Software Engineering Institute

# Incorporating Software Requirements into the System RFP

## Survey of RFP Language for Software by Topic, v. 2.0

Edited by Charlene Gross

**MAY 2009**

**SPECIAL REPORT**
CMU/SEI-2009-SR-008

**Acquisition Support Program**


http://www.sei.cmu.edu

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.



For information about purchasing paper copies of SEI reports, please visit the publications section of our website (http://www.sei.cmu.edu/publications/).

# Table of Contents


**1 Introduction 1**

**2 Overview of RFP Sections C, M, and L 2**

**3 Licensing Intellectual Property for Government Use 5**

3.1 Deferred Delivery of Technical Data or Computer Software 6
3.2 Deferred Ordering of Technical Data or Computer Software 7
3.3 Identification and Assertion of Use, Release, or Disclosure Restrictions 8
3.4 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends 11
3.5 Rights in Bid or Proposal Information 14
3.6 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation 16
3.7 Rights in Noncommercial Technical Data and Computer Software—Small Business Innovation Research (SBIR) Program 27
3.8 Rights in Special Works 40
3.9 Rights in Technical Data and Computer Software (Foreign) 42
3.10 Technical Data or Computer Software Previously Delivered to the Government. 43
3.11 Third Party Development 44
3.12 Validation of Asserted Restrictions - Computer Software 45
3.13 Validation of Restrictive Markings on Technical Data 50

**4 Process and Product Support Activities 55**

4.1 Automated Development and Support Environment 56
4.2 Certification and Accreditation Processes 57
4.3 Configuration Management Audit 58
4.4 Defect Prevention 59
4.5 Measures 60
4.6 Quality Assurance Program General Requirements 64
4.7 Quality Assurance Program Plan 66
4.8 Quality Assurance Reviews and Audits 67
4.9 Risk Identification and Mitigation Approach 68
4.10 Risk Management 69
4.11 Risk Program Approach 70
4.12 Securely Configuring Proprietary Commercial Software 71
4.13 Security Controls and Standards 72
4.14 Software Assurance Case Submission 73
4.15 Software Security Acceptance and Measurement Criteria 74
4.16 Trustworthy Software 75

**5 Project Management 77**

5.1 Contractor Monitoring 78
5.2 Contractor Statement of Work (CSOW) 79
5.3 Contractor Work Breakdown Structure (CWBS) 84
5.4 Corrective Action 85
5.5 Cost and Schedule 86
5.6 Design Information Documentation 87

| | | | |
|---|---|---|---|
| | 5.7 | Information Development Environment (IDE) | 88 |
| | 5.8 | Integrated Master Plan Approach | 90 |
| | 5.9 | Management Plan Approach | 95 |
| | 5.10 | Modular Open Systems Support Plan | 97 |
| | 5.11 | Operations and Maintenance | 98 |
| | 5.12 | Past Performance Qualifications | 99 |
| | 5.13 | Process Maturity | 105 |
| | 5.14 | Program Protection Plan and Information Assurance (IA) | 108 |
| | 5.15 | Software Development Plan (SDP) | 109 |
| | 5.16 | Software Documentation | 113 |
| | 5.17 | Software Integrated Process Team | 114 |
| | 5.18 | Subcontractor Control | 115 |
| | 5.19 | Support Planning | 116 |
| | 5.20 | Systems Engineering Approach | 119 |
| | 5.21 | Technical Management Process | 122 |
| | 5.22 | Transition Plan | 124 |
| | 5.23 | Treatment of Proprietary or Vendor Unique Elements | 125 |
| **6** | **Safety-Critical Software** | | **127** |
| | 6.1 | Flight Readiness Review (FRR) | 128 |
| | 6.2 | Hazard and SFMECA Testing | 129 |
| | 6.3 | Hazard Criticality Matrix | 130 |
| | 6.4 | Safety-Critical Software - Developer Design Reviews | 131 |
| | 6.5 | Safety-Critical Software - Failure Analysis | 137 |
| | 6.6 | Safety-Critical Software - Hazard Causal Factor Analysis | 138 |
| | 6.7 | Safety-Critical Software - Identification | 139 |
| | 6.8 | Safety Critical Software - Incremental SW Product Delivery | 140 |
| | 6.9 | Safety-Critical Software - Interface Requirements Specification | 141 |
| | 6.10 | Safety-Critical Software - Preliminary Hazard Analysis | 142 |
| | 6.11 | Safety-Critical Software - Required RFP Items for Airworthiness | 143 |
| | 6.12 | Safety-Critical Software - Required RFP Items for Safety | 144 |
| | 6.13 | Safety-Critical Software - Safety Assessment Report | 145 |
| | 6.14 | Safety-Critical Software - SW Safety Critical Function Analysis (SSCFA) Report | 146 |
| | 6.15 | Safety-Critical Software - Software/Firmware Safety Assessment Process | 147 |
| | 6.16 | Safety-Critical Software - Software/Subsystem Hazard Analysis | 148 |
| | 6.17 | Safety-Critical Software - Software Hazard Analysis Tracking Reports | 149 |
| | 6.18 | Safety-Critical Software - Structural Coverage Analysis/Test | 150 |
| | 6.19 | Safety-Critical Software - Structural Testing | 151 |
| | 6.20 | Safety-Critical Software - System/Software Safety Program Plan | 152 |
| **7** | **Software Architecture and Quality Attributes** | | **153** |
| | 7.1 | Software Architecture Definitions | 154 |
| | 7.2 | Modeling and Simulation | 155 |
| | 7.3 | Modular Design and Technology Insertion | 156 |
| | 7.4 | Modular Open Systems Approach (MOSA) | 157 |
| | 7.5 | Modular Open Systems Design | 164 |
| | 7.6 | Open Architecture | 165 |
| | 7.7 | Open Systems and Life-Cycle Management | 166 |
| | 7.8 | Quality Attribute Requirements | 168 |

