined software reliability as the probability that software will provide failure-free operation for a defined use and interval of time. Unlike hardware faults, which are physical faults, software faults are non-physical faults due to design, environment, or data. These are harder to visualize, classify, detect, and correct. Failures tend to be use driven and time independent.

Software does not wear out like hardware; however, software may cause failures from many different root causes. Due to the immense size of today's complex software-intensive systems, finding all the root causes in development and test is a challenge given time and budget constraints. For software, the likelihood of each failure is driven by:

- How detectable the underlying defect is in development and test.
- Whether there are any controls over the failure.
- The level of rigor of the test activities.

Software does not have to be "down" to cause a major function failure. Software can cause failures even when operating by:

- Executing irreversible actions or decisions that contribute to a hazardous event.
- Executing a required function incorrectly.
- Executing the function at the wrong time or order.
- Inadvertently executing a function in the wrong state.
- Not executing a function at all when commanded.
- An inability to detect and recover from faults in itself and in the system.
- Causing degraded function or malfunction of the subsystems, components, and interfaces.

Hardware reliability is based on the measure of its design and failure mechanisms, depending on its expected environment conditions (e.g., mission profile, temperature, humidity, vibration). Software failures, conversely, are not a result of external environmental conditions. Conditions that may induce software failures are harder to identify because software deals with process states, data quality, system loading, and other factors. Another significant difference is that hardware failure mechanisms can be understood independent of the mission. On the other hand, software failures are almost exclusively tied to the mission and cannot be understood without the mission context. To have highly reliable software, rigorous and disciplined development and thorough testing are needed.

3.2.5. Interoperability and Vendor-Agnostic Requirements

Contractors should demonstrate the ability to integrate with a diverse set of large language models (LLMs) and operate across multiple cloud and on-premises environments. This is critical for future-proofing our acquisitions and maintaining operational flexibility.

- The system specification should mandate interoperability across multiple LLMs and platforms, ensuring no vendor lock-in. The contractor should demonstrate the ability to integrate and operate seamlessly with Government approved artificial intelligence (AI) models. This includes support for model-agnostic training and deployment across cloud-agnostic environments and at the edge, on-premises, or air-gapped environments.

- The contractor should provide evidence of scalability and sustainability in ingesting data across multiple LLM stacks without duplicative efforts. This includes a unified platform approach to minimize redundancy and ensure efficient data ingestion and management.

3.2.6. Software Definitions

IEEE 1633-2016 established definitions for software reliability, software reliability engineering, and software quality (Table 3-2). Also, IEEE 1633-2016 established definitions of software defects and failure (Table 3-3). According to ANSI, software reliability is the probability of failure-free software operation for a specified period in a specified environment.

Software reliability engineering applies to both development and operations. Software quality and reliability have significantly different definitions: software quality is associated with how the functionality of the software compares with some known standard (specifications, attributes, expectations, needs) while reliability focuses on the period the software continues to operate under specified conditions in an acceptable manner (usually without failure).

Table 3-2. Fundamental Software Quality/Reliability Definitions

Term	IEEE 1633-2016 Definition
Software Reliability (SReliability)	▪ The probability that software will not cause the failure of a system for a specified time under specified conditions. ▪ The ability of a program to perform a required function under stated conditions for a stated period.
Software Reliability Engineering (SRE)	▪ The application of statistical techniques to data collected during system development and operation to specify, estimate, or assess the reliability of software-based systems probabilistically.* ▪ The application of software reliability best practices to enhance reliability characteristics of software being developed & integrated into a system.
Software Quality (SQ)	▪ The totality of features and characteristics of a software product that bear on its ability to satisfy given needs, such as conforming to specifications. ▪ The degree to which software possesses a desired combination of attributes. ▪ The degree to which a customer or user perceives that software meets the user's composite expectations. ▪ The composite characteristics of software that determine the degree to which the software in use will meet the expectations of the customer. ▪ Capability of the software product to satisfy stated and implied needs when used under specified conditions.

* In this definition, probability is a function of inputs to and use of the system, as well as a function of defects in the software. The inputs to the system determine whether existing defects, if any, are encountered.

Table 3-3. Definitions Related to Defects and Failures

Term	IEEE 1633-2016 Definition
Error	A human action that produced an incorrect result, such as software containing a fault.
Defect	A problem that, if not corrected, could cause an application either to fail or to produce incorrect results.
Fault	A defect in the code that can be the cause of one or more failures. A manifestation of an error in the software.
Failure	The inability of a system or system component to perform a required function within specified limits. The termination of the ability of a product to perform a required function or its inability to perform within previously specified limits. Departure of program operation from program requirements. Failure may occur when a fault is encountered and a loss of expected service results.
Problem	Difficulty or uncertainty experienced by one or more persons, resulting from an unsatisfactory encounter with a system in use. A negative situation to overcome.

Notes: (1) For the purposes of this document, defects are the result of errors that are manifest in the system requirements, software requirements, interfaces, architecture, detailed design, or code. A defect may result in one or more failures. It is also possible that a defect will never result in a fault if the operational profile is such that the code containing the defect is never executed. (2) A failure may be produced when a fault is encountered and loss of the expected service to the user results. (3) There may not be a one-to-one relationship between faults and failures. This disconnect can happen if the system has been designed to be fault tolerant. It can also happen if a fault either does not result in a failure because it is not severe enough to result in a failure or does not manifest into a failure due to the system not achieving that operational or environmental state that would trigger it.

3.3. Contract Section C – Guidance for the Statement of Work

The SOW is the contract vehicle for defining the work to be performed by contractors in support of an acquisition program. Preparing the SOW is an important step in planning and defining the acquisition process and work responsibilities. R&M activity descriptions are included in section 3 of the proposed SOW and serve to implement the R&M program outlined in the RFP. The description of all R&M activities involving design verification and data collection should be explicit. The general format for the SOW is shown in Table 3-4. This format is generally applicable to all acquisition phases. Refer to MIL-HDBK-245E for additional information on SOW format and content.

R&M engineering activities should be fully integrated within the program's systems engineering process. The R&M program plan should address the entire life cycle; however, the SOW for each contract will contain only the contractor's execution of the required activities appropriate to the program phase and that can be accomplished during the contract period of performance.

Table 3-4. Statement of Work Outline

SOW Section	Content
1. Scope	This section includes a brief description of SOW coverage. This section should not include direction to the contractor to perform work activities, discuss data requirements, or identify deliverable products.
2. Applicable Documents	Section 2 should list only documents referenced in the SOW Section 3, Requirements. Contractual citing of standards, specifications, and other documents needed to clarify the work activity should be limited to currently available documents in effect at the time the contract is executed. Referenced documents should be cited specifically and directly by number and title. Listing documents in this section without referencing them in the SOW Requirements section can adversely affect program costs by adding unnecessary data requirements.
3. Requirements	This section includes the specific work tasks (activities) the contractor must perform to satisfy program needs, technical objectives and goals, and specific design requirements. Activities generally are dictated by program requirements but should be presented in chronological order. The R&M engineer should tailor the R&M engineering activities by selecting those that are applicable, beneficial, and cost-effective for the program. The description of activities should be complete and stated in clear, plain language. Any references to standards or other sources should be accurate, current, and applicable to the requirements the contractor must fulfill. If the requirements or references are ambiguous, the contractor may assume total compliance is required and encumber the program with unnecessary costs. This section of the SOW should not be used to specify design requirements.

The tailoring guidance provided herein assumes that the quantitative R&M requirements, FDSC, and other requirements were used in developing the performance requirements and defined verification methodology in the system specification. If there will be a down-selection at the end of the contract based, in part, on demonstrated or projected R&M performance, language explaining how the R&M data will be used in the down-selection process should be included in the contract as appropriate.

3.3.1. R&M Engineering Activities

Program-related R&M activities may involve R&M analyses and tests, program plans, subcontract management and controls, problem and risk identification and control, fault/defect review processes and forums, and other program requirements essential for an effective R&M engineering program and practical for a Software Acquisition pathway program. General reference to guidance documents or standards is insufficient for contractor planning, execution, or cost analyses.

Following are examples of key R&M points to consider when developing contractual language.

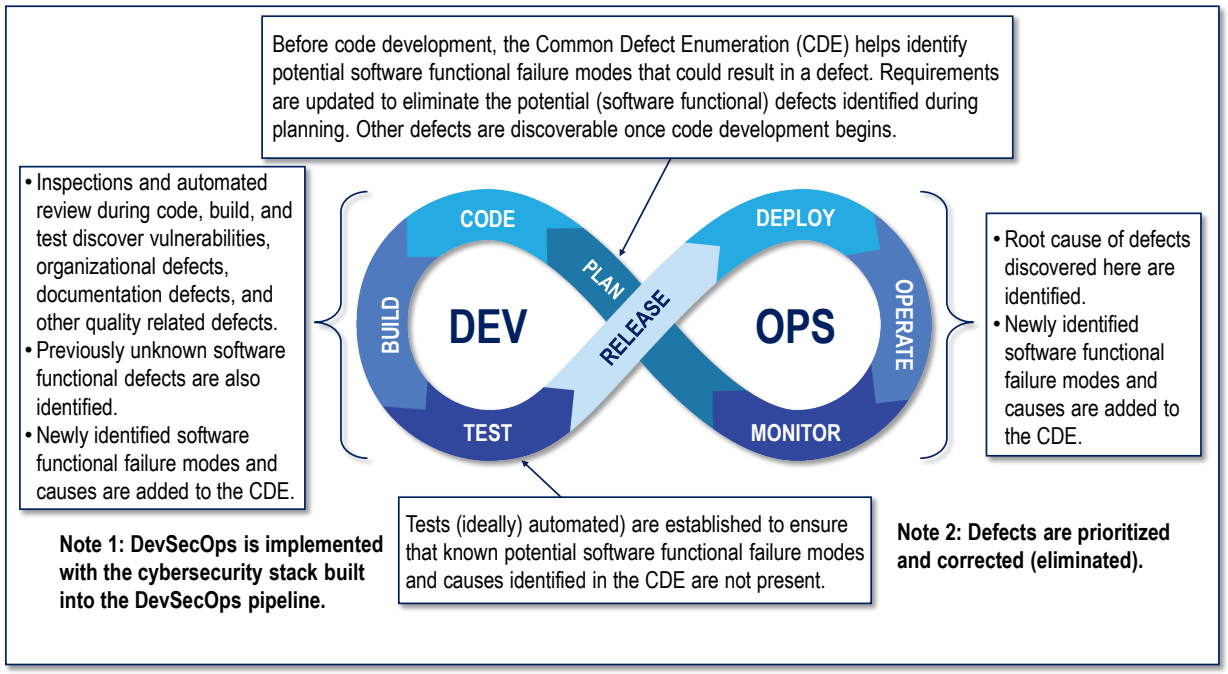
1. Reliability parameters such as MTBF or MTBOMF are difficult to estimate because methods to predict quantitative values for them are ill-suited to software or IT systems that are typically developed through the Software Acquisition pathway. Instead:
    - Use downtime parameters such as mean restore time or recovery time.
    - Ensure design constraints drive the software development to meet mission timelines.
    - Ensure the design includes the failure recovery architecture.
    - Understand how operational mission degradation caused by software downing events, may or may not affect operational availability.
    - Provide criteria on the amount time allowed to recover from degraded failures.
    - Provide limits on the number of allowable corrective actions for software reboots and the duration of downtime for all allowable corrective actions acceptable to the user. Ideally limit allowable corrective actions on redundant items within the system. Depending on the nature, and associated downtime, downing events may affect A_O or cause increased burden on the operator (e.g., constant resets nuisance factor).
    - Define downtime (DT) to include time to implement software patches, installation of new releases, etc., should ensure the cause of the downing event can be attributed to either the system or the infrastructure (i.e., power, cooling, facilities, enterprise hardware, network, software services, and external interfaces). Define the infrastructure boundaries e.g., enterprise hardware, network, software services.
2. Software for most systems will continue to change and evolve while the system is used, and the R&M activities will mirror the extent of development being completed.
    - Software will have continuous updates for security, bug fixes, refactoring and user enhancements. The program should analyze these changes to ensure that the system's R&M performance does not degrade over time.
    - Using the agile DevSecOps Iterative continuous integration/continuous delivery (CI/CD) acquisition model for the Software Acquisition pathway, defects are continually evaluated and prioritized, with continuous automated testing and frequent user involvement.
    - Assessments should focus on Computer Software Configuration Items (CSCIs) with large numbers of discrepancies or late discovery defects (defects not found in unit or integration tests). These may indicate changes needed in the architecture or testing.
    - It is essential that software be tested for stressing usage, fault injection and for fuzz (corner cases, erroneous data/input, and valid input out of range or inconsistent) to verify error and exception handling meets the mission requirement needs.

3. Failure Modes and Effects Analysis (FMEA)

- For software, a qualitative criticality analysis, similar to methods described in SAE Standard 1025, should be performed. This analysis assesses risk based on the severity of effects and a qualitative likelihood of occurrence, which considers factors such as defect existence and controls. Traditional hardware-based quantitative criticality analysis remains unsuitable for software.[13]
- The SwFMEA should be performed to assess the severity of the effects of software component/subsystem failure modes on system performance.
- The SwFMEA should incorporate relevant views (e.g., Interface, Functional, and Usability). For software developed under the MCA pathway, a preliminary analysis would be expected by PDR with the final by CDR. For software developed using the Software Acquisition pathway, an initial SwFMEA should be completed during the Planning phase and updated as needed as the code is being written, tested, and released. An alternative would be to conduct a software fault tree to identify what can go wrong with the software (this is typically less expensive than a SwFMEA).
- The detection methods and mitigations from the SwFMEA informs the development of the error and exception handling concept for the Software Development Plan (SDP).[14]
- Individuals who understand the software, the mission to be performed by the software, and potential software failure modes should conduct the SwFMEA. Effective SwFMEAs typically are conducted by an integrated product team with inputs from engineers, software developers, and analysts.
- The SwFMEA should identify Common Defect Enumeration (CDE). The CDE provides a listing of software defects applicable for virtually all software intensive systems. Figure 3-1 shows the goals of the CDE within a continuous development environment. The goal for the CDE is to include defects that:
    - Can be tested.
    - Are not detected by automated code analysis tools.
    - Represent the things that can and have gone wrong with software systems.
    - Can be identified in the specifications and design as opposed to code reviews.
    - Are less expensive to fix earlier rather than later.

[13] For software, a separate criticality analysis is the Mission-Critical Function and Critical Component risk assessment. See DoDI 5200.44, "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks (TSN)," for more information.