7.9 Reliability, Availability, and Maintainability (RAM) 169
7.10 Scalability Support 173
7.11 Software Architecture Approach 174
7.12 Software Architecture Development 176
7.13 Software Architecture - Documentation of Engineering Efforts 177
7.14 Software Architecture Evaluation 178
7.15 Software Architecture 185
7.16 Software Architecture Pre-Award Demonstration 186
7.17 Software Architecture Quality Requirements 188
7.18 Software Architecture Reviews and Technical Interchange Meetings 190
7.19 Software Architecture System Evaluations 191
7.20 Software Architecture System Specifications 192
7.21 Throughput Timing 193

**8 Technical Solutions and Products 194**
8.1 Commercial Off-The-Shelf Software (COTS) 195
8.2 Commercial Off-The-Shelf Software Use 197
8.3 Human Systems Integration/Human Factors Engineering 198
8.4 Independent Witnessing of Software Test Activities 199
8.5 Interface Design and Management 200
8.6 Inter-Component Dependencies 202
8.7 Net-Centric Strategy 203
8.8 Net-Centric Technical Requirements Document (TRD) 205
8.9 Network Architecture and Functionality 206
8.10 Network Management and Operations 210
8.11 Programming Language Selection 216
8.12 Requirements Traceability 217
8.13 Requirements Verification 218
8.14 Reuse 219
8.15 Software Design Assessments 221
8.16 System Requirements 222
8.17 Technical Performance Requirements Criteria 223
8.18 Technology Readiness Assessment 225
8.19 Technical Solution and Technical Supporting Data 226
8.20 Test and Evaluation 227

**References 228**

**Index 233**

# 1 Introduction

Organizations that are in the process of developing a Request for Proposal (RFP) have often looked to existing sources for ideas on how to phrase language to cover a specific topic. They are often disappointed to learn that the search for RFP language examples is a time-consuming exercise that involves searching across multiple publications that may or may not include the topical information that they seek.

The Carnegie Mellon Software Engineering Institute™ (SEI) has initiated an effort to compile publicly available recommendations for RFP content and examples of language for RFP Sections C, M, and L. The sources are referenced in the text and fully listed at the end of this document. This paper was developed in response to Task 2.2.2 of the FY09 Strategic Software Improvement Plan (SSIMP), which is the implementation plan for the Army Strategic Software Improvement Program (ASSIP). Task 2.2.2 seeks to "define and communicate the software engineering and management events and deliverables necessary to be included in the Request for Proposal (RFP) or the contract to support successful acquisition of software intensive systems."[1]

Please note that we have elected to discuss the specifics of Section M before L since that is the order in which the effort is needed. Evaluation factors are defined before one can complete the Instructions to Offerors, so that Section L directly elicits information supporting Section M.

It should also be noted that the material is provided exactly as written in the original sources, and there is no information in these sources regarding the effectiveness or appropriateness of the language in a particular context. However, this information can serve as a starting point for determining phrasing that will lead to desired results. These language suggestions should be tailored for organizational needs and in accordance with the acquirers' legal authorities and organizational policies and procedures.

We invite the community to provide additional examples of language and recommendations for the sections covered by this document or for additional sections that it would be useful to add. Send your comments and recommendations to*: rfp-survey@sei.cmu.edu*

™ Carnegie Mellon and Software Engineering Institute are trademarks of Carnegie Mellon University.

1 ASSIP is a long-term partnership among the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA(ALT)); the Army's Program Executive Officers (PEOs), direct reporting program managers (DRPMs), and the SEI to dramatically improve the acquisition of software intensive systems. The Army's Software Engineering Centers (SECs), Training and Doctrine Command (TRADOC), Army Test and Evaluation Command (ATEC), and the Army CIO-G6 also participate in ASSIP. The ASSIP is focused on acquisition programs, people, production/sustainment, and institutionalizing continuous improvement.

# 2 Overview of RFP Sections C, M, and L

The government solicits proposals from potential offerors through the issuance of a solicitation. In negotiated procurements, this document is called a Request for Proposal (RFP). The RFP includes information necessary for the offerors to understand what the government is buying, what information they must provide, and how their proposals will be evaluated [Army 2008].

The success of an acquisition is directly linked to the quality of the RFP. A well-written RFP will

- facilitate a fair competition
- limit criteria to discriminators that add value
- clearly detail information required by the offerors
- clearly identify the evaluation and award criteria
- preserve the offerors' flexibility to propose innovative solutions
- convey a clear understanding of the government's requirements
- specify areas where the offerors can make technical and cost tradeoffs in their proposals [Army 2008]

Our focus on Sections C, M, and L is based on the number of examples of publicly available language that were available. Please note that we treat Section M before Section L because understanding the evaluation factors precedes developing a list of required proposal information.

*Uniform Contract Format*

| **Section** | **Title** |
|---|---|
| Part I—The Schedule | |
| A | Solicitation/contract form |
| B | Supplies or services and prices/costs |
| C | Description/specifications/statement of work |
| D | Packaging and marking |
| E | Inspection and acceptance |
| F | Deliveries or performance |
| G | Contract administration data |
| H | Special contract requirements |
| Part II—Contract Clauses | |
| I | Contract clauses |
| Part III—List of Documents, Exhibits, and Other Attachments | |
| J | List of attachments |

| Part IV—Representations and Instructions | |
|---|---|
| K | Representations, certifications, and other statements of offerors or respondents |
| L | Instructions, conditions, and notices to offerors or respondents |
| M | Evaluation factors for award |

[FAR]

**Section C** is part of *Part 1 – The Schedule* of the typical RFP. In our search for publicly available language, we found that Section C provided publicly accessible and attributable language in sufficient quantity to be included in this document. Section C (includes Description/Specification/ Statement of Objectives (SOO) or Statement of Work (SOW) and contains the description of the products to be delivered or the work to be performed under the contract. This section typically includes the government's SOO (or SOW) and preliminary system performance specification [DOD 2006].

Sections **L and M** are in *Part IV—Representations and Instructions.* **Section M** of the RFP states the evaluation factors that are used for selecting the contractor. Section M should be carefully structured to address only those elements determined to be discriminators in the source selection to select the best proposal with acceptable program risk. The most effective Section M evaluation factors are measurable, relevant to the program, traceable, with expected differentiation among the offers, and under the offeror's control. Section M should not contain any evaluation factors or subfactors for which there is not a corresponding request for proposal information in Section L. In preparing Sections M and L, be aware of the proposal preparation time and page limitations. Ask only for information that should be readily available to offerors and that is necessary to accomplish the source selection evaluation [DOD 2006].

**Section L** of the RFP instructs the offerors on how to structure their proposal and what should be included in each proposal section. It needs to clearly identify the structure and composition of each volume and section of the proposal and should track to the evaluation factors in Section M [DOD 2006].

The technical definition of the computer software architecture and data metamodel, estimated sizing, throughput timing, and growth migration strategy also need to be defined as criteria in Section L and in the offeror's proposal [SMC 2004].

The questions below help to develop the technical aspects of Section M and Section L [DOD 2006].

**Example questions for developing specific software engineering-related criteria and instructions for Sections M and L**

1. How will the evaluation team establish an understanding of the offerors' technical approach?
2. How can the evaluation team develop confidence that the offerors' proposed technical design solutions will meet all technical requirements, including operational performance and logistics/sustainment requirements?
3. Is the technical approach implemented within performance, cost, and schedule requirements?

4. How will the evaluation team evaluate the system-of-systems (SOS) or family-of-systems (FOS) interfaces and integration issues on the program?
5. How will the evaluation team establish whether the specific plans for implementing and managing the technical (i.e., software engineering [SE]) and technical management processes are based on company enterprise processes? Is there objective evidence of the capability or maturity of these processes based on industry best practices? How will they be evaluated for consistency and compatibility with the government's technical and management processes (as defined in the Systems Engineering Plan [SEP])?
6. How will the evaluation team determine that the domain experience, past performance, and process maturity of the specific project team, company subgroup, teammates, and subcontractors proposed to execute the work directly related to the program being bid?
7. How will the evaluation team understand whether the proposed technical solution is adequately supported by studies, analyses, modeling and simulations, and demonstrations?
8. How will the evaluation team evaluate the fidelity and appropriateness of modeling and simulation proposed for the project, and how will it be validated?
9. How will the evaluation team determine whether the offeror's proposed information architecture (IA) approach solution meets Department of Defense (DoD) requirements? How will it do the same for any security or safety engineering requirements?
10. How will the evaluation team assess the maturity and application of the offeror's proposed processes in the proposal risk assessment?
11. How will the evaluation team determine that the risk management approach proposed is appropriate for the program being bid (for example, consistent and compatible with the government's risk management process)?
12. How will the evaluation team determine that technical cost and resources proposed for the program are reasonable and realistic for the planned program approach?

    How will the evaluation team establish that the offeror's proposed schedule is realistic and that the critical path(s) analysis is realistic [DOD 2006]?

**NOTE:** For our discussion in this report's Section 3, Licensing Intellectual Property for Government Use, we have included RFP **Section I** – Contract Clauses. Because the acquisition of rights to computer software and computer software documentation is a special interest in the community, we have incorporated examples of Section I language that are relevant for acquiring these rights. Contracting officers are well-versed on the clauses that should be included to address specific issues, but acquiring organizations should have some knowledge regarding clause content and applicability. These clauses consist of Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), and other local clauses, and are readily available in those regulations. Section I incorporates the clauses by reference with the same force and effect as if they were given in full text.

# 3 Licensing Intellectual Property for Government Use

This section of this report includes examples of contract clauses (Section I) that can be used in RFPs to define the type(s) of “license to use” that the government expects or requires when acquiring software and software documentation. While contracting officers are responsible for inserting contract clauses, data managers or other requirements personnel are responsible for identifying the government's minimum needs. To do this, data managers and requirements personnel must understand their options.

In addition to desired software performance, compatibility, or other technical considerations, needs determinations should consider factors such as multiple-site or shared use requirements; whether the government’s software maintenance philosophy will require the right to modify or have third parties modify the software; and any special computer software documentation requirements. Due to the shared responsibility between data manager and contracting and the cost associated with failures to understand options, the pertinent DFARS contract clauses are shown here to increase the understanding of those who are participating in RFP development [DOD 2007].

### 3.1 Deferred Delivery of Technical Data or Computer Software

#### 3.1.1 Section C - SOW/SOO; Requirements

#### 3.1.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7026]

As prescribed at 227.7103-8(a) and 227.7203-8, use the following clause:

Deferred Delivery Of Technical Data Or Computer Software

(Apr 1988)

*The Government shall have the right to require, at any time during the performance of this contract, within two (2) years after either acceptance of all items (other than data or computer software) to be delivered under this contract or termination of this contract, whichever is later, delivery of any technical data or computer software item identified in this contract as "deferred delivery" data or computer software. The obligation to furnish such technical data required to be prepared by a subcontractor and pertaining to an item obtained from him shall expire two (2) years after the date Contractor accepts the last delivery of that item from that subcontractor for use in performing this contract.*

(End of clause)

GENERAL RECOMMENDATIONS

This clause applies to Technical Data and Computer Software/Documentation. Review the complete text of DFARS 227.71 and DFARS 227.72 for [DOD 2007]:

- Specific uses of 252.227-7026
- Clauses used in conjunction with 252.227-7026.
- Clauses used instead of 252.227-7026