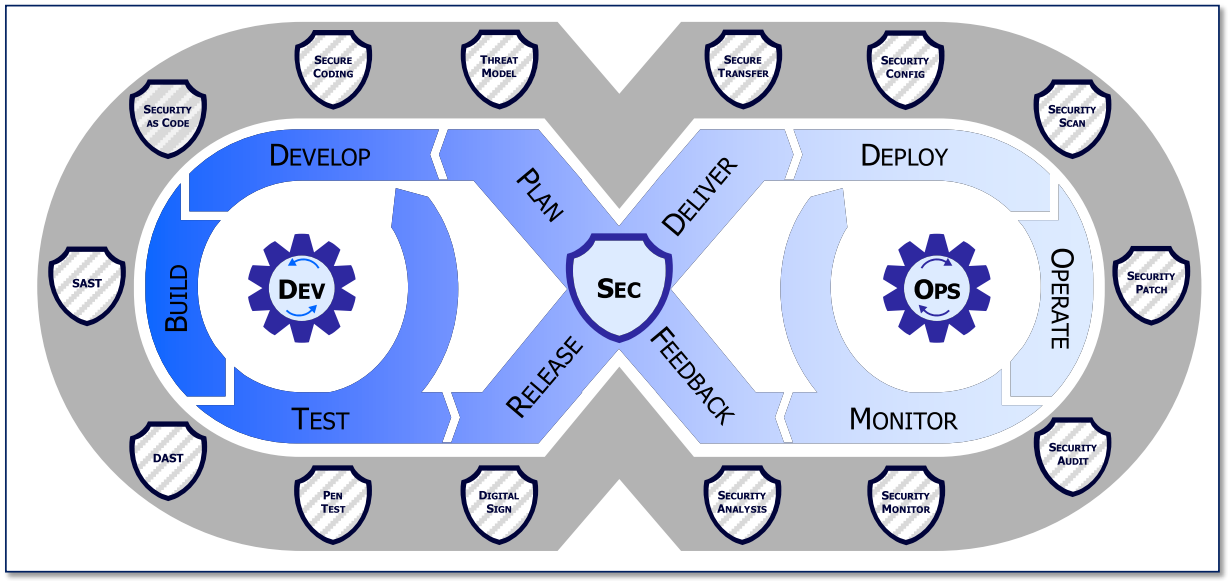
[14] For software developed using the Software Acquisition pathway using an Agile Software Development strategy, the SDP is required to be developed in the Planning phase. See Data Item Description DI-IPSC-81427B, Software Development Plan.



Source: FCDD-AMR-MR-22-08 (2022).

Figure 3-1. Goal of the CDE within DevOps

As early as 2019, the DoW began transitioning from a DevOps to a DevSecOps strategy. As noted in Figure 3-2, DevSecOps is implemented with the cybersecurity stack incorporated in the DevOps pipeline.[15]



Source: DoD Enterprise DevSecOps Strategy Guide, V 2.0, March 2021.

Figure 3-2. DevSecOps Model

[15] For more information see the DevSecOps Community of Practice website: https://software.af.mil/dsop/community-of-practice/.

4. The SDP and TEMP should include software test methods to identify and correct software failures and that there is high degree of confidence the system can be recovered from any software failures that may occur after fielding.
    - Ensure that design constraints drive the software development to meet mission timelines (e.g., 15-minute processing requirement upon receipt of data).
    - The defect find versus fix rate should be evaluated to ensure the software baseline is stable for the production system.
    - Software use cases or equivalent should be performed to address the concept for deploying initial and subsequent releases, patches (Operating System, COTS, government off-the-shelf (GOTS), and applications) and failure recovery for each applicable level (self, on-site administrator, help desk, remote).
    - Analyze restarts of system, applications, and processes occurring during operations to determine failure modes, failure causes and underlying failure mechanisms.
    - Ensure the software design includes a failure recovery architecture.
    - Developers should describe or understand Service-Level Agreements for interfaces, services, GOTS software, and provided infrastructure (e.g., DoW provider services).
5. The CONOPS should provide enough information to establish operational tempo and constraints for releases, patches, and failure recovery for software services (functions) and interfaces.
    - These constraints include periods of continuous operations, deployed to a connected or disconnected mode and the composition of the operations team.
    - Describe how operational mission degradation caused by software downing events, may or may not impact operational availability.
6. Unified Platform and Zero-Trust Security
    - The contractor should implement a unified platform that consolidates all LLMs into a single user interface, ensuring streamlined access and management. The platform should support zero-trust security architecture to safeguard sensitive data and comply with DoW Impact Level (IL) 5/IL6 standards.
    - The contractor should ensure that the platform supports real-time explainability and source attribution for all artificial intelligence (AI)-generated outputs, providing transparency and accountability in decision-making processes.

7. Reliability Testing and Failure Reporting
    - The reliability engineer and software designers should focus on software maturity metrics (e.g., defect tracking by integration and test event). It is critical that the software fault rates be analyzed to ensure that the software does not have an increasing fault rate.
    - Software-intensive systems should address reliability growth by providing either a reliability growth planning curve (RGPC) or reliability growth tracking curve (RGTC). If a RGPC is appropriate for the program, then the TEMP should provide a RGPC based on an appropriate methodology. The Crow-Extended and the AMSAA Projection Methodology (PM2) models are two recommended reliability growth planning models. If using a RGTC, programs should follow the guidance for hybrid systems. For software-intensive systems that are primarily software, the RGTC may be more appropriate. The selection of the appropriate curve for inclusion in the TEMP should be reflective of the program. System-level reliability growth for hybrid systems can be planned using an RGPC. The RGPC should be stated in a series of intermediate goals and tracked using a suitable RGTC.
    - For software, the reliability test approach should include appropriate tests (load/stress testing, failure injection testing, out of bound, database re-indexing, data aging, hard drive re-optimization, etc.) to precipitate software failure modes and associated defects.
    - For software, stresses will include operating in Denied, Degraded, Intermittent, and Limited (D-DIL) network environments; timing; loading; and other potential performance bottlenecks or externally induced failure modes.
    - For software, reliability testing should include testing throughout development to identify failure modes and evaluate failure detection and system recovery.
    - Software should be tested to meet not only its reliability and other performance requirements but also the planned operational tempo and potential timing and performance extremes.
    - For critical software components or CSCIs, software tests should include testing to failure based on capacity required, fuzz testing, out of bounds testing and out-of-order execution, include reviewing logs, software error messaging and focus on fault detection, fault isolation, and restore time.
    - For systems developed in the Software Acquisition pathway, the help desk and problem reporting system should be integrated in the FRACAS system.

Table 3-5 summarizes how key software R&M tasks would be integrated into a system SOW. Table 3-6 summarizes these tasks and why they are needed.

Table 3-5. Key Software Reliability Tasks in the SOW

SOW Reliability Tasks	Application to Software
Reliability, Availability, and Maintainability Program Plan (RPP)	Reference the Reliable Software Program Plan (RSPP) that: Addresses R&M/SE Coordination Refers to software size and schedule estimates Includes COTS/Reuse Analysis
SRM	Include software components in the SRM
Reliability Allocations	Include software reliability allocations
Reliability Models & Predictions	Include an assessment (prediction) of software reliability
Reliability Evaluation	Address software Reliability Evaluation (description of stresses, loading, corner cases, fuzz (random, invalid or unexpected data) and out of bounds data used to test the software.) and Growth Planning, including reliability-driven software testing
FMEA	Conduct a software FMEA that references: Fault and failure management; Software FTA
Software Maintainability	Conduct maintainability analysis (see next subsection)
FRACAS	Ensure FRACAS includes software failures/anomalies

Table 3-6. Need for Key Software R&M Tasks

Tasks	Why This Task Is Needed
RSPP	Ensures tasks required for reliable software are integrated with the engineering processes and that the software, reliability and systems engineering personnel are interfacing with each other.
Inclusion of Software in SRM	Ensures software is explicitly integrated into the system model to avoid underestimating the system reliability.
Software Reliability Allocations	Ensures software is not ignored in system reliability allocations and the software team knows that they must test to a specific reliability goal.
Software Reliability Predictions	Ensures contractor predicts software reliability early in development while time remains to determine alternative solutions
Software Maintainability	Ensures software code will be repairable, easy to improve, and understandable.
Reliable Software Evaluation	Ensures contractor is demonstrating that the actual software reliability in testing is trending towards the allocation.
Software FMEA	Identifies failure modes in the software that are very difficult to identify during testing but are costly in terms of mission failures.
Inclusion of Software in FRACAS	Ensures contractor is providing any software failures to the Government for review.
Software Reliability Risk Assessment	Ensures commonly overlooked risks do not derail the software Reliability.
Reliable Software Testing	Provides confidence to the DoW that the software has been exercised in a manner consistent with its operational use.

3.4. Tailoring Software R&M Acquired Using the Software, MCA, and MTA Pathways

3.4.1. Software Acquisition Pathway Tailoring Guide

This section provides the Government reliability engineer the reliable software tasks, rationale, and tailoring guidance applicable to the Software Acquisition pathway (Applications path) and to the Embedded Software path for MCA and MTA programs.[16]

Given the unique requirements for a UCA program, this guide does not address embedded software for UCA programs, nor does it address embedded software relating to the Acquisition of Services or DBS pathways. DBS and UCA systems may include COTS hardware, for which the Applications path would be useful. See DoDIs 5000.02 (AAF), 5000.81 (UCA), 5000.75 (DBS), and 5000.74 (Services) and the R&M BoK for further information and guidance.

3.4.2. Applications Path

The Applications path provides for rapidly developing and deploying software running on commercial hardware, including modified hardware, and cloud computing platforms. Programs executed through the Applications path may not have typical reliability requirements (e.g., MTBF, MTBOMF, MTBCF), in which case reliability (failure-rate-based) allocations and predictions should not be used. Software failures, unlike hardware failures, tend to be use driven and time independent: the engineering focus should be on failure detection and recovery.

The ability to recover without repair is an important capability that differentiates software systems from traditional hardware systems. While hardware systems can have redundancy that allows continuous operation, the redundancy is finite, is depreciated with each failure, and can be restored only through repair. For software systems, processes can be restarted or moved to different virtual machines or cloud instances without limit or requiring a hardware replacement.

Many of the tasks and techniques used to design hardware with adequate R&M characteristics do not apply to software. Software (unless it already exists and is fielded) does not have an inherent reliability. These statements do not imply that reliability is not required for software or IT systems, just that they require a different focus than hardware. Appropriate R&M activities[17] include FMEA, FTA, maintainability analysis, reliability modeling, and FRACAS.

- *FMEA.* FMEA is used rather than FMECA because the criticality analysis of the FMECA requires a failure probability for the failure mode.

[16] A Defense Business System (DBS) often includes a software engineering element that should be addressed to support the system availability requirement.

[17] See IEEE 1633-2016, IEEE Recommended Practice on Software Reliability, for guidance on software reliability engineering processes, prediction models, growth models, tools, and practices of an organization.

- *Software*. Software should be designed with error and exception handling, and with design requirements for time to detect, isolate, and recover based on the operational mission profile.
- *FTA.* A software FTA is conducted to find critical events concerning fault introduction, relate those events to the development process, and develop appropriate actions that will reduce the probabilities of these events and the subsequent probability of the top event.
- *Maintainability Analysis.* Software maintainability can be defined as the degree to which an application is understood, repaired, or enhanced. Designing for software maintainability involves:
  - Iterative development and regular reviews to improve quality.
  - Writing readable code that is easy to understand.
  - Refactoring code for understandability.
  - Developing relevant documentation to help developers understand the software.
  - Using automated build to make code easy to compile.
  - Using automated tests to verify implementing changes does not introduce other faults.
  - Using continuous integration to make the code easier to build and test.
  - Implementing version control to keep code, tests, and documentation current and synchronized.
- *Software Reliability Modeling.* Since the early 1970s, more than 200 software reliability models have been developed. No individual model can be used in all situations. No model is complete or even representative. The two basic categories of models are software reliability prediction and software reliability estimation. To support reliability growth, a software reliability prediction model would be used.
  - Software Prediction Model. Uses historical information, usually before development or test and as early as the concept phase, to predict reliability at some future time.
  - Software Reliability Estimation. Uses development data later in the life cycle (not typically in concept or development phases) to estimate reliability at the present or future time.
- *FRACAS.* MIL-HDBK-2155 describes procedures for conducting a FRACAS for software and hardware programs. The former requires the systematic reporting and analysis of software failures to determine root cause and develop effective corrective actions (involving a change to the software code) to prevent recurrence of the failures. To support reliability growth, the FRACAS should capture cumulative execution time at the time of failure.

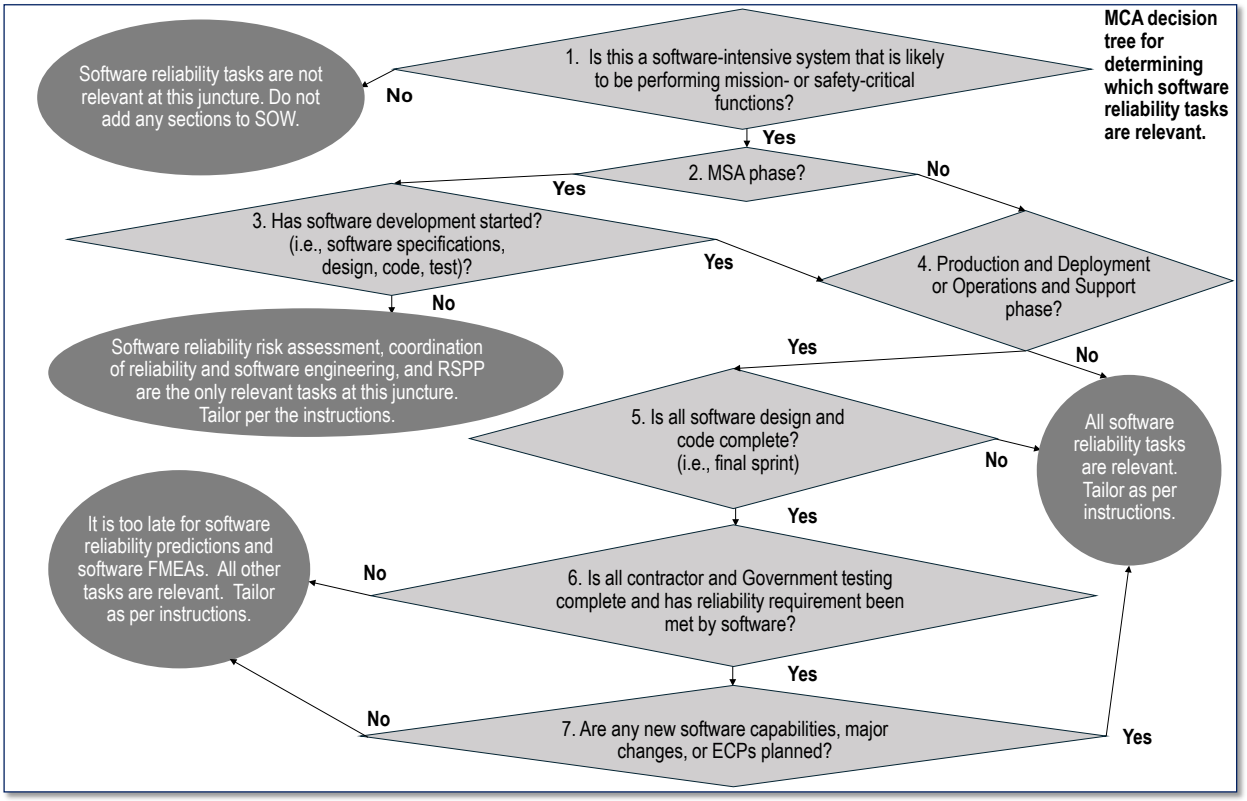
- *Continuous Integration and Deployment* must be included in modern software products.
    - The contractor should adopt modern DevSecOps practices, including automated testing, continuous integration, and real-time monitoring, to ensure agility and delivery velocity. The platform should support continuous authority to operate (cATO) and accelerated accreditation processes.
    - The contractor should demonstrate the ability to deploy new models and updates as soon as possible, ensuring responsiveness to emerging threats and technological advancements.

3.4.3. Embedded Software Path

This Embedded Software path provides for the rapid development, deployment, and insertion of upgrades and improvements to software embedded in weapon systems and other military-unique hardware systems. The system in which the software is embedded could be acquired via other acquisition pathways (e.g., MCA). Existing acquisition programs may elect to update their Acquisition Strategy to transition to the Software Acquisition pathway or use it in addition to their current pathway. Software may be a part of a program following the MCA or MTA pathway.

The first step is to identify which tasks[18] shown in Tables 3-5 and 3-6 are relevant for the program, as shown in Figure 3-3 for MCA and Figure 3-4 for MTA.

[18] From FCDD-AMR-MR-22-08 (2022).



Source: FCDD-AMR-MR-22-08 (2002). ECP: Engineering Change Proposal; FMEA: Failure Modes and Effects Analysis; MCA: Major Capability Acquisition; MSA: Materiel Solution Analysis; RSPP: Reliable Software Program Plan; SOW: Statement of Work.

Figure 3-3. Top-Level Decision Tree for Determining Relevant Reliable Software Tasks for an MCA Program

3.4.3.1 MCA Program

The first decision is assessing whether (1) the program is software intensive and (2) the software is mission critical. For most modern military systems, these will be true. The WarU Glossary defines software intensive as "a system in which software represents the largest segment in one or more of the following criteria: system development cost, system development risk, system functionality, or development time."

For this document, the definition of "software intensive" is broader in that any weapon or combat system with software is in scope. If there is any doubt, the reliability engineer should discuss the program with the software and systems engineering counterpart.

The second decision is determining whether the program is beyond the MSA phase. Typically, there is software development in the MSA phase and the relevant tasks for TMRR or EMD apply to MSA. If a specific reliability objective is not yet established in MSA, reliability software tasks are still relevant. The software FMEA and risk assessment tasks are not tagged to a specific quantitative objective. If the software development has not started in MSA (decision #3), only

the reliable software risk assessment and coordination of reliability and software personnel are relevant.

If software development has started and it is neither the Production and Deployment (P&D) nor Operations and Support (O&S) phase (decision #4), all reliable software tasks are relevant and should be tailored. If the phase is either P&D or O&S and software development activities continue (decision #5), all reliable software tasks again are relevant.

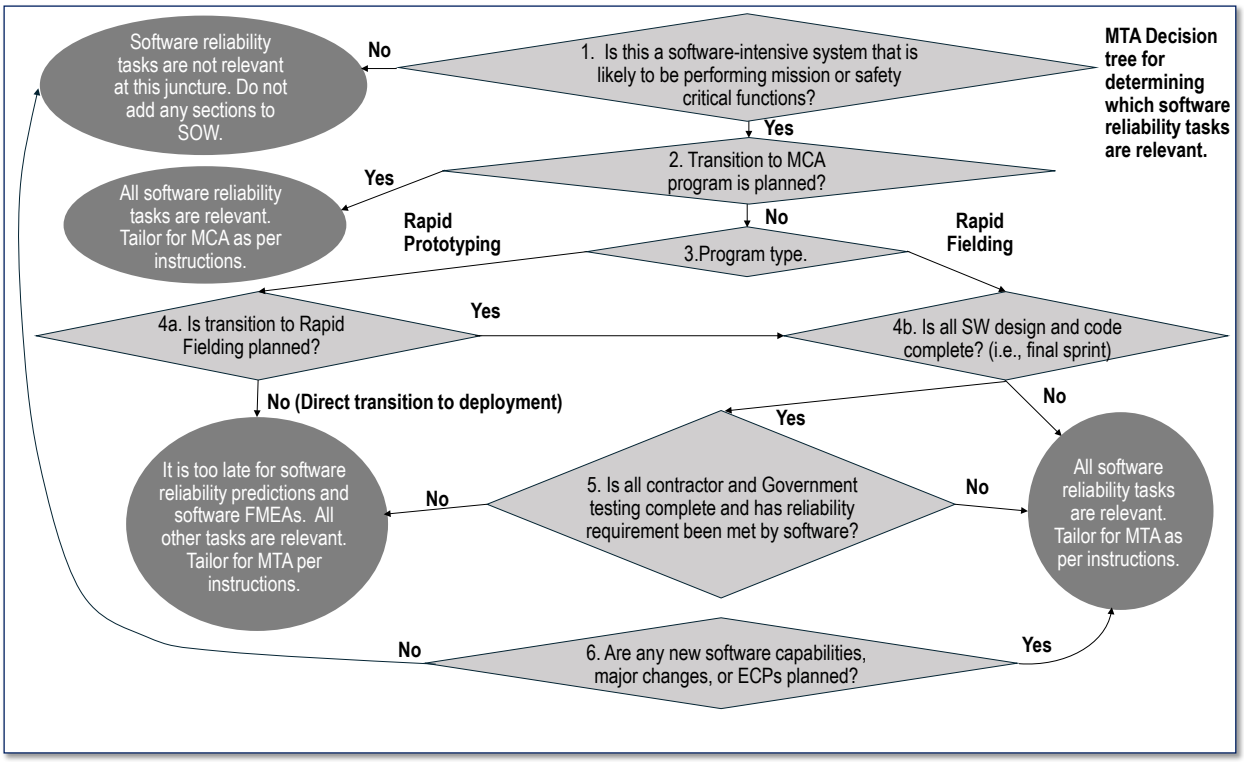
If development is complete but the reliability objective has not been met (decision #6), then it is too late for the software reliability predictions or software FMEA. If the reliability objective has been met by the software and there are no more planned ECPs, major changes or planned new capabilities (decision #7), the software reliability tasks are not relevant. Otherwise, any of the reliability tasks is relevant and should be tailored.

3.4.3.2 MTA Program

The MTA decision path for reliable software starts similarly to the MCA path in that only programs with software performing a mission-critical function for a combat, weapon, or mission system are subject to the reliable software tasks. The second decision point is whether this MTA will transition to an MCA. If so, the MCA decision tree should be used and tailored. The third decision regards whether the MTA program is Rapid Prototyping (RP) or Rapid Fielding (RF).

If the MTA program type is RP and a direct transition to deployment is planned (decision #4), several of the reliable software tasks are not relevant because of the lack of calendar time. Only the reliable software growth evaluation allocations, including software in the FRACAS and testing for reliable software, can be accomplished in that calendar time.

If the RP will transition to RF, tasks should be tailored as if the program is RF. If software development is complete (final sprint), the remaining decisions are like decisions 5-7 in the MCA path. If development is incomplete (decision #5), the reliable software tasks must be tailored to fit into the 5-year schedule required for MTA, or some tasks might be removed if the calendar time available is particularly short.



Source: FCDD-AMR-MR-22-08 (2022). ECP: Engineering Change Proposal; FMEA: Failure Modes and Effects Analysis; MCA: Major Capability Acquisition; MTA: Middle Tier of Acquisition; SOW: Statement of Work; SW: software.

Figure 3-4. Top-Level Decision Tree for Determining Which Reliable Software Tasks Are Relevant for an MTA Program

Table 3-7 summarizes the tailoring scheme for the Level of Rigor (LOR) for the MCA and MTA pathways. For most of the tasks, there are minimalist or detailed approaches available. Depending on the phase of the program, the complexity of the software, and other factors, the LOR can be selected. This table assumes that the program is software intensive and has mission-critical software.

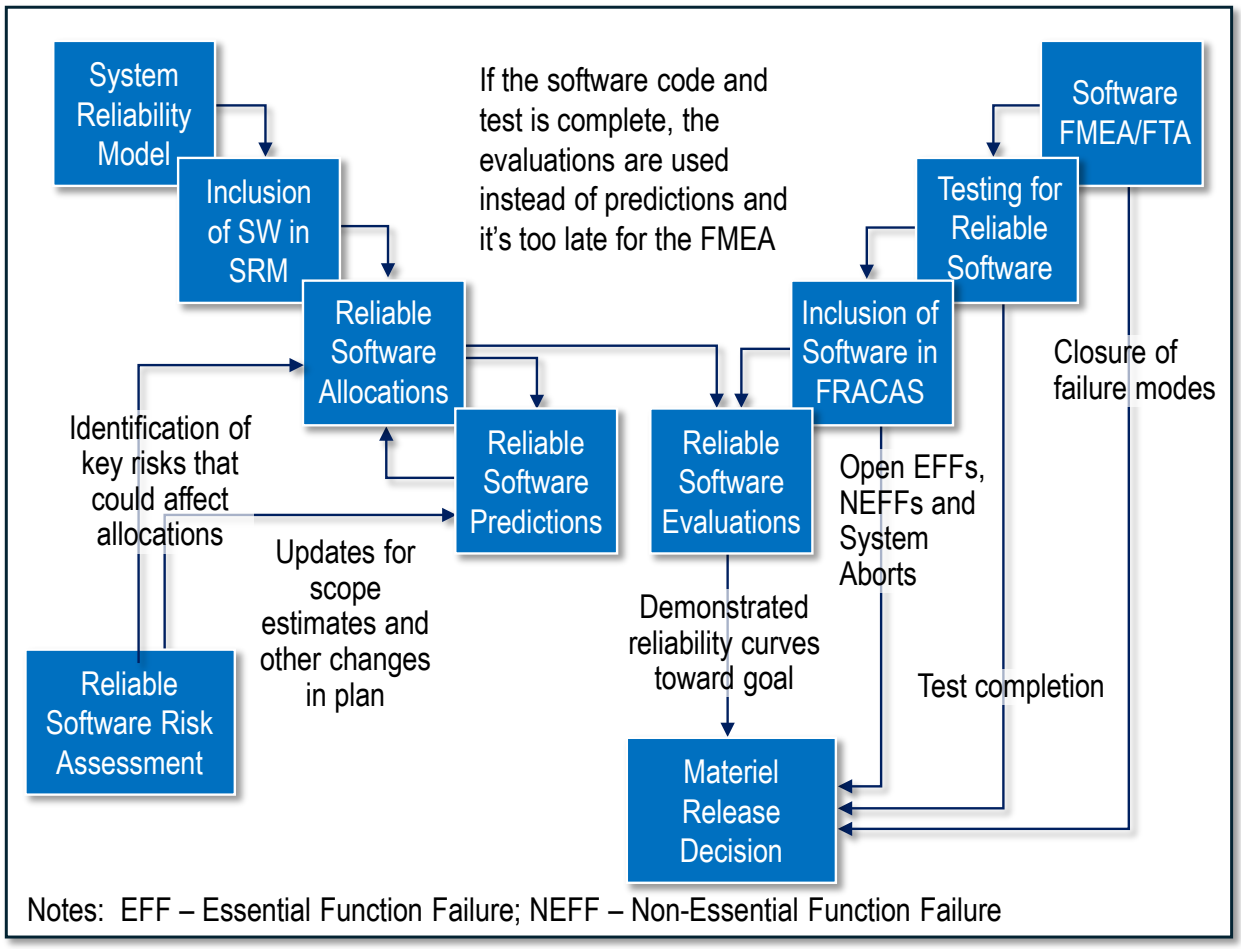
Table 3-7. Tailoring for Level of Rigor for MCA and MTA Acquisition Paths

R&M Task	MCA or MTA with Transition to MCA	MTA RP Path with Direct Transition to Deployment	MTA RP Transition to RF	MTA RF
Reliable Software Program Plan	√	√	√	√
Inclusion of Software (SW) in SRM	Model can be tailored to complexity of SW/hardware (HW)[1]	Can be tailored for simple model[1]	Can be tailored for simple model[1]	Can be tailored for simple model[1]
SW Reliability Allocations	Select model based on data accuracy & availability[1]	Can be tailored for simple model[1]	Can be tailored for simple model[1]	Can be tailored for simple model[1]
SW Reliability Predictions	Select models based on risk[2]	Either remove task or use simplest models[2]	Either remove task or use simplest models[2]	Either remove task or use simplest models[2]
Software Reliability Growth	Select the Crow-Extended or the AMSAA Projection Methodology (PM2)	Either remove task or use simplest model	Either remove task or use simplest model	Either remove task or use simplest modes
Reliable Software Evaluation	Select models depending on risk[3]	Full or minimal metric set depending on risk[3]	Full or minimal metric set depending on risk[3]	Full or minimal metric set depending on risk[3]
SW FMEA	Tailored by risk.[4]	Tailored by risk.[4]	Tailored by risk.[4]	Tailored by risk.[4]
Software Maintainability Analyses	√	√	√	√
Inclusion of Software in FRACAS	√	√	√	√
SW Reliability Risk Assessment	√	√	√	√
Reliable SW Testing	Tailored to apply to the most mission-critical software LRUs			
Software Maintainability	√	√	√	√

Notes for Table 3-7:
√ Applicable anytime there is mission-critical software-intensive system.
1. Software/Hardware. Relevant if either the software reliability predictions or software reliability growth evaluation is relevant.
2. Not useful if the coding activities are complete.
3. Unless the reliability objective has been demonstrated this task is relevant.
4. Most useful before code is complete, not useful if all testing is complete.
   - **Testing for reliable software for mission-critical software LRUs**. If nothing else, the best way to achieve reliable software is to test the trajectories, boundaries, faults, data, zero values, etc. This task alone provides the most confidence in the reliability of the mission-critical software.
   - **Reliable software evaluation**. If the software is highly unstable, this evaluation will make that clear. It can and will identify the additional test effort needed to make the software stable, but it does not guarantee that the contractor has or will test the inputs that are most likely to result in a software failure. This task should always be in addition to the testing for reliable software and not in lieu of it.
   - **Top level software FMEA**. This task can identify top level failure modes that should be considered in testing. However, without the testing for reliable software task, the tests might not get executed.