#### 3.1.3 Section M - Evaluation

#### 3.1.4 Section L - Instructions to Offerors

## 3.2 Deferred Ordering of Technical Data or Computer Software

### 3.2.1 Section C - SOW/SOO; Requirements

### 3.2.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7027]

As prescribed at 227.7103-8(b) and 227.7203-8, use the following clause:

Deferred Ordering Of Technical Data Or Computer Software

(Apr 1988)

*In addition to technical data or computer software specified elsewhere in this contract to be delivered hereunder, the Government may, at any time during the performance of this contract or within a period of three (3) years after acceptance of all items (other than technical data or computer software) to be delivered under this contract or the termination of this contract, order any technical data or computer software generated in the performance of this contract or any subcontract hereunder. When the technical data or computer software is ordered, the Contractor shall be compensated for converting the data or computer software into the prescribed form, for reproduction and delivery. The obligation to deliver the technical data of a subcontractor and pertaining to an item obtained from him shall expire three (3) years after the date the Contractor accepts the last delivery of that item from that subcontractor under this contract. The Government's rights to use said data or computer software shall be pursuant to the "Rights in Technical Data and Computer Software" clause of this contract.*

(End of clause)

GENERAL RECOMMENDATIONS

This clause applies to Technical Data and Computer Software/Documentation Review the complete text of DFARS 227.71 and 227.72 for:

- Specific uses of 252.227-7027
- Clauses used in conjunction with 252.227-7027
- Clauses used instead of 252.227-7027

### 3.2.3 Section M - Evaluation

### 3.2.4 Section L - Instructions to Offerors

## 3.3 Identification and Assertion of Use, Release, or Disclosure Restrictions

### 3.3.1 Section C - SOW/SOO; Requirements

### 3.3.2 Section I - Contract Clauses

**EXAMPLE 1**

[DFARS 252.227.7017]

As prescribed in 227.7103-3(b), 227.7104(e)(2), and 227.7203-3(a), use the following provision:

Identification And Assertion Of Use, Release, Or Disclosure Restrictions (Jun 1995)

(a) *The terms used in this provision are defined in following clause or clauses contained in this solicitation—*

1) *If a successful offeror will be required to deliver technical data, the Rights in Technical Data—Noncommercial Items clause, or, if this solicitation contemplates a contract under the Small Business Innovative Research (SBIR) Program, the Rights in Noncommercial Technical Data and Computer Software—Small Business Innovative Research (SBIR) Program clause.*

2) *If a successful offeror will not be required to deliver technical data, the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause, or, if this solicitation contemplates a contract under the SBIR Program, the Rights in Noncommercial Technical Data and Computer Software—Small Business Innovative Research (SBIR) Program clause.*

(b) *The identification and assertion requirements in this provision apply only to technical data, including computer software documentation, or computer software to be delivered with other than Unlimited rights. For contracts to be awarded under the SBIR Program, the notification and identification requirements do not apply to technical data or computer software that will be generated under the resulting contract. Notification and identification is not required for restrictions based solely on copyright.*

(c) *Offers submitted in response to this solicitation shall identify, to the extent known at the time an offer is submitted to the Government, the technical data or computer software that the Offeror, its subcontractors or suppliers, or potential subcontractors or suppliers, assert should be furnished to the Government with restrictions on use, release, or disclosure.*

(d) *The Offeror's assertions, including the assertions of its subcontractors or suppliers or potential subcontractors or suppliers, shall be submitted as an attachment to its offer in the following format, dated and signed by an official authorized to contractually obligate the Offeror:*

Identification and Assertion of Restrictions on the Government's Use, Release, or Disclosure of Technical Data or Computer Software.

The Offeror asserts for itself, or the persons identified below, that the Government's rights to use, release, or disclose the following technical data or computer software should be restricted:

| Technical Data or Computer Software to be Furnished With Restrictions* | Basis for Assertion** | Asserted Rights Category*** | Name of Person Asserting Restrictions**** |
|---|---|---|---|
| (LIST)***** | (LIST) | (LIST) | (LIST) |

*For technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process. For computer software or computer software documentation identify the software or documentation.

**Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions. For technical data, other than computer software documentation, development refers to development of the item, component, or process to which the data pertain. The Government's rights in computer software documentation generally may not be restricted. For computer software, development refers to the software. Indicate whether development was accomplished exclusively or partially at private expense. If development was not accomplished at private expense, or for computer software documentation, enter the specific basis for asserting restrictions.

***Enter asserted rights category (e.g., Government purpose license rights from a prior contract, rights in SBIR data generated under another contract, limited, restricted, or Government purpose rights under this or a prior contract, or specially negotiated licenses).

****Corporation, individual, or other person, as appropriate.

*****Enter “none” when all data or software will be submitted without restrictions.

Date ______________________________________
Printed Name and Title ______________________________________
______________________________________
Signature ______________________________________

(End of identification and assertion)

*(e) An offeror's failure to submit, complete, or sign the notification and identification required by paragraph (d) of this provision with its offer may render the offer ineligible for award.*

*(f) If the Offeror is awarded a contract, the assertions identified in paragraph (d) of this provision shall be listed in an attachment to that contract. Upon request by the Contracting Officer, the Offeror shall provide sufficient information to enable the Contracting Officer to evaluate any listed assertion.*

*(End of provision)*

GENERAL RECOMMENDATIONS

This clause applies to both Technical Data and Computer Software/Documentation. Review the complete text of DFARS 227.71 and 227.72 for:

- Specific uses of 252.227-7017
- Clauses used in conjunction with 252.227-7017.
- Clauses used instead of 252.227-7017

### 3.3.3 Section M - Evaluation

### 3.3.4 Section L - Instructions to Offerors

## 3.4 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends

### 3.4.1 Section C - SOW/SOO; Requirements

### 3.4.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7025]

As prescribed in 227.7103-6(c), 227.7104(f)(1), or 227.7203-6(d), use the following clause:

Limitations On The Use Or Disclosure Of Government-Furnished Information Marked With Restrictive Legends

(Jun 1995)

*(a) 1) For contracts requiring the delivery of technical data, the terms "License to use computer software" and "Government purpose rights" are defined in the Rights in Technical Data—Noncommercial Items clause of this contract.*

*2) For contracts that do not require the delivery of technical data, the terms "Government purpose rights" and "restricted rights" are defined in the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause of this contract.*

*3) For SBIR program contracts, the terms "License to use computer software" and "restricted rights" are defined in the Rights in Noncommercial Technical Data and Computer Software—Small Business Innovative Research (SBIR) Program clause of this contract.*

*(b) Technical data or computer software provided to the Contractor as Government-furnished information (GFI) under this contract may be subject to restrictions on use, modification, reproduction, release, performance, display, or further disclosure.*

*1) GFI marked with limited or restricted rights legends. The Contractor shall use, modify, reproduce, perform, or display technical data received from the Government with License to use computer software legends or computer software received with restricted rights legends only in the performance of this contract. The Contractor shall not, without the express written permission of the party whose name appears in the legend, release or disclose such data or software to any person.*

*2) GFI marked with Government purpose rights legends. The Contractor shall use technical data or computer software received from the Government with Government purpose rights legends for Government purposes only. The Contractor shall not, without the express written permission of the party whose name appears in the restrictive legend, use, modify, reproduce, release, perform, or display such data or software for any commercial purpose or disclose such data or software to a person other than its subcontractors, suppliers, or prospective subcontractors or suppliers, who require the data or software to* *submit offers for, or perform, contracts under this contract. Prior to disclosing the data or software, the Contractor shall require the persons to whom disclosure will be made to complete and sign the non-disclosure agreement at 227.7103-7 of the Defense Federal Acquisition Regulation Supplement (DFARS).*

3) *GFI marked with specially negotiated license rights legends. The Contractor shall use, modify, reproduce, release, perform, or display technical data or computer software received from the Government with specially negotiated license legends only as permitted in the license. Such data or software may not be released or disclosed to other persons unless permitted by the license and, prior to release or disclosure, the intended recipient has completed the non-disclosure agreement at DFARS 227.7103-7. The Contractor shall modify paragraph (1)(c) of the non-disclosure agreement to reflect the recipient's obligations regarding use, modification, reproduction, release, performance, display, and disclosure of the data or software.*

*(c) Indemnification and creation of third party beneficiary rights. The Contractor agrees—*

1) *To indemnify and hold harmless the Government, its agents, and employees from every claim or liability, including attorneys fees, court costs, and expenses, arising out of, or in any way related to, the misuse or unauthorized modification, reproduction, release, performance, display, or disclosure of technical data or computer software received from the Government with restrictive legends by the Contractor or any person to whom the Contractor has released or disclosed such data or software; and*
2) *That the party whose name appears on the restrictive legend, in addition to any other rights it may have, is a third party beneficiary who has the right of direct action against the Contractor, or any person to whom the Contractor has released or disclosed such data or software, for the unauthorized duplication, release, or disclosure of technical data or computer software subject to restrictive legends.*

(End of clause)

GENERAL RECOMMENDATIONS

This clause applies to both Technical Data and Computer Software/Documentation. Review the complete text of DFARS 227.71 and 227.72 for:

- Specific uses of 252.227-7025
- Clauses used in conjunction with 252.227-7025.
- Clauses used instead of 252.227-7025

### 3.4.3 Section M - Evaluation

### 3.4.4 Section L - Instructions to Offerors

EXAMPLE 1

Attachment CDX to Volume X: Technical Data Restrictions [USAF 2005]

*Pursuant to DFARS provision 252.227-7013, list any data which the Offeror proposes to deliver with other than unlimited rights, and define the limitations it proposes to apply (e.g., limited rights, Government Purpose License Rights, etc.). If the Offeror notifies the Government that technical data will be delivered with other than unlimited rights, the notice shall be accompanied by the representation found in DFARS 252.227-7013(j), and shall be included herein. For all such instances, include:*

*Name of party claiming rights in data (the prime or subcontractor)*

*Type of items, components, processes or computer software*

*Description of technical data or computer software*

*Type of Government rights restrictions*

### 3.5 Rights in Bid or Proposal Information

#### 3.5.1 Section C - SOW/SOO; Requirements

#### 3.5.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7016]

*As prescribed in 227.7103-6(e)(1), 227.7104(e)(1), or 227.7203-6(b), use the following clause:*

*Rights In Bid Or Proposal Information*

*(Jun 1995)*

*Definitions.*

*For contracts that require the delivery of technical data, the terms “technical data” and “computer software” are defined in the Rights in Technical Data—Noncommercial Item clause of this contract or, if this is a contract awarded under the SBIR Program, the Rights in Noncommercial Technical Data and Computer Software—Small Business Innovative Research (SBIR) Program clause of this contract.*

*(2) For contracts that do not require the delivery of technical data, the term “computer software” is defined in the Rights in Noncommercial Computer and Noncommercial Computer Software Documentation clause of this contract or, if this is a contract awarded under the SBIR Program, the Rights in Noncommercial Technical Data and Computer Software—Small Business Innovative Research (SBIR) Program clause of this contract.*

*(b) Government rights prior to contract award. By submission of its offer, the Offeror agrees that the Government—*

*(1) May reproduce the bid or proposal, or any portions thereof, to the extent necessary to evaluate the offer.*

*(2) Except as provided in paragraph (d) of this clause, shall use information contained in the bid or proposal only for evaluation purposes and shall not disclose, directly or indirectly, such information to any person including potential evaluators, unless that person has been authorized by the head of the agency, his or her designee, or the Contracting Officer to receive such information.*