For MTA programs not transitioning to MCA, all the reliable software tasks should be tailored for minimal metrics or minimalistic models. However, further tailoring may be needed due to the limited calendar time available for the tasks. The tasks with a √ are neither costly nor time consuming. As for the other tasks, they are listed in rank order of importance to MTA programs.

For MCA programs with limited time or funding, the tailoring scheme just described can also be applied. Figure 3-5 illustrates the process for how reliable software tasks interface with each other.



EFF: Essential Function Failure; NEFF: Non-Essential Function Failure.

Figure 3-5. How Reliable Software Tasks Interface with Each Other

3.4.4. Tailoring the SOW for the Embedded Path

Table 3-8 provides guidance in tailoring the Reliable Software Program (RSP) SOW when the intent is to transition the software to an MCA or MTA program. Guidance in selecting relevant software reliability tasks is provided in decision trees (Figures 3-3 and 3-4).

Table 3-8. Tailoring Guide (Program Phase and Equipment Type)

Basic SPW Statement for RSP Plan	Tailoring Instructions
PROGRAM PLAN. The contractor shall provide the Government an overview of their system reliability program (SRP) that includes scope to develop reliable hardware and software, as a briefing at the Post-Award Orientation. The reliable software program (RSP) shall address: <remove items per column 2> (1) Inclusion of software in the reliability model (2) Reliability allocations for software (3) How the contractor will predict and demonstrate reliability growth of the software in a diverse operational environment (4) How software failure modes will be identified and mitigated early in development (5) Software failure mode/defect tracking (6) Software risk management (7) How software will be developed and tested for reliability (8) Coordination of the reliability, test, design, systems, software, embedded software functional areas (9) How software reliability tasks are integrated into the software development schedule to ensure reliability is designed in early (10) A site reliability engineer. The contractor shall identify all mission-critical software LRUs and functions. The contractor shall describe the planning and implementation of reliable software activities as well as coordination with reliability, test, design, systems, software, and embedded software. The contractor shall integrate the reliable software effort with the overall SRP. The contractor shall participate and be prepared to share any reliable software task updates during the government working group meetings per the program integrated master schedule R&M Working Group. The contractor shall reference the RSPP in the software development plan. The contractor shall deliver the Reliable Software Program Plan (RSPP) as part the R&M Program Plan (RPP) per DI-SESS-81613."	1. Determine which software reliability tasks are relevant for the program as per decision trees (Figures 3-2 and 3-3). 2. Modify the SOW language: 3. Remove bolded sections from the reliable software SOW associated with software reliability tasks irrelevant for the program. 4. Remove this text < remove items per column 2> 5. Write the RSPP SOW language to have only the chosen software reliability tasks 6. Revise SOW language to ensure SDP is referenced in the RSPP. 7. If either of the following conditions is not true, remove (11). A site reliability engineer may be required in the SOW language for the RSPP. Unless the weapon/system is a providing network capability, the site reliability engineer is likely to be out of scope for the program. • Software downtime requires immediate action by on-site engineer. • The site reliability engineer is funded by the program. 8. The RSPP section of the Reliability, Availability, and Maintainability Program Plan must be explicitly referred from the SDP to ensure the software engineering is aware of the reliability requirements and is working to meet the requirements. The Data Item Description (DID) for the SDP is DI-IPSC-81427 Rev. B. This may require SOW language for the SDP. 9. Merge the RSPP language with the reliability program plan language for the hardware. 10. Ensure the RAM office symbol is in block 14 of the SDP CDRL. 11. Tailoring for Agile/DevSecOps. The SOW language for the RSPP is unaffected by development framework. Frequency of updates are reflected in each task CDRL/1423 block 10.

Table 3-8. Tailoring Guide (Program Phase and Equipment Type) *(continued)*

Basic SPW Statement for RSP Plan	Tailoring instructions
SOFTWARE FMEA. The contractor shall define mission-critical software and link to the SRS requirements or user stories. Each mission-critical SRS/user story shall be verified during First Qualification Test. The contractor shall identify, confirm, and mitigate software failure modes (FMs) affecting mission-critical functions. The contractor shall demonstrate understanding of software controls independent of human interaction and that link to mitigating mission-critical functions. The contractor shall analyze **<top level FMs per the Joint Software Systems Safety Engineering Handbook>**, mission-critical design, use cases, user stories, software specifications and features <that are traced to any changes in mission time, payload, hardware, or interface> from the software functional FMEA viewpoint employing the software centric failure modes IAW IEEE 1633 2016 Clauses 5.2.2 and Annex A. Also, the contractor shall consider the sources of software faults discussed in the Joint Software Systems Safety Engineering Handbook that apply to both software safety and mission-critical software. **<Identify specific modes here>** mission modes shall be considered in the analysis. **<The contractor shall employ fault trees and defect root cause analysis in preparation for the Software FMEA as per IEEE 1633 2016 clauses 5.2.1 and 5.2.3.>** The SwFMEA shall be conducted prior to the completion of the software code with or by a cross functional team of among software engineers, systems engineers, and reliability engineers. At least one team member must understand software development. If agile/CI/CD framework is employed, the SwFMEA is conducted incrementally prior to code development per the IEEE 1633 2016 Table 10, as guidance, and continuing throughout the lifecycle for the increment. Interim results of the SwFMEA shall provide inputs for the software test plan and FRACAS. The contractor shall illustrate tracing of FMs to specific test cases. Final SwFMEA shall be delivered in contractor format, electronically searchable and filterable, in the overall FMECA	1. Identify the appropriate approach(es) from the decision trees and section 1.6 of the SOW guidance document. 2. Include or excluded the bolded text based on that guidance 3. Merge the language for the software FMEA with the hardware language in the SOW section C. 4. Identify appropriate approach(es) from decision trees and section 1.6 of the SOW guidance document. **Tailoring for DevSecOps.** SwFMEAs unaffected by development framework. Frequency of deliverables are reflected in DI-SESS-81495B Failure Mode, Effects, and Criticality Analysis Report CDRL/1423 block 10. https://www.cto.mil/wp-content/uploads/2023/08/Joint-SW-SSE-2010.pdf

Table 3-8. Tailoring Guide (Program Phase and Equipment Type) *(continued)*

Basic SPW Statement for RSP Plan	Tailoring instructions
report as per DI-SESS-81495B except for column M, P, R, S, T, and U, which do not apply to software failure modes. The contractor shall derive software requirements for identification and recovery for <*severity defined by the writer depending on application type as per the guidance*> identified in the SwFMEA and shall ensure derived software requirements are tested. The contractor shall define fault tolerance for mission-critical software and link to SRS requirement/user story and verify fault tolerance, controls, and mitigations via fault injection testing. The contractor shall avoid "one size fits all" fault handling by determining the most appropriate means on an individual fault-by-fault basis	
FRACAS. The Contractor shall tag all software failure reports found from Development Test onwards (i.e., reliability growth), and FMs identified via the SwFMEA or fault trees as failures that can be filtered. The failure reports shall conform to DI-SESS-80255B in contractor format, electronically searchable and filterable format, and made available upon request. Failures shall be captured in an automated system. The contractor should show evidence (via regression testing) that corrective actions did not cause any adverse effect on the software. The contractor shall prioritize fixing of the root cause of the software failure.	1. Always relevant for any software intensive system with mission-critical software 2. Merge this language into the language for the hardware FRACAS in the SOW. **Tailoring for DevSecOps.** Task unaffected by development framework. Frequency of deliverables is reflected in the Failure Reporting Corrective Action CDRL/1423 block 10.
SOFTWARE RELIABILITY RISK ASSESSMENT. All risks identified in clause 5.1.3 and Figure 16 of the IEEE 1633 2016 <*include any other risks here not captured in clause 5.1.3*> shall be identified, managed, and mitigated. The contractor shall manage these risks and make plans for mitigating these risks available to the Government. The identified risks and plans for mitigating shall be delivered, in the software portion of the Reliability Program Plan IAW DI-SESS-81613.	1. Always relevant for any software intensive system with mission-critical software 2. Modify block 10 of RPP CDRL/1423 with same initial delivery and update frequency as the SDP. 3. Merge this language into the RPP language for the hardware. 4. Tailoring for DevSecOps. Task unaffected by development framework. Frequency of deliverables is reflected in the RPP, CDRL/1423 block 10.

Table 3-8. Tailoring Guide (Program Phase and Equipment Type) *(continued)*

Basic SPW Statement for RSP Plan	Tailoring instructions
TESTING FOR RELIABLE SOFTWARE. The contractor shall conduct <Either day "all" or list the specific tests> tests on mission-critical software tagged to <list specific mission hazards here. If the software LRUs are established, then list those tagged to the system-level hazards.> to ensure reliable software as listed the Joint Software Systems Safety Engineering Handbook (applicable for mission-critical software as well as safety significant software functionality). The reliability driven test plans shall be identified early to ensure Test-Driven Development (TDD). The contractor shall derive software requirements for endurance, peak loading, boundaries, and fault injection. The contractor shall automate testing and use static code analyzers. Tests shall be conducted against the assessed mission-critical functions. Contractors shall conduct engineering evaluation tests for all applicable mission characteristics using a test-like-you-operate (TLYO) approach to demonstrate product meets mission requirements for applicable mission phase and timeline. The TLYO approach shall ensure the test article is evaluated, as is practical, in a configuration matching the expected operational configuration and environment. The contractor shall update and maintain a Software Test Plan (STP) IAW DI-IPSC-81438, for each software external release which defines the plan, for new or modified software, to fully exercise the software as discussed above. The contractor shall develop Software Test Descriptions (STD) IAW DI-IPSC-81439 for each software external release IAW the approved STP. The contractor shall perform all software test activities IAW the SRM and the approved STP and develop and deliver Software Test Reports (STR) IAW DI-IPSC-81440 for each external software release."	1. This task is always relevant for any software intensive system with mission-critical software 2. Merge this language into the STP, STD, STR SOW language. 3. Ensure that RAM office symbol is in block 14 of STP, STD and STR CDRL/1423 4. Tailoring for DevSecOps. This task unaffected by development framework. Frequency of deliverables is reflected in the STP, STD and STR CDRL/1423 block 10.

Table 3-8. Tailoring Guide (Program Phase and Equipment Type) *(continued)*

Basic SPW Statement for RSP Plan	Tailoring instructions
MAINTAINABILITY ANALYSIS. The contractor shall conduct analysis to ensure the software is understood, repairable, or can be enhanced. The reliable software program shall address: (1) Inclusion of software in the R&M model (2) Maintainability allocations for software (3) How the maintainability characteristics of the software will be predicted and demonstrated (4) How software will be developed to be maintainable	This task is always relevant for any software intensive system with mission-critical software. Modify the SOW RSPP language: • To have only the chosen software maintainability tasks • The RSPP section of the RPP must be explicitly referred from the SDP to ensure the software engineering is aware of the maintainability requirements and is working to meet the requirements. The Data Item Description (DID) for the SDP is DI-IPSC-81427 Rev. B. This may require SOW language for the SDP.

3.4.5. Software Figures of Merit

If the result from Figures 3-3 or 3-4 and/or Table 3-7 determines that a reliable software model task is relevant, the government reliability engineer needs to identify the Figures of Merit (FOMs) [19] in the SOW language. For example, if availability and Mean Time Between Essential Function Failures (MTBEFF) are required to be measured then place the metrics into the SOW as appropriate. Examples of software FOM are:

- "Reliability" – the probability of success over some specific mission time. This measure is applicable for any software involved with a "mission." This would include missiles, aircraft, landing gear, vehicles, etc.; however, if the mission is an extended duration, "availability" typically makes more sense. Example: Refrigerators are always on. Dishwashers are on only for discrete time periods (missions) per day.
- "Maintainability" – the ease with which a software system or component can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment.
- "Availability" – a FOM that is appropriate for systems that are on for an extended duration, such as security systems, networks, radar, or any system that does continuous monitoring. Availability measures the downtime for preventive and restorative actions. To estimate software availability, the restore time must be predicted. Availability can be measured in different ways, including dividing uptime by total time.

[19] Definitions are taken from the ANSI/IEEE Standard Glossary of Software Engineering Terminology and from FCDD-AMR-MR-22-08, Reliable Software Statement of Work Language Guidance (2022).

- "Mean Time to Software Restore (MTTSR)" – the metric to measure software downtime. This includes time to: (1) restart, (2) reboot, (3) workaround, (4) reinstall software, (5) downgrade software, and/or (6) wait for a software upgrade. These are listed in relative order of time required. Not all software failures can be addressed with a restart or reboot. Some may need to be avoided with a workaround. In a few rare cases, some issues are resolved by reinstalling the software. In cases in which a new version of software has defects not seen in prior releases, the software might have to be downgraded. In some cases, in which a software failure cannot be avoided or worked around and effects the mission the software might not be used until the software engineering team fixes the problems and deploys an upgrade. Mean Time to Repair (MTTR) does not apply to software because software does not wear out in the same manner as hardware.
- "Mean Time Between System Abort (MTBSA), MTBEFF, etc., and Failure Rate" – FOMs that can be measured for any software system.
- "Total Predicted Software Defects" – a valid metric for contractor Development Tests and/or field operation. While the predicted software defects cannot be necessarily merged with hardware predictions, the software defect prediction can be a useful indicator for validating the other predictions. If the contractor's predictions for defects are unreasonable (i.e., very close to 0 for example) then the contractor prediction for failure rate and availability will also be unreasonable.

3.5. Contract Section C – Sample Statement of Work Language

The R&M engineer should tailor the SOW language in Table 3-9 based on the Tailoring Guide shown in Table 3-8. The items in bold at the end of the paragraphs are CDRL (DD Form 1423) deliverables. The paragraph numbering is shown for illustration only. The associated sample CDRLs are shown in "EXHIBIT A" after Section 3.6, "Contract Section J – List of Attachments," of this document.