*(c) Government rights subsequent to contract award. The Contractor agrees—*

*(1) Except as provided in paragraphs (c)(2), (d), and (e) of this clause, the Government shall have the rights to use, modify, reproduce, release, perform, display, or disclose information contained in the Contractor's bid or proposal within the Government. The Government shall not release, perform, display, or disclose such information outside the Government without the Contractor's written permission.*

*(2) The Government’s rights to use, modify, reproduce, release, perform, display, or disclose information that is technical data or computer software required to be delivered under this contract are determined by the Rights in Technical Data—Noncommercial Items, Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation, or Rights in Noncommercial*

*Technical Data and Computer Software—Small Business Innovative Research (SBIR) Program clause(s) of this contract.*

(d) *Government-furnished information (GFI). The Government's rights with respect to technical data or computer software contained in the Contractor's bid or proposal that were provided to the Contractor by the Government are subject only to restrictions on use, modification, reproduction, release, performance, display, or disclosure, if any, imposed by the developer or licensor of such data or software.*

(e) *Information available without restrictions. The Government's rights to use, modify, reproduce, release, perform, display, or, disclose information contained in a bid or proposal, including technical data or computer software, and to permit others to do so, shall not be restricted in any manner if such information has been released or disclosed to the Government or to other persons without restrictions other than a release or disclosure resulting from the sale, transfer, or other assignment of interest in the information to another party or the sale or transfer of some or all of a business entity or its assets to another party.*

(f) *Flowdown. The Contractor shall include this clause in all subcontracts or similar contractual instruments and require its subcontractors or suppliers to do so without alteration, except to identify the parties.*

(End of clause)

GENERAL RECOMMENDATIONS

This clause applies to both Technical Data and Computer Software/Documentation. Review the complete text of DFARS 227.71 and 227.72 for:

- Specific uses of 252.227-7016
- Clauses used in conjunction with 252.227-7016.
- Clauses used instead of 252.227-7016

### 3.5.3 Section M - Evaluation

### 3.5.4 Section L - Instructions to Offerors

## 3.6 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation

### 3.6.1 Section C - SOW/SOO; Requirements

### 3.6.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7014]

Rights In Noncommercial Computer Software And Noncommercial Computer Software Documentation

*(a) Definitions. As used in this clause:*

*(1) "Commercial computer software" means software developed or regularly used for non-Governmental purposes which—*

*(i) Has been sold, leased, or licensed to the public;*

*(ii) Has been offered for sale, lease, or license to the public;*

*(iii) Has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this contract; or*

*(iv) Satisfies a criterion expressed in paragraph (a)(1)(i), (ii), or (iii) of this clause and would require only minor modification to meet the requirements of this contract.*

*(2) "Computer database" means a collection of recorded data in a form capable of being processed by a computer. The term does not include computer software.*

*(3) "Computer program" means a set of instructions, rules, or routines, recorded in a form that is capable of causing a computer to perform a specific operation or series of operations.*

*(4) "Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer databases or computer software documentation.*

*(5) "Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.*

*(6) "Developed" means that—*

*(i) A computer program has been successfully operated in a computer and tested to the extent sufficient to demonstrate to reasonable persons skilled in the art that the program can reasonably be expected to perform its intended purpose;*

*(ii)* *Computer software, other than computer programs, has been tested or analyzed to the extent sufficient to demonstrate to reasonable persons skilled in the art that the software can reasonably be expected to perform its intended purpose; or*

*(iii)* *Computer software documentation required to be delivered under a contract has been written, in any medium, in sufficient detail to comply with requirements under that contract.*

*(7)* *"Developed exclusively at private expense" means development was accomplished entirely with costs charged to indirect cost pools, costs not allocated to a Government contract, or any combination thereof.*

*(i)* *Private expense determinations should be made at the lowest practicable level.*

*(ii)* *Under fixed-price contracts, when total costs are greater than the firm-fixed-price or ceiling price of the contract, the additional development costs necessary to complete development shall not be considered when determining whether development was at Government , private, or mixed expense.*

*(8)* *"Developed exclusively with Government funds" means development was not accomplished exclusively or partially at private expense.*

*(9)* *"Developed with mixed funding" means development was accomplished partially with costs charged to indirect cost pools and/or costs not allocated to a Government contract, and partially with costs charged directly to a Government contract.*

*(10)* *"Government purpose" means any activity in which the United States Government is a party, including cooperative agreements with international or multi-national defense organizations or sales or transfers by the United States Government to foreign Government s or international organizations. Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose computer software or computer software documentation for commercial purposes or authorize others to do so.*

*(11)* *"Government purpose rights" means the rights to—*

*(i)* *Use, modify, reproduce, release, perform, display, or disclose computer software or computer software documentation within the Government without restriction; and*

*(ii)* *Release or disclose computer software or computer software documentation outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose the software or documentation for United States Government purposes.*

*(12)* *"Minor modification" means a modification that does not significantly alter the non-Governmental function or purpose of the software or is of the type customarily provided in the commercial marketplace.*

*(13)* *"Noncommercial computer software" means software that does not qualify as commercial computer software under paragraph (a)(1) of this clause.*

*(14)* *"Restricted rights" apply only to noncommercial computer software and mean the Government's rights to—*

*(i)* *Use a computer program with one computer at one time. The program may not be accessed by more than one terminal or central processing unit or time shared unless otherwise permitted by this contract;*

*(ii)* *Transfer a computer program to another Government agency without the further permission of the Contractor if the transferor destroys all copies of the program and related computer software documentation in its possession and notifies the licensor of the transfer. Transferred programs remain subject to the provisions of this clause;*

*(iii)* *Make the minimum number of copies of the computer software required for safekeeping (archive), backup, or modification purposes;*

*(iv)* *Modify computer software provided that the Government may—*

*(A)* *Use the modified software only as provided in paragraphs (a)(14)(i) and (iii) of this clause; and*

*(B)* *Not release or disclose the modified software except as provided in paragraphs (a)(14)(ii), (v) and (vi) of this clause;*

*(v)* *Permit contractors or subcontractors performing service contracts (see 37.101 of the Federal Acquisition Regulation) in support of this or a related contract to use computer software to diagnose and correct deficiencies in a computer program, to modify computer software to enable a computer program to be combined with, adapted to, or merged with other computer programs or when necessary to respond to urgent tactical situations, provided that—*

*(A)* *The Government notifies the party which has granted restricted rights that a release or disclosure to particular contractors or subcontractors was made;*

*(B)* *Such contractors or subcontractors are subject to the use and non-disclosure agreement at 227.7103-7 of the DFARS or are Government contractors receiving access to the software for performance of a Government contract that contains the clause at DFARS 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends;*

*(C)* *The Government shall not permit the recipient to decompile, disassemble, or reverse engineer the software, or use software decompiled, disassembled, or reverse engineered by the Government pursuant to paragraph (a)(14)(iv) of this clause, for any other purpose; and*

*(D)* *Such use is subject to the limitation in paragraph (a)(14)(i) of this clause; and*

*(vi)* *Permit contractors or subcontractors performing emergency repairs or overhaul of items or components of items procured under this or a related contract to use the computer software when necessary to perform the repairs or overhaul, or to modify the computer software to reflect the repairs or overhaul made, provided that—*

*(A)* *The intended recipient is subject to the use and non-disclosure agreement at DFARS 227.7103-7 or is a Government contractor receiving access to the software for performance of a Government contract that contains the clause at DFARS 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends; and*

*(B) The Government shall not permit the recipient to Decompile, disassemble, or reverse engineer software, or use software decompiled, disassembled, or reverse engineered by the Government pursuant to paragraph (a)(14)(iv) of this clause, for any other purpose.*

*(15) "Unlimited rights" means rights to use, modify, reproduce, release, perform, display, or disclose computer software or computer software documentation in whole or in part, in any manner and for any purpose whatsoever, and to have or authorize others to do so.*

*(b) Rights in computer software or computer software documentation. The Contractor grants or shall obtain for the Government the following royalty free, world-wide, nonexclusive, irrevocable license rights in noncommercial computer software or computer software documentation. All rights not granted to the Government are retained by the Contractor.*

*(1) Unlimited rights. The Government shall have Unlimited rights in—*

*(i) Computer software developed exclusively with Government funds;*

*(ii) Computer software documentation required to be delivered under this contract;*

*(iii) Corrections or changes to computer software or computer software documentation furnished to the Contractor by the Government;*

*(iv) Computer software or computer software documentation that is otherwise publicly available or has been released or disclosed by the Contractor or subcontractor without restriction on further use, release or disclosure, other than a release or disclosure resulting from the sale, transfer, or other assignment of interest in the software to another party or the sale or transfer of some or all of a business entity or its assets to another party;*

*(v) Computer software or computer software documentation obtained with Unlimited rights under another Government contract or as a result of negotiations; or*

*(vi) Computer software or computer software documentation furnished to the Government, under this or any other Government contract or subcontract there under with—*

*(A) Restricted rights in computer software, License to use computer software in technical data, or Government purpose license rights and the restrictive conditions have expired; or*

*(B) Government purpose rights and the Contractor's exclusive right to use such software or documentation for commercial purposes have expired.*

*(2) Government purpose rights.*

*(i) Except as provided in paragraph (b)(1) of this clause, the Government shall have Government purpose rights in computer software developed with mixed funding.*

*(ii) Government purpose rights shall remain in effect for a period of five years unless a different period has been negotiated. Upon expiration of the five-year or other negotiated period, the Government shall have Unlimited rights in the computer software or computer software documentation. The Government purpose rights period shall commence upon execution of the contract, subcontract, letter contract (or similar contractual instrument), contract*

*modification, or option exercise that required development of the computer software.*

(iii) *The Government shall not release or disclose computer software in which it has Government purpose rights to any other person unless—*

(A) *Prior to release or disclosure, the intended recipient is subject to the use and non-disclosure agreement at DFARS 227.7103-7; or*

(B) *The recipient is a Government contractor receiving access to the software or documentation for performance of a Government contract that contains the clause at DFARS 252.227-7025, Limitations on the Use or Disclosure of Government Furnished Information Marked with Restrictive Legends.*

(3) *Restricted rights*

(i) *The Government shall have restricted rights in noncommercial computer software required to be delivered or otherwise provided to the Government under this contract that were developed exclusively at private expense.*

(ii) *The Contractor, its subcontractors, or suppliers are not required to provide the Government additional rights in noncommercial computer software delivered or otherwise provided to the Government with restricted rights. However, if the Government desires to obtain additional rights in such software, the Contractor agrees to promptly enter into negotiations with the Contracting Officer to determine whether there are acceptable terms for transferring such rights. All noncommercial computer software in which the Contractor has granted the Government additional rights shall be listed or described in a license agreement made part of the contract (see paragraph (b)(4) of this clause). The license shall enumerate the additional rights granted the Government.*

(4) *Specifically negotiated license rights.*

(i) *The standard license rights granted to the Government under paragraphs (b)(1) through (b)(3) of this clause, including the period during which the Government shall have Government purpose rights in computer software, may be modified by mutual agreement to provide such rights as the parties consider appropriate but shall not provide the Government lesser rights in computer software than are enumerated in paragraph (a)(14) of this clause or lesser rights in computer software documentation than are enumerated in paragraph (a)(13) of the Rights in Technical Data—Noncommercial Items clause of this contract.*

(ii) *Any rights so negotiated shall be identified in a license agreement made part of this contract.*