Table 3-9. Sample Statement of Work Language

3.19 (U) Reliability, Maintainability (R&M) Program requirements.
3.19.1 (U) General. The contractor shall have an active R&M engineering program during the Execution phase. This program shall be directed towards ensuring R&M is factored into the software design solution decisions to ensure the system R&M characteristics meet the specification requirements. The contractor shall prepare and follow an R&M program plan that identifies and describes the planned contractor activities for implementation of the R&M program. (**CDRL, Reliability & Maintainability Program Plan**).
3.19.1.1 (U) R&M. The contractor shall designate an individual responsible for the planning, implementation, and evaluation of R&M program activities. This individual shall be delegated sufficient authority to effectively implement the R&M program and shall serve as the principal contact for the Government.
3.19.1.2 (U) Subcontractor R&M. The contractor shall be responsible for ensuring that the software R&M levels achieved by the subcontractors and suppliers are consistent with the performance requirements of the **(Program Name)** performance specification(s). The contractor shall be responsible for flowing R&M quantitative requirements, analyses and test activities down to subcontractors and suppliers.
3.19.1.3 (U) Trade Studies. The contractor shall ensure that software R&M aspects are addressed in trade studies and must consider total life cycle costs including user operations and maintenance. The results of trade studies in R&M shall be presented to the Government and discussed at appropriate program and design reviews.
3.19.1.4 (U) Market Survey. The contractor shall explore COTS/NDI alternatives to determine what software R&M attributes exist and what resources would be required to meet the **(Program Name)** performance specification requirements before a decision is made to proceed with the use of COTS/GOTS/GFS/FOSS. The contractor shall conduct a market survey and a Product Support Analysis (performed by the product support team) to ensure that the COTS/GOTS/GFS/FOSS is reliable, maintainable, and supportable prior to its procurement and fielding. The contractor shall also consider the adequacy of technical data that would have to be used for maintenance by user personnel during operational use. [In some cases, this data may also include details of the R&M engineering activities associated with the design of the software, e.g., FMEA, Failure Reporting, Analysis, and Corrective Action System (FRACAS), to assess where adequate usage data are not available to support a contractor's claim of inherent R&M for the COTS/NDI software.
3.19.2 R&M Design Analyses
3.19.2.1 (U) Mission Profile Definition. The contractor shall analyze the mission profile (OMS/MP) provided by the Government to ensure it represents a description of system use duty cycles throughout the mission period for which software reliability is to be specified and that it identifies a time sequence description of operational events required, in the mission period, to accomplish the objective(s), and shall be documented in the Mission Profile Definition Report. This profile shall include identification of the total envelope of environments that will exist in the mission sequence and the functions to be performed in the mission sequence. **(CDRL, Mission Profile Definition Report)**

Table 3-9. Sample Statement of Work Language *(continued)*

3.19.2.2 (U) Reliable Software Program Plan (RSPP). The contractor shall establish, maintain, and operate a reliable software program acceptable to the Government. The contractor shall provide the RSPP within the overall Reliability and Maintainability Program Plan (RMPP). The contractor shall provide the Government an overview of their software reliability program as a briefing at the Post-Award Orientation. The contractor shall develop and operate a closed-loop reliable software program. The reliable software program shall achieve the following objectives: 1) ensure system reliability includes the contribution of the software; (2) design for reliable software; and (3) monitor, assess and demonstrate reliability of the software. The contractor shall describe the planning and implementation of reliable software activities as well as coordination with reliability, test, design, systems, hardware, software, firmware, and FPGA engineering. The contractor shall provide software system assessment, software failure /defect review in support of the government Reliability Working Group after each software build and system/subsystem test. The contractor's RSPP shall address software specific management and technical tasks and methods including software size and schedule estimates, COTS/reuse analysis, prediction and allocations, software FMEA, reliability growth, and demonstrating that software products meet their allocated requirements. **CDRL: Reliability & Maintainability Program Plan**
3.19.2.3 The Software Development Plan (SDP). The contractor shall establish, maintain, and execute a Software Development Plan (SDP) to provide the Government with insight into and a tool for monitoring the processes to be followed for software development, the methods to be used, the approach to be followed for each activity, and project schedules, organization, and resources. **CDRL: Software Development Plan (SDP)**
3.19.2.4 Reliability, Maintainability Block Diagrams, Math Models, Allocations and Predictions. The contractor shall incorporate software, firmware, FPGA code, COTS, FOSS, GOTS, GFS, and any other software components into the overall system reliability model (SRM). The SRM shall consist of the list of executables IAW IEEE 1633 and their relationships to each other. The software components identified in the SRM shall be traceable and consistent with the software components identified in the software design. Critical items are those whose failure significantly impacts mission success or safety. An item is considered critical if its inoperability prevents mission completion or affects essential functions as defined by Failure Definition and Scoring Criteria, Preliminary Hazard Analysis, or Functional Hazard Analysis. Items are also classified as critical if they perform safety-significant functions, which include both safety-critical and safety-related functions. Safety-critical functions are those whose failure or incorrect operation directly causes catastrophic or critical severity mishaps. Safety-related functions are those whose failure or incorrect operation directly causes marginal or negligible severity mishaps. Additionally, items are considered critical if their failure rates significantly contribute to overall system degradation. This classification helps prioritize items that require enhanced design attention, testing, or monitoring to ensure mission success and safety. The contractor shall assess the software R&M of each software, firmware, FPGA code, FOSS, COTS, GFS, GOTS, and any other software configuration item. The contractor shall deliver the software reliability assessment integrated in the R&M Prediction Report.

Table 3-9. Sample Statement of Work Language *(continued)*

The contractor shall identify the method and justification for each allocation in order of preference: 1) Reliability analysis from comparable deployed software items; 2) Historical reliability from software components with similar software size and complexity, software maturity, hardware maturity, degree of reuse and COTS, development capabilities and application type; and 3) Software reliability prediction and estimation models from industry accepted models such as IEEE 1633 Recommended Practices for Software Reliability. The software reliability assessment shall be updated whenever there are updates to 1) software size, 2) development methods, 3) software schedule changes, 4) software staffing changes or 5) changes in software test effort or schedule.

The contractor shall include size estimates for software, firmware, FGPA code, GFS, FOSS in the estimations as per IEEE 1633 Clause Annex B.1. The contractor's estimations shall be used as inputs to the planning process. The size estimate shall be recorded in the contractor's Software Development Plan IAW DI-IPSC-81427.

The Contractor shall allocate and update the system R&M requirements to each of the software, firmware, FPGA code, COTS, GOTS, GFS, FOSS, and any other software components IAW the SRM and IEEE 1633. The results of the software R&M allocation shall be incorporated into the system R&M model per DI-SESS-81968. The contractor's Software Requirements Specification (SRS) or user story shall include a statement of the numerical reliability goals (consistent with the system Figure of Merit (FOM) for hardware and system) for each identified software LRU. For Agile/ Continuous Improvement (CI)/Continuous Development (CD) framework IEEE 1633 2016 clause 4.4 and Table 16 provide guidance. The contractor shall keep the allocations up to date and be prepared to share any updates during working group meetings. The contractor shall deliver the allocated reliability of the software of each software LRU as part of the Reliability and Maintainability (R&M) Report IAW DI-SESS-81968. Newly developed, modified, reused, auto-generated code shall be included in the allocations. R&M requirements using appropriate FOMs shall be allocated to each indenture level for contractor and their suppliers. The contractor shall identify the method used for each allocation in order of preference: 1) R&M analysis from comparable deployed software items; 2) Historical reliability from software components with similar software size and complexity, software maturity, hardware maturity, degree of reuse and COTS, development capabilities and application type; 3) Software reliability allocation from industry accepted models; or project cost; and 4) Subject matter expert (SME) engineering estimates.

The contractor shall allocate system R&M requirements to Computer Software Configuration Item (CSCI) or to a Line Replaceable Unit (LRU) when the CSCI is composed of more than one LRU. The contractor's Software Requirements Specification (SRS) shall include a statement of the numerical reliability goals for each identified software configuration item.

CDRL, Reliability & Maintainability Block Diagrams and Mathematical Models Report, Reliability & Maintainability Allocation Report, Reliability & Maintainability Prediction Report)

Table 3-9. Sample Statement of Work Language *(continued)*

3.19.2.5 (U) Software Failure Modes, and Effect Analysis (SwFMEA). The contractor shall identify, confirm, and mitigate the software failure modes affecting mission-critical functions. The contractor shall analyze the software specifications and features from the software FMEA viewpoint employing the software centric failure modes IAW IEEE 1633 Clauses 5.2.2 and Annex A. The contractor shall address sources of software faults in the Joint Software Systems Safety Engineering Handbook. All mission modes shall be considered in the analysis. The contractor shall employ fault trees and defect root cause analysis in preparation for the software FMEA as per IEEE 1633 clauses 5.2.1 and 5.2.3. The SwFMEA shall be conducted by personnel having experience with software development or shall be a cross functional effort between software engineering, systems engineering and reliability engineering prior to the development completion of the software code. If incremental or agile models are employed, the SwFMEA is conducted incrementally prior to the development of the code for the increment. The SwFMEA shall be~~,~~ as part of the FMECA report. The contractor shall derive software requirements for identification and recovery for each specific fault identified in the SwFMEA. The software fault and failure management requirements shall be incorporated into the software requirements, software design, software test and verification plans IAW DI-IPSC-81433, DI-IPSC-81435, DI-IPSC-81438, and DI-IPSC-81439. All the above apply to software, firmware, FGPAs, COTS, GOTS, GFS, FOSS, and any other software. **(CDRL, Failure Modes, Effects and Criticality Analysis Report)**
3.19.2.6 (U) Fault Tree Analysis (FTA). The contractor shall use FTA as a defect-prevention tool. It shall be performed before baselining the design to provide valuable information on application failures and their mechanisms. This information shall be used to improve the design by preventing potential defects or by introducing fault-tolerance. FTA should be applied to more complex functions and not to simple functions of a software application. The Government will be provided results in a report. **DID, System Safety Hazard Analysis Report**
3.19.2.7 (U) Documentation/Data Items. The contractor shall prepare, submit, and maintain R&M documentation/data items (e.g., plans, procedures, reports, and data) in accordance with the related CDRL and the RMPP. The absence from the CDRL of documentation required by this document does not alleviate the contractor of the responsibility to prepare and maintain the documents on file and made available for Government review. An electronic file is the preferred submission method, which is compatible with **[Enter R&M software program name]** software for required analyses.
3.19.2.8 (U) Multi-Modal Capabilities. The contractor should provide multi-modal capabilities, including text generation and analysis, image generation and analysis, audio transcription, video analysis with threat/intel reporting, and speech-to-text/text-to-speech functionalities. These capabilities should be integrated into the unified platform and accessible through a single interface.

Table 3-9. Sample Statement of Work Language *(continued)*

3.19.3 (U) R&M Tests
3.19.3.1 (U) Testing for Reliable Software. The contractor shall conduct all tests to ensure reliable software as listed in the Joint Software Systems Safety Engineering Handbook. These tests shall be conducted against all mission and safety critical software functionality. Contractors developing flight and space systems shall conduct engineering evaluation tests for all applicable mission characteristics using a test-like-you-fly (TLYF) approach to demonstrate product meets mission requirements for applicable mission phase and timeline. The TLYF approach shall ensure the test article is evaluated, to the fullest practical extent, in a configuration matching the expected operational configuration and environment. The contractor shall update and maintain a STP for each software build which defines the plan, for new or modified software, to fully exercise the software as discussed above. The contractor shall develop STDs for each software build IAW the approved STP. The contractor shall perform all software test activities IAW the SRM and approved STP and develop and deliver Software Test Reports for each software build. **CDRLs: Software Test Plan (STP) Software Test Description (STD), Software Test Report (STR)**
3.19.3.2 (U) Reliability Demonstration Growth Test. The contractor shall describe Reliability Demonstration Growth Testing (RDGT) as part of the R&M Program Plan using MIL-HDBK 189C as a guide. The contractor shall perform software Reliability Growth Modeling IAW IEEE 1633 clauses 5.4.4, 5.4.5, 6.2 and Annex C and shall identify: 1) how software reliability growth shall be integrated into the system reliability growth program; 2) planned capability drops and effect on reliability growth; 3) Estimated test hours and test assets to achieve the specified/allocated reliability and 4) Methodology and rationale for selected software reliability growth models. The contractor shall include software, firmware, FGPA code, COTS, GOTS, GFS, FOSS and any other software deployed with the system in the reliability growth models and evaluations. The contractor shall: 1) evaluate the software reliability growth by exercising the software in the system environment to demonstrate achievement of the software reliability requirements; 2) address and mitigate defects and failure modes prior to the next software release, consistent with the correlation to the Failure Definition and Scoring Criteria (FDSC), performance, priority level and total lifecycle cost until software meets the allocated software reliability; and 3) ensure that reliability does not degrade with each software upgrade. **CDRL: Reliability Development Growth Test (RDGT) Report**
3.19.3.3 (U) Subsystem/Equipment Level BIT Assessment Tests. BIT assessment tests shall be conducted on **[type of category of equipment]**. The BIT assessment tests are structured to identify problems, both hardware and software, and shall verify compliance with the individual equipment specification(s) BIT requirements. The contractor is expected to provide procedures including fault determination, fault selection, test conduct, data recording and analysis. The Government reserves the right to witness the BIT assessment tests. **(CDRLs, Reliability and Maintainability Test Plan, Maintainability and BIT Demonstration Test Procedure, and Maintainability, and BIT Demonstration Test Report)**

Table 3-9. Sample Statement of Work Language *(continued)*

3.19.3.4 (U) System-Level Reliability, Maintainability and BIT Demonstration. The contractor shall incorporate into system test articles corrective actions identified from the subsystem/equipment level growth tests, subsystem/equipment BIT assessment tests, environmental qualification tests and relevant system-level integration tests. This configuration shall be tested in accordance with a procedure approved by the Government to verify the overall R&M of the system meets the **(Program Name)** specification requirements. The contractor shall perform reliability evaluations on data from analysis, modeling & simulation, test, and the field. The contractor shall track the evaluations as a function of time and compare them against reliability allocations, reliability requirements, and values to be achieved at various points during development to verify the implementation of corrective actions. When applicable, the Contractor shall use formal reliability growth methodology to plan, track, and project reliability improvement. The ground rules for this evaluation shall be in accordance with **[Add reference to Service/Agency scoring criteria]** to this document and the Government-approved contractor-prepared test procedures. **(CDRL, Maintainability and BIT Demonstration Test Procedure, Maintainability and BIT Demonstration Test Report, Test Procedure, and Reliability Test Report)**
3.19.3.3 (U) Software FRACAS**.** The Contractor shall establish and utilize a closed-loop FRACAS as its mechanism for monitoring and communicating (throughout the organization) the failures from software, firmware, FPGA code, COTS, FOSS, GFS, and other software components. Failures found in test and field shall be captured and identified in the FRACAS. **CDRL, Failure Summary and Analysis Report (FACAR)**
3.19.3.3.1 (U) Failure Reporting. Failures, anomalies or non-conformances experienced on software configuration item articles during laboratory, qualification, R&M tests and demonstrations, walk-throughs, inspections, acceptance tests and system tests shall be recorded in the FRACAS by the contractor. The FRACAS database shall be maintained with failure and anomalies analyses, and corrective actions to reduce or prevent repetition of failures and anomalies.
3.19.3.3.2 (U) Failure Analyses. The contractor shall analyze all software failures and anomalies to the level required to determine the root cause of the failure/anomaly, and to develop corrective actions to eliminate or limit their recurrence.
3.19.3.3.3 Corrective Actions. The contractor, in conjunction with the failure analysis effort, shall develop and implement effective corrective actions to eliminate or minimize recurrence of software failures and anomalies.
3.19.4 Software COTS/Reuse Analysis. The contractor shall evaluate reused COTS/GFE software products to determine suitability with regards to reliability. Reused software includes previously developed software used for project development as is or with adaptation. The contractor shall identify: 1) Identification of any changes in mission or hardware and effect on existing software; 2) Identification of any differences in language, software, or hardware interfaces; 3) Evidence of the product's suitability, including an assessment of the relationship between the software's original intended environment and the proposed environment; and 4) Justification for developing new code as opposed to using COTS or reused code. The COTS/reuse analysis shall be delivered in the software portion of the Reliability & Maintainability Program Plan. **CDRL: Reliability & Maintainability Program Plan**

Table 3-9. Sample Statement of Work Language *(continued)*

3.19.5 Value Assessments. The contractor shall include Value Engineering principles during the initial and annual Value Assessments by addressing the following questions. This will enable a thorough evaluation of mission improvements, efficiencies, and the overall return on investment for the delivered software capabilities: 1) Was an alternative architecture considered that can perform the same function more effectively or at less cost with equal effectiveness; 2) Is there a more effective hardware/software mix; 3) Was a commercial product or a custom product or modifications to existing products considered to provide better value; 4) Were any unnecessary test procedures, operations, or steps considered for removal; 5) Was there consideration of alternatives (products, requirements, procedures, or methods); 6) Is there a more efficient way to accomplish a function or process; 7) What efficiencies were considered for developing and fielding new capability; and 8) Were there opportunities to add value associated with hardware development of procurement.

3.6. Contract Section J – List of Attachments

3.6.1. Contract Attachments

Section J of the RFP lists all attachments, including all data requirements. The contractor will develop valuable data sets in conducting work and completing required activities. R&M engineering data are defined as data resulting from the performance of R&M activities in direct support of an equipment or system acquisition program. Each imposed R&M activity will have some associated technical data, and each contract normally requires contractors to retain all such data in their files and make them available for Government review upon request. The Government identifies in a Contract Data Requirements List (CDRL), listed in Section J of the RFP as an attachment (usually called an Exhibit), only those items of data to be delivered to the Government as required by the SOW.

The ordering and delivery of data is legally defined and scheduled through the combined use of the CDRL (DD Form 1423) and the appropriate list(s) of DIDs and/or NDDs. Since these documents only describe the data to be submitted by the contractor, neither the CDRL nor the DID, nor the NDD, may impose a requirement for the performance of work tasks. Each CDRL entry, however, must reference the paragraph number, document title, and associated task of the SOW. When completed by the contractor, these references aid in generating the data ordered by the CDRL.

Referencing a task in the CDRL does not obviate the need for a DID and/or an NDD.

- The DID is used to describe the format and content of the deliverable data.
- The NDDs also describe the format and content of the deliverable data but is contained within the contract (not a published DID).
    - Concepts and questions regarding the language to manage NDDs include:

- Does a DID exist that meets the need for defining this data deliverable?
  - If so, use it.
  - If not, create an NDD.
- What are the NDDs?
- What components of the NDDs are the stakeholders vested or interested in, e.g., capability, feature, function, or bug correction?
- What data and metrics are needed to track the progress against development of the NDDs, and at what level?

Guidance for R&M data typically required in the conduct of a materiel acquisition program that should be listed in a CDRL is found in this section.

The combination of the CDRLs and appropriate DIDs and/or NDDs defines and schedules the ordering and delivery of data as required by the SOW. Since these documents describe only the data to be submitted by the contractor, neither the CDRL, nor the DID, nor the NDD may impose a requirement for the performance of work tasks. Specifically, the following phrases are prohibited (see MIL-STD-963C) because they task the contractor to perform work:

- "The contractor shall…"
- "… records shall be maintained..."
- "… data shall be prepared…"
- "… data shall be submitted…"
- "… data shall be reviewed…"
- "… data shall be approved by…"

Each CDRL entry, however, must reference the paragraph number, document title, and associated task of the SOW. When completed by the contractor, these references aid in generating the data ordered by the CDRL.

Programs may tailor out DID requirements, but in accordance with MIL-STD-963C, they may not add requirements by tailoring. According to MIL-STD-963C, DIDs should not include the following phrases because they imply requirements can be added by tailoring the DID in the CDRL:

- "… shall include but not be limited to…".
- "… shall include as a minimum…"
- the term "and/or"

Referencing a task in the CDRL does not obviate the need for a DID and/or an NDD. The DID and/or the NDD is used to describe the format and content of the deliverable data.

The contract should require the contractor to provide the Government all the engineering information (data) needed to:

- Show the software design will work in the intended operating environment with the required performance.
- Ensure there are no catastrophic failure modes that will cause loss of life or equipment.
- Identify all critical failure modes (Severity 2) along with the mitigations and compensating provisions needed to provide the warfighter assurance that the software design will meet the mission needs.

Obtaining the preceding engineering information will require non-trivial engineering and analysis, and the R&M engineer will have to work closely with the designer. For COTS or NDI software, there likely will be actual data that shows the design is viable (i.e., it will work satisfactorily), there are no catastrophic failure modes, and all other failure modes previously identified through analysis of failures reported through COTS warranties.

The order of validity of data (objective evidence must be provided in evaluating the validity of data.), from most to least, is:

- Actual operating performance in the intended environment.
- Demonstrated performance in an operating environment.
- Test data from laboratory environment.
- Modeling and simulation data.

The software should also provide for data integration and knowledge base connectivity and processing. The contractor should ensure access to application programming interfaces (APIs), AI agent builders, and seamless integration with existing DoW data lakes, warehouses, and APIs. The platform should support real-time RAG (Retrieval-Augmented Generation) and knowledge base integration to enhance decision-making and operational efficiency.

The remainder of this section provides guidance and examples of R&M data typically required in the conduct of a materiel acquisition program that should be listed in a CDRL. Attachments, such as the CDRL, are often called Exhibits. This sample Exhibit A would be just one of those attachments. The due dates shown in the CDRLs that follow are examples only. R&M engineering should establish due dates based on the program schedule and technical and technology challenges, in coordination with the LSE. When establishing dates, programs should allow sufficient read-ahead time for the R&M engineer, systems engineers, and others to

adequately review the material in advance of the stated event. Due dates could vary between 30 to 60 days (or longer) and would not be applicable in a model-based continuous integration environment. In a digital environment, the contract should define an initial access date for accessing and viewing the data and at a specified frequency.

3.6.2. Sample Contract Data Requirements Lists (DD Form 1423)

All information related to due dates, frequency, and Government approval shown in the following CDRLs are for illustration purposes only. Note that not all the CDRLs apply to software developed under the Software Acquisition pathway. The R&M engineer should coordinate with software engineers to complete all blocks based on program-specific information. This list of CDRLs is not inclusive; a program may need other data, such as from a testability analysis, maintenance task analysis, and other activities stated in a SOW.

Steps for tailoring the DIDs are as follows.

Step 1: Do not create a separate CDRL for software. Insert language for both the hardware reliability and reliable software plans in the same CDRL for the R&M Program Plan, DI-SESS-81613.

Step 2: All information related to due dates, frequency, and Government approval shown in the example CDRLs are recommendations. The reliability engineer should complete all blocks based on program-specific information. Coordinate with the software engineering counterpart so that this deliverable coincides with the SDP.

Step 3: Coordinate with the software engineering counterpart and ensure that the reliability engineer's office symbol is placed into block 14 of the SDP CDRL. The DID for the SDP is DI-IPSC-81427.

Step 4: Remove any shaded text within < >.

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

(1 Data Item)	*OMB No. 0704-0188*	C. CATEGORY: TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
001	Reliability and Maintainability Program Plan	Reliable Software Program Plan (RSPP)

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SESS-81613A	SOW Para: 3.19.1	Reliability Engr Ofc Symbol

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	C	ANNLY	7 DAC
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION
A		BLK 16	BLK 16

16. REMARKS

<This document is not to be copied and pasted into 1423 for contract submittal. It must be tailored as a simplified document \ per the Reliable Software Guidance Document and the Acquisition Strategy. >

Block 8, 11, 13: The Government will review and approve/disapprove. If disapproved the contractor shall correct and resubmit within 30 days after notification of comments.

Block 9: Distribution Statement C - Distribution is authorized to US Government agencies and their contractors; other requests for this document shall be referred to the controlling DOD office.

Export-Control Act Warning – Not Required.

Block 14:

Block 14.a: Addressee –

Point of Contact: RAM Engineer's Name

Email Address: RAM Engineer's E-mail.civ@army.mil

Block 14.b: Submit [via contractor digital engineering environment compatible with XXXXX software] and PDF format via the DoW SAFE file exchange system, https://safe.apps.mil/.

14. DISTRIBUTION

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Reliability Ofc Sym	1	1	0
See BLK 16			

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
002	Risk Management Status Report	Software Reliability Risk Assessment

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SESS-81495B	SOW Para: 3.19.2.5	Reliability Engr Ofc Symbol

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	C	BLK 16	BLK 16
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION
A (See block 16)		BLK 16	BLK 16

16. REMARKS

<This document is not to be copied and pasted into 1423 for contract submittal. It must be tailored per the Reliable Software Guidance Document and the Acquisition Strategy. >

Block 8, 10, 11, 13: The Contractor shall provide the Government with reliable software risk assessment as required..

Block 9: Distribution Statement C - Distribution is authorized to US Government agencies and their contractors; other requests for this document shall be referred to the controlling DOD office.

Export-Control Act Warning – Not Required.

Block 14:

Block 14.a: Addressee –

Point of Contact: RAM Engineer's Name

Email Address: RAM Engineer's E-mail.civ@army.mil

Block 14.b: Submit [via contractor digital engineering environment compatible with XXXXX software] and PDF format via the DoW SAFE file exchange system, https://safe.apps.mil/.

14. DISTRIBUTION

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Reliability Ofc Sym	1	1	0
See BLK 16			

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
003	Scientific and Technical Reports	Mission Profile Definition Report

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-MISC-80711A	SOW Para: 3.19.2.1	Reliability Engr Ofc Symbol

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION
LT	D	ONE/R	(See block 16)	
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION	
A		N/A	ASREQ (See block 16)	

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Other offices: logistics and safety			

16. REMARKS

Block 12: Submission is due as defined in contract.
Block 13: Final Submission is due as defined in contract.

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
004	Reliability and Maintainability Block Diagrams and Mathematical Models Report	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SESS-81496B	SOW Para: 3.19.2.4	Reliability Engr Ofc Symbol

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	C	BLK 16	BLK 16
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION
A (See block 16)		BLK 16	BLK 16

14. DISTRIBUTION			
a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Reliability Ofc	1	1	0
See BLK 16			

16. REMARKS

<This document is not to be copied and pasted into 1423 for contract submittal. It must be tailored per the Reliable Software Guidance Document and the Acquisition Strategy. >

Block 8, 11, 13: The Government will review and approve/disapprove. If disapproved the contractor shall correct and resubmit within 30 days after notification of comments.

Block 9: Distribution Statement C - Distribution is authorized to US Government agencies and their contractors; other requests for this document shall be referred to the controlling DOD office.

Export-Control Act Warning – Not Required.

Block 10: Deliver as required by contract.

Block 12: Deliver as required by contract.

Block 14:

Block 14.a: Addressee –

Point of Contact: RAM Engineer's Name

Email Address: RAM Engineer's E-mail.civ@army.mil

Block 14.b: Submit [via contractor digital engineering environment compatible with XXXXX software] and PDF format via the DoW SAFE file exchange system, https://safe.apps.mil/.

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
005	Reliability and Maintainability Allocation Report	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SESS-81968	SOW Para: 3.19.2.4	Reliability Engr Ofc Symbol

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	C	BLK 16	BLK 16
8. APP CODE		**11. AS OF DATE**	**13. DATE OF SUBSEQUENT SUBMISSION**
A		BLK 16	BLK 16

16. REMARKS

<This document is not to be copied and pasted into 1423 for contract submittal. It must be tailored per the Reliable Software Guidance Document and the Acquisition Strategy. >

Block 8, 11, 13: The Government will review and approve/disapprove. If disapproved the contractor shall correct and resubmit within 30 days after notification of comments.

Block 9: Distribution Statement C - Distribution is authorized to US Government agencies and their contractors; other requests for this document shall be referred to the controlling DOD office.

Export-Control Act Warning – Not Required.

Block 10: Deliver as required by contract.

Block 12: Deliver as required by contract.

Block 14:

Block 14.a: Addressee –

Point of Contact: RAM Engineer's Name

Email Address: RAM Engineer's E-mail.civ@army.mil

Block 14.b: Submit [via contractor digital engineering environment compatible with XXXXX software] and PDF format via the DoW SAFE file exchange system, https://safe.apps.mil/.

14. DISTRIBUTION

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Reliability Ofc Sym	1	1	0
See BLK 16			

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
006	Reliability and Maintainability Predictions Report	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SESS-81497B	SOW Para: 3.19.2.4	Reliability Engr Ofc Symbol

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION			
LT	C	BLK 16	BLK 16	a. ADDRESSEE	b. COPIES		
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION		Draft	Final	
A (See block 16)		BLK 16	BLK 16			Reg	Repro
16. REMARKS Block 8: Government comments or approval will be provided within 30 days after receipt of initial submission. The revised of the report shall be submitted within 30 days after receipt of Government comments. Block 12: Deliver as required by contract. Block 13: Deliver as required by contract.				Other offices: logistics and system safety			

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
007	Failure Modes, Effects, and Criticality Analysis Report (FMECA)	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SESS-81495C	SOW Para: 3.19.2.5	Reliability Engr Ofc Symbol

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	C	BLK 16	BLK 16
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION
A (See block 16)		BLK 16	BLK 16

14. DISTRIBUTION

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Reliability Ofc Sym	1	1	0
See BLK 16			

16. REMARKS

<This document is not to be copied and pasted into 1423 for contract submittal. It must be tailored per the Reliable Software Guidance Document and the Acquisition Strategy. >

Block 8, 11, 13: The Government will review and approve/disapprove. If disapproved the contractor shall correct and resubmit within 30 days after notification of comments.

Block 9: Distribution Statement C - Distribution is authorized to US Government agencies and their contractors; other requests for this document shall be referred to the controlling DOD office.

Export-Control Act Warning – Not Required.

DI Tailoring: For software, omit columns M, P, R, S, T, and U in accordance with the Reliable Software Guidance Document.

Block 10: Deliver as required by contract.

Block 12: Deliver as required by contract.

Block 14:

Block 14.a: Addressee –

Point of Contact: RAM Engineer's Name

Email Address: RAM Engineer's E-mail.civ@army.mil

Block 14.b: Submit [via contractor digital engineering environment compatible with XXXXX software] and PDF format via the DoW SAFE file exchange system, https://safeappsmil/

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
008	System Safety Hazard Analysis Report	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SAFT-80101	SOW Para: 3.19.2.6	

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION			
LT	D	ONE/R	(See block 16)	a. ADDRESSEE	b. COPIES		
					Draft	Final	
						Reg	Repro
8. APP CODE A (See block 16)		11. AS OF DATE N/A	13. DATE OF SUBSEQUENT SUBMISSION ASREQ (See block 16)				
16. REMARKS							
Block 8: Government comments or approval will be provided within 30 days after receipt of initial submission. The revised of the report shall be submitted within 30 days after receipt of Government comments.							
Block 4: Change Section 7.1 of the DID to read, “This Data Item Description (DID) contains the content and format preparation instructions for the data product generated by the Fault Tree Analysis requirement as stated in the contract reference.”				Other offices: logistics and system safety			
Block 4: In Section 10 of the DID, change all occurrences of “component” to “software configuration item”.							
Block 12: A preliminary FTA shall be submitted as required by contract.							

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
009	Reliability Development Growth Test Report	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SESS-81628	SOW Para: 3.19.3.2	

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION
LT	D	ONE/R	(See block 16)	

8. APP CODE	11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION
A (See block 16)	N/A	ASREQ (See block 16)

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Other offices: logistics and system safety			

16. REMARKS

Block 8: Government comments or approval will be provided within 30 days after receipt of initial submission. The revised of the report shall be submitted within 30 days after receipt of Government comments.

Block 12: Submit preliminary report 60D prior to PDR for review and comment. Submit final 60D prior to CDR. Updates as required.

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	**Form Approved** **OMB No. 0704-0188**

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
013	Maintainability and Built-in-Test Demonstration Procedure	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SESS-81604B	SOW Para: 3.19.3.3 and 3.19.3.4	

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION			
LT	D	ONE/R	(See block 16)	a. ADDRESSEE	b. COPIES		
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION		Draft	Final	
A (See block 16)		N/A	ASREQ (See block 16)			Reg	Repro
16. REMARKS							
Block 8: Government comments or approval will be provided within 30 days after receipt of initial submission. The revised of the report shall be submitted within 30 days after receipt of Government comments.				Other offices: logistics and system safety			
Block 12: Submit as required by contract.							

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	Form Approved OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO. 1	B. EXHIBIT A	C. CATEGORY: TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM PROGRAM NAME	E. CONTRACT/PR NO. N00019-01-XXXX	F. CONTRACTOR TBD

1. DATA ITEM NO 011	2. TITLE OF DATA ITEM Maintainability and Built-in-Test Demonstration Report	3. SUBTITLE

4. AUTHORITY (Data Acquisition Document No.) DI-SESS-81603B	5. CONTRACT REFERENCE SOW Para: 3.19.3.3 and 3.19.3.4	6. REQUIRING OFFICE

7. DD 250 REQ LT	9. DIST STATEMENT REQUIRED D	10. FREQUENCY ONE/R	12. DATE OF FIRST SUBMISSION (See block 16)
8. APP CODE A (See block 16)		11. AS OF DATE N/A	13. DATE OF SUBSEQUENT SUBMISSION ASREQ (See block 16)

14. DISTRIBUTION			
a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Other offices: logistics and system safety			

16. REMARKS

Block 4: Applicable for each maintainability and BIT test preformed.
Block 8: Government has 30 days to review and approve.
Block 12 and 13: Submit 60 days after completion of each test

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
010	Software Test Plan	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-IPSC-81438A	SOW Para: 3.19.3.1	

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	D	ONE/R	(See block 16)
8. APP CODE A (See block 16)		11. AS OF DATE N/A	13. DATE OF SUBSEQUENT SUBMISSION ASREQ (See block 16)

14. DISTRIBUTION			
a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Other offices: logistics and system safety			

16. REMARKS

Block 8: Government comments or approval will be provided within 30 days after receipt of initial submission. The revised plan shall be submitted within 30 days after receipt of Government comments.

Block 12 and 13: Submit prior to each software test. Revisions submitted 30 days after receipt of Government comments. Not applicable to programs implementing Agile software development.

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
011	Software Test Description	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-IPSC-81439A	SOW Para: 3.19.3.1	

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION
LT	D	ONE/R	(See block 16)	
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION	
A (See block 16)		N/A	ASREQ (See block 16)	

16. REMARKS	a. ADDRESSEE	b. COPIES		
		Draft	Final	
			Reg	Repro
Block 4: Applicable for each software test preformed. Block 8: Government has 7days to review and approve. Block 12 and 13: Submit 7 days prior to each software test				
	Other offices: logistics and system safety			

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
012	Software Test Report	

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-IPSC-81440A	SOW Para: 3.19.3.1	

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	D	ONE/R	(See block 16)
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION
A (See block 16)		N/A	ASREQ (See block 16)

14. DISTRIBUTION			
a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Other offices: logistics and system safety			

16. REMARKS

Block 8: Government comments or approval will be provided within 30 days after receipt of initial submission. The revised of the report shall be submitted within 30 days after receipt of Government comments.

Block 12: Submit as required by contract. Updates as required to address changes in test program.

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
1	A	TDP _____ TM _____ OTHER ___PS_____

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
PROGRAM NAME	N00019-01-XXXX	TBD

1. DATA ITEM NO	2. TITLE OF DATA ITEM	3. SUBTITLE
013	Failure Summary and Analysis Report	FRACAS

4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-SESS-81628B	SOW Para: 3.19.3.3	Reliability Engr Ofc Symbol

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	C	BLK 16	BLK 16
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION
A (See block 16)		BLK 16	BLK 16

16. REMARKS

<This document is not to be copied and pasted into 1423 for contract submittal. It must be tailored per the Reliable Software Guidance Document and the Acquisition Strategy.>

Block 8, 11, 12, 13: Tailor to key events in Program Milestone.

Block 9: Distribution Statement C - Distribution is authorized to US Government agencies and their contractors; other requests for this document shall be referred to the controlling DOD office.

Export-Control Act Warning – Not Required.

Block 14:

Block 14.a: Addressee –

Point of Contact: RAM Engineer's Name

Email Address: RAM Engineer's E-mail.civ@army.mil

Block 14.b: Submit [via contractor digital engineering environment compatible with XXXXX software] and PDF format via the DoW SAFE file exchange system, https://safeappsmil/.

14. DISTRIBUTION

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
Reliability Ofc Sym	1	1	0
See BLK 16 Also refer to System Safety Ofc.			

3.6.3. Contract Section L – Proposal Instructions (Notice to Offerors)

10 U.S.C. 4328 (formerly 10 U.S.C. 2443) requires that sustainment factors, including R&M, be given ample emphasis in the process for source selection and encourages the use of objective R&M criteria in the evaluation of competitive proposals. Programs address this requirement in section L and M of contracts. Section 4328 is instantiated in DoDI 5000.88: "For ACAT I (MDAPs) and II (Major Systems) weapon systems designs, the PM will include in the contract and in the process for source selection, clearly defined and measurable R&M requirements and engineering activities as required by Section 4328. The PMs of MDAPs and Major Systems must provide justification in the acquisition strategy for not including R&M requirements and engineering activities in TMRR, EMD, or production solicitations or contracts."

3.6.3.1 Instructions for Use

Section L will ask for submission only of sufficient R&M information to support proposal evaluation in accordance with the criteria in Section M. The RFP may provide that an Offeror's proposed specification with values better than required by the RFP may be incorporated into the contract at the time of award. Note that Section M will be carefully structured to include only those criteria likely to be discriminators in the source selection, so the corresponding proposal instructions in Section L will be similarly streamlined.

3.6.3.2 Sample Language

Table 3-10 shows sample Section L language. The R&M engineer should tailor the language based on any responses received from the RFI or draft RFP and to meet any program-specific needs. Programs can add other R&M/BIT proposal requirements as necessary to support the evaluation criteria. To reinforce the critical dependency between sections L and M, bolded text in brackets is included with the sample proposal content requirements as a reference to the contract Section M evaluation criterion.

The sample language applies to all R&M tasks. Software has been integrated into the language. If a particular paragraph does not apply to software, then there is no mention of software in the paragraph. Also, some paragraphs only apply to embedded software.

Table 3-10. Sample Section L Language

(1) Provide system R&M models and predictions that support the software specification requirements (or any higher values proposed by the offeror) and that identify the allocated R&M values of each configuration item. Provide details of data (including field and historical demonstrated data) used in the R&M models to support compliance with the R&M requirements. **EVALUATION FACTOR 1**
(2) Describe the proposed software reliability growth strategy, including the reliability growth planning curve, to plan, track, assess, and improve software reliability. **EVALUATION FACTOR 2**
(3) Provide the R&M program plan strategy and supporting data that consider each element/interface, and functional area for the conduct of R&M activities and how they interface with other internal and external organizations over the life cycle to meet requirements. The proposal shall describe the Offeror's R&M processes, tools, procedures, practices, and schedules for integrating R&M engineering into the system engineering process and the roles and responsibilities of R&M engineers in design, fabrication, and testing of the system, including the integration of software. **EVALUATION FACTOR 3**
(4) Describe proposed R&M design activities and tests to meet the software specification requirements (4.1) Describe the approach and methodology for developing the R&M block diagrams and math models, allocations, and predictions, as well as the process to ensure results are used to impact the software design and coding. Describe the process to ensure analyses are iteratively updated to reflect the current configuration of software configuration items. **EVALUATION FACTOR 4** (4.2) Describe the approach for conducting the SwFMEA. Include the proposed indenture level (i.e., software configuration item) at which the SwFMEA will begin and describe how the FMEA results will be used by the logistic support analysis effort. Describe the process for ensuring that the results of the SwFMEA are used to influence the software design and describe the process for ensuring the SwFMEA is iteratively updated to reflect the current configuration of the software. **EVALUATION FACTOR 4** (4.3) Describe how the failure definition and scoring criteria will be used during development to minimize the occurrence of failures in the field. **EVALUATION FACTOR 4** (4.4) Describe the use of other R&M design activities any other Offeror R&M design techniques to develop reliable software. **EVALUATION FACTOR 4** (4.5) Describe the FRACAS methods to be used during all program phases. Include details of what data will be captured, how failures and anomalies will be analyzed to determine root cause, how corrective actions will be verified as effective, and how results will be communicated throughout the organization for appropriate approval/action. Describe how and when failure review boards, R&M review boards, and other failure and corrective action reviews will be conducted. **EVALUATION FACTOR 4**
(5) Describe the maintainability demonstration (M-demo) and integrated BIT (at the subsystem and system levels) approach to mature system performance to meet the specification requirements.[20] **[EVALUATION FACTOR 5]**

[20] If software is embedded, the M-demo that would be required for the hardware and will implicitly address any software functions related to fault detection and diagnosis. The M-demo and integrated BIT approach applies to all hardware, firmware, and software associated with fault detection, isolation, and diagnosis.

(6) Describe the use of reliability and software tests to identify failures and anomalies, that may or not be detectable by BIT which if uncorrected could cause the level of software reliability to be unacceptable during later stages of integration, testing, or fielding. **EVALUATION FACTOR 5**
(7) Describe how R&M testing is an integral part of the test program and systems engineering verification process. Describe the strategy for verifying software R&M requirements under operationally realistic conditions. **EVALUATION FACTOR 5**
(8) Describe how your internal Value Management program will support Value Assessments to enable a thorough evaluation of mission improvements, efficiencies, and the overall return on investment for the delivered software capabilities. Describe how you will effectively consider and submit Value Engineering Change Proposals (VECPs) to reduce costs on government contracts while improving value to software development efforts. **EVALUATION FACTOR 6**

Other R&M proposal requirements can be added as necessary to support the evaluation criteria.

3.7. Contract Section M – Evaluation Factors for Award R&M Language

10 U.S.C. 4328 requires that sustainment factors, including R&M, be given ample emphasis in the process for source selection and encourages the use of objective R&M criteria in the evaluation of competitive proposals. A program should address this requirement in section L and M of contracts. 10 U.S.C. 4328 is instantiated in DoDI 5000.88: "For ACAT I (MDAPs) and II (Major Systems) weapon systems designs, the PM will include in the contract and in the process for source selection, clearly defined and measurable R&M requirements and engineering activities as required by 10 U.S.C. 4328. The PMs of MDAPs and Major Systems must provide justification in the acquisition strategy for not including R&M requirements and engineering activities in TMRR, EMD, or production solicitations or contracts."

3.7.1. Instructions for Use

Section M should contain short and concise evaluation factors listed in order of priority. Section M should be streamlined to include only those criteria likely to be discriminators in the source selection. Contractor-proposed R&M activities should be supported by appropriate Basis of Estimates (BOE) to ensure R&M cost factors are accounted for in the proposal cost volume. Table 3-11 shows sample Section M language and the R&M engineer should ensure it is aligned with Section L.

Section M needs to be clear that software is a key consideration in the proposal and the following criteria are met.

- The design is proven – the proposed system or subsystems will be built, tested, and documented to meet the proposed R&M requirements.
- The concept is proven – the proposed concept has been demonstrated and documented to meet the proposed R&M requirements.

- There is a documented plan for achieving the following objectives:
    1. R&M is incorporated into all aspects of the system engineering design **including hardware and software.**
    2. The design includes specific features which enhance ease of performing maintenance.
    3. The R&M requirements contained within the Offeror's proposal are achieved and verified throughout the performance of R&M design analyses and test activities including **hardware and software.**
- There is a documented understanding of R&M requirements and plans for the management, design, monitoring, testing, and verification efforts **for both hardware and software**.

3.7.2. Sample Section M Language

Table 3-11 illustrates sample descriptions for the contract evaluation factors. In this case it outlines the criteria of the compliance factors, the plans for the R&M plan, and other key criteria.

Table 3-11. Sample Section M Language

Factor 1: Compliance with Specification Requirements. Compliance with specification R&M requirements for the system that are established by the results of extensive use or by the development methods proposed by the Offeror. Documented understanding of R&M requirements and plans for the management, design, monitoring, testing, and verification efforts for both hardware and software.
Factor 2: Reliability Growth Plan. The adequacy of the proposed software reliability growth plan.
Factor 3: R&M Management. The proposed plan, organization, policies, procedures, and schedules to meet the software specification R&M requirements. Documented plan for achieving the following objectives: (1) R&M is incorporated into all aspects of the system engineering design including hardware and software. (2) The design includes specific features which enhance ease of performing maintenance. (3) The R&M requirements contained within the Offeror's proposal are achieved and verified throughout the performance of R&M design analyses and test activities including hardware and software
Factor 4: R&M design activities. The adequacy of the proposed R&M activities to include design, tests (both development and production), and manufacturing processes to meet the R&M specification requirements. (1) Proven design – the proposed system or subsystems have been built, tested, and documented to meet the proposed R&M requirements. (2) Proven concept – the proposed concept has been demonstrated and documented to meet the proposed R&M requirements.
Factor 5: R&M Verification Testing: The Offeror's approach to compliance with specification verification test requirements.
Factor 6: Value Management Program: The Offeror's plan to incorporate Value Engineering/Analysis techniques in order to reduce costs, technological obsolescence, and acquisition risks, to include the approach for submitting VECPs to reduce Government costs while maintaining system functionality and performance.
Factor 7: Scalability and Vendor-Agnostic Evaluation: The evaluation criteria should prioritize scalability, interoperability, and vendor-agnostic capabilities. Offerors should demonstrate the ability to support multiple LLMs and platforms without duplicative data ingestion efforts. Proposals that include proprietary or locked-in solutions should be considered for disqualification.

Acronyms

AAF	Adaptive Acquisition Framework
ACAT	Acquisition Category
ALT	Accelerated Life Testing
BIT	Built-In Test
BoK	Body of Knowledge
CCMD	Combatant Command
CDD	Capability Development Document
CDE	Common Defect Enumeration
CDRL	Contract Data Requirements List
CI	Commercial Item
CI/CD	Continuous Integration/Continuous Delivery
CNS	Capability Needs Statement
CSCI	Computer Software Configuration Item
CJCS	Chairman of the Joint Chiefs of Staff
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
DBS	Defense Business Systems
D-DIL	Denied, Degraded, Intermittent, and Limited
DevOps	Development and Operations
DevSecOps	Development, Security, and Operations
DID	Data Item Description
DoD	Department of Defense
DoDI	Department of Defense Instruction
DoW	Department of War
cATO	Continuous Authority to Operate
EMD	Engineering and Manufacturing Development
ESS	Environmental Stress Screening
FAR	Federal Acquisition Regulation
FDSC	Failure Definition and Scoring Criteria
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FOSS	Free and Open Source Software
FPGA	Field Programmable Gate Array
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FRB	Failure Review Board
FRP	Full-Rate Production
GFE	Government-Furnished Equipment

GFS	Government Furnished Software
GOTS	Government-Off-the-Shelf
HALT	Highly Accelerated Life Testing
ICD	Initial Capabilities Document
JCIDS	Joint Capabilities Integration and Development System
LSE	Lead Systems Engineer
MBT	Main Battle Tank
MCA	Major Capability Acquisition
MDAP	Major Defense Acquisition Program
MSA	Materiel Solution Analysis
MTA	Middle Tier of Acquisition
MTBF	Mean Time Between Failures
MVCR	Minimum Viable Capability Release
MVP	Minimum Viable Product
NDD	Negotiated Data Deliverable
NDI	Non-Developmental Item
O&S	Operations and Support
OEM	Original Equipment Manufacturer
OMS/MP	Operational Mode Summary/Mission Profile
P&D	Production and Deployment
PM	Program Manager
PM&P	Parts, Materials, and Processes
PoF	Physics-of-Failure
R&M	Reliability and Maintainability
RAM	Reliability, Availability, and Maintainability
RAM-C	Reliability, Availability, Maintainability, and Cost
RCM	Reliability-Centered Maintenance
RFI	Request for Information
RFP	Request for Proposal
RGT	Reliability Growth Testing
PHA	Preliminary Hazard Analysis
RPP	Reliability, Availability, and Maintainability Program Plan
RSP	Reliable Software Program
RSPP	Reliable Software Program Plan
SDP	Software Development Plan
SwFMEA	Software FMEA
SME	Subject Matter Expert
SOW	Statement of Work
SRE	System Reliability Engineering

SRM	System Reliability Model
SQ	Software Quality
TEMP	Test and Evaluation Master Plan
TMRR	Technology Maturation and Risk Reduction
UCA	Urgent Capability Acquisition
UCF	Uniform Contract Format
UON	Urgent Operational Need
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USW(A&S)	Under Secretary of War for Acquisition and Sustainment
VE	Value Engineering
VECP	Value Engineering Change Proposal

References

10 USC, Armed Forces, Section 2430, “Major Defense Acquisition Program Defined.”

10 USC, Armed Forces, Section 4328, “Weapon System Design: Sustainment Factors.”

41 USC, Public Contracts, Section 1711, “Value Engineering.”

Acquisition Knowledge Matrix. Warfighting Acquisition University. [Accessed March 2026.] https://www.dau.edu/news/introducing-acquisition-knowledge-matrix

Adaptive Acquisition Framework (AAF). Defense Acquisition University, 2020. [Accessed March 2026.] https://aaf.dau.edu/

Adaptive Acquisition Framework (AAF) Pathways. Defense Acquisition University, 2020. [Accessed March 2026.] https://aaf.dau.edu/aaf/aaf-pathways/

Agile Software Acquisition Guidebook: Best Practices & Lessons Learned from the FY18 NDAA Section 873/874 Agile Pilot Program. Version 1.0. Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), February 2020. https://www.waru.edu/sites/default/files/Migrated/CopDocuments/AgilePilotsGuidebook%20V1.0%2027Feb20.pdf

Agile Software Development. Wikipedia. https://en.wikipedia.org/wiki/Agile_software_development

ANSI/IEEE Standard Glossary of Software Engineering Terminology. STD-729-1991. American National Standards Institute/Institute for Electrical and Electronics Engineers, 1991.

CJCS Instruction 5123.01H, Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS). Washington, D.C.: Joint Chiefs of Staff, August 31, 2018. https://acqnotes.com/wp-content/uploads/2018/11/CJCSI-5123.01H-Charter-of-the-Joint-Requirements-Oversight-Council-JROC-and-Implementation-of-the-JCIDS-31-Aug-2018.pdf

Data Item Description DI-IPSC-81427B, Software Development Plan. https://assist.dla.mil/

DAU Glossary. *See* Warfighting Acquisition University (WarU) Glossary. https://www.waru.edu/glossary

Defense Federal Acquisition Regulation Supplement (DFARS) Part 215 - Contracting by Negotiation https://www.acquisition.gov/dfars/part-215-contracting-negotiation

DevSecOps. *See* DISA DevSecOps. DoD Cyber Exchange, Defense Information Systems Agency. https://public.cyber.mil/devsecops/

DevSecOps Community of Practice. Air Force DevSecOps. [Accessed March 17, 2026.] https://software.af.mil/dsop/community-of-practice/

Director, Operational Test and Evaluation (DOT&E) Test and Evaluation Master Plan (TEMP) Guidebook 3.1, January 19, 2017.

https://www.dote.osd.mil/Guidance/DOT-E-TEMP-Guidebook/
https://www.dote.osd.mil/Portals/97/docs/TEMPGuide/TEMP_Guidebook_3.1a.pdf?ver=tvFoN__t4Ayelyf5KW2RFA%3d%3d

DISA DevSecOps. DoD Cyber Exchange, Defense Information Systems Agency. https://public.cyber.mil/devsecops/

DoD Directive 5000.01, The Defense Acquisition System. Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), September 9, 2020.

DoD Directive 5000.71, Rapid Fulfillment of Combatant Commander Urgent Operational Needs, USD(A&S), May 25, 2020.

DoD Enterprise DevSecOps Strategy Guide, Version 2.0. DoD Chief Information Officer (CIO) and Principal Deputy Assistant Secretary of Defense for Acquisition, March 2021. https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsStrategyGuide.pdf

DoD Instruction 4245.14, "DoD Value Engineering Program." Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)), October 1, 2024.

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework (AAF)." USD(A&S), January 23, 2020.

DoD Instruction 5000.75, "Business Systems Requirements and Acquisition." USD(A&S), January 24, 2020.

DoD Instruction 5000.80, "Operations of the Middle Tier of Acquisitions (MTA)." USD(A&S), December 30, 2019.

DoD Instruction 5000.81, "Urgent Capability Acquisition." USD(A&S), December 31, 2019.

DoD Instruction 5000.85, "Major Capability Acquisition." Director, Cost Assessment and Program Evaluation (CAPE), November 5, 2021.

DoD Instruction 5000.87, "Operation of the Software Acquisition Pathway." Director, CAPE, October 2, 2020.

DoD Instruction 5000.88, "Engineering of Defense Systems." USD(R&E), November 18, 2020.

DoD Instruction 5000.91, "Product Support Management for the Adaptive Acquisition Framework." USD(A&S), November 4, 2021.

DoD Instruction 5010.44, "Intellectual Property (IP) Acquisition and Licensing." OUSD(A&S), October 16, 2019.

DoD Instruction 5200.44, "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks (TSN)." OUSD(R&E) and Office of the DoD CIO.

DoD Source Selection Procedures: Defense Federal Acquisition Regulation Supplement Procedures, Guidance and Information Subpart 215.3-Source Selection. OUSD(A&S) and Defense Pricing and Contracting, August 2022. https://www.acq.osd.mil/dpap/policy/policyvault/USA000740-22-DPC.pdf

DOT&E TEMP Guidebook. *See* Director, Operational Test and Evaluation (DOT&E) Test and Evaluation Master Plan (TEMP) Guidebook 3.1, January 19, 2017. https://www.dote.osd.mil/Guidance/DOT-E-TEMP-Guidebook/ https://www.dote.osd.mil/Portals/97/docs/TEMPGuide/TEMP_Guidebook_3.1a.pdf?ver=tvFoN__t4Ayelyf5KW2RFA%3d%3d

FCDD-AMR-MR-22-08, Reliable Software Statement of Work Language Guidance. U.S. Army Combat Capabilities Development Command, December 2022.

Federal Acquisition Regulation (FAR). https://www.acquisition.gov/browse/index/far.

Federal Acquisition Regulation (FAR) Subpart 15.2 – Solicitation and Receipt of Proposals and Information. https://www.acquisition.gov/far/part-15#FAR_Subpart_15_2

Joint Software Systems Safety Engineering Handbook. Joint Software Systems Safety Engineering Group, Naval Ordnance and Security Activity, August 2010.

Manual for the Operation of the Joint Capabilities Integration and Development System. Joint Staff J8, October 30, 2021.

MIL-HDBK-61B, Configuration Management Guidance, April 7, 2020.

MIL-HDBK-217, Reliability Prediction of Electronic Equipment, February 28, 1995.

MIL-HDBK-245E, Preparation of Statement of Work (SOW), June 14, 2021.

MIL-HDBK-338B, Electronic Reliability Design, Section 7.4.2, "Parameter Degradation and Circuit Tolerance Analysis," October 1998.

MIL-HDBK-470A, Designing and Developing Maintainable Products and Systems, Volume I, August 4, 1997.

MIL-HDBK-2155, Failure Reporting, Analysis and Corrective Action Taken, September 10, 2014.

MIL-STD 882E W/CHANGE 1, 27 September 2023, Department of Defense Standard Practice, System Safety.

MIL-STD-961E, Defense and Program-Unique Specifications Format and Content, July 16, 2020.

MIL-STD-963C, Data Item Descriptions (DIDs), September 24, 2014.

Monje, Andrew. "Guidance for the Tailoring of R&M Engineering Data." Office of the Deputy Assistant Secretary of Defense, Systems Engineering, April 2016. https://www.cto.mil/wp-content/uploads/2023/09/Tailoring-RM-2016.pdf%20

National Defense Authorization Act (NDAA) for FY 2016, Section 804, Middle Tier Acquisition. 114th Congress.

National Defense Authorization Act (NDAA) for FY 2017, Section 805, Modular Open System Approach in Development of Major Weapon Systems.

National Defense Authorization Act (NDAA) for FY 2017, Section 806, Weapon System Prototyping.

National Defense Authorization Act (NDAA) for FY 2020. Public Law 116-92. 116th Congress, December 20, 2019. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf

Office of the Secretary of War Memorandum. "Reforming the Joint Requirements Process to Accelerate Fielding of Warfighting Capabilities," November 7, 2025, reissue of memo published by Office of the Secretary of Defense, August 20, 2025. https://media.defense.gov/2025/Nov/10/2003819442/-1/-1/1/REFORMING-THE-JOINT-REQUIREMENTS-PROCESS-TO-ACCELERATE-FIELDING-OF-WARFIGHTING-CAPABILITIES.PDF

Reliability and Maintainability Engineering Management Body of Knowledge (R&M BoK). OUSW(R&E), 2025. https://www.cto.mil/sea/rm

Software Acquisition. Adaptive Acquisition Framework. Defense Acquisition University, 2023. [Accessed March 2026.] https://aaf.dau.edu/aaf/software/

Warfighting Acquisition University (WarU) Glossary. https://www.waru.edu/glossary

Commercial Standards

IEEE 1633-2016 Recommended Practices for Software Reliability, January 2017

SAE JA1003: 201205 Software Reliability Program Implementation Guide

SAE JA 1005: 2012 Software Supportability Program Implementation Guide

SAE JA1006: 201205 Software Support Concept

This page is intentionally blank.

Reliability and Maintainability Engineering Contract Language for the Software Acquisition Pathway

April 2026

Office of the Under Secretary of War for Research and Engineering
Systems Engineering and Architecture
osd-sea@mail.mil
https://www.cto.mil/sea/