(5) *Prior Government rights. Computer software or computer software documentation that will be delivered, furnished, or otherwise provided to the Government under this contract, in which the Government has previously obtained rights shall be delivered, furnished, or provided with the pre-existing rights, unless—*

(i) *The parties have agreed otherwise; or*

(ii) *Any restrictions on the Government's rights to use, modify, reproduce, release, perform, display, or disclose the data have expired or no longer apply.*

(6) *Release from liability. The Contractor agrees to release the Government from liability for any release or disclosure of computer software made in accordance with paragraph (a)(14) or (b)(2)(iii) of this clause, in accordance with the terms of a*

*license negotiated under paragraph (b)(4) of this clause, or by others to whom the recipient has released or disclosed the software, and to seek relief solely from the party who has improperly used, modified, reproduced, released, performed, displayed, or disclosed Contractor software marked with restrictive legends.*

(c) *Rights in derivative computer software or computer software documentation. The Government shall retain its rights in the unchanged portions of any computer software or computer software documentation delivered under this contract that the Contractor uses to prepare, or includes in, derivative computer software or computer software documentation.*

(d) *Third party copyrighted computer software or computer software documentation. The Contractor shall not, without the written approval of the Contracting Officer, incorporate any copyrighted computer software or computer software documentation in the software or documentation to be delivered under this contract unless the Contractor is the copyright owner or has obtained for the Government the license rights necessary to perfect a license or licenses in the deliverable software or documentation of the appropriate scope set forth in paragraph (b) of this clause, and prior to delivery of such—*

(1) *Computer software, has provided a statement of the license rights obtained in a form acceptable to the Contracting Officer; or*

(2) *Computer software documentation, has affixed to the transmittal document a statement of the license rights obtained.*

(e) *Identification and delivery of computer software and computer software documentation to be furnished with restrictions on use, release, or disclosure.*

(1) *This paragraph does not apply to restrictions based solely on copyright.*

(2) *Except as provided in paragraph (e)(3) of this clause, computer software that the Contractor asserts should be furnished to the Government with restrictions on use, release, or disclosure is identified in an attachment to this contract (the Attachment). The Contractor shall not deliver any software with restrictive markings unless the software is listed on the Attachment.*

(3) *In addition to the assertions made in the Attachment, other assertions may be identified after award when based on new information or inadvertent omissions unless the inadvertent omissions would have materially affected the source selection decision. Such identification and assertion shall be submitted to the Contracting Officer as soon as practicable prior to the scheduled date for delivery of the software, in the following format, and signed by an official authorized to contractually obligate the Contractor:*

Identification and Assertion of Restrictions on the Government's Use, Release, or Disclosure of Computer Software.

The Contractor asserts for itself, or the persons identified below, that the Government's rights to use, release, or disclose the following computer software should be restricted:

| Computer Software | | | Name of Person |
|---|---|---|---|
| to be Furnished | Basis for | Asserted Rights | Asserting |
| With Restrictions* | Assertion** | Category*** | Restrictions**** |
| (LIST) | (LIST) | (LIST) | (LIST) |

*Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions on the Government's rights to use, release, or disclose computer software.

**Indicate whether development was exclusively or partially at private expense. If development was not at private expense, enter the specific reason for asserting that the Government's rights should be restricted.

***Enter asserted rights category (e.g., restricted or Government purpose rights in computer software, Government purpose license rights from a prior contract, rights in SBIR software generated under another contract, or specifically negotiated licenses).

****Corporation, individual, or other person, as appropriate.

| | |
|---|---|
| Date | ______________________________ |
| Printed Name and Title | ______________________________ |
| | ______________________________ |
| Signature | ______________________________ |

(End of identification and assertion)

(4) *When requested by the Contracting Officer, the Contractor shall provide sufficient information to enable the Contracting Officer to evaluate the Contractor's assertions. The Contracting Officer reserves the right to add the Contractor's assertions to the Attachment and validate any listed assertion, at a later date, in accordance with the procedures of the Validation of Asserted Restrictions—Computer Software clause of this contract.*

(f) *Marking requirements. The Contractor, and its subcontractors or suppliers, may only assert restrictions on the Government's rights to use, modify, reproduce, release, perform, display, or disclose computer software by marking the deliverable software or documentation subject to restriction. Except as provided in paragraph (f)(5) of this clause, only the following legends are authorized under this contract: the Government purpose rights legend at paragraph (f)(2) of this clause; the restricted rights legend at paragraph (f)(3) of this clause; or the special license rights legend at paragraph (f)(4) of this clause; and/or a notice of copyright as prescribed under 17 U.S.C. 401 or 402.*

(1) *General marking instructions. The Contractor, or its subcontractors or suppliers, shall conspicuously and legibly mark the appropriate legend on all computer software that qualify for such markings. The authorized legends shall be placed on the transmittal document or software storage container and each page, or portions thereof, of printed material containing computer software for which restrictions are asserted. Computer software transmitted directly from one computer or computer terminal to another shall contain a notice of asserted restrictions. However, instructions that interfere with or delay the operation of computer software in order to display a restrictive rights legend or other license statement at any time prior to or during use of the computer software, or otherwise cause such interference or delay, shall not be inserted in software that will or might be used in combat or situations that simulate combat conditions, unless the Contracting Officer's written permission to deliver such software has been obtained prior to delivery. Reproductions of computer software or any portions thereof subject to asserted restrictions, shall also reproduce the asserted restrictions.*

(2) *Government purpose rights markings. Computer software delivered or otherwise furnished to the Government with Government purpose rights shall be marked as follows:*

GOVERNMENT PURPOSE RIGHTS

Contract No.

Contractor Name

Contractor Address

Expiration Date

The Government's rights to use, modify, reproduce, release, perform, display, or disclose this software are restricted by paragraph (b)(2) of the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause contained in the above identified contract. No restrictions apply after the expiration date shown above. Any reproduction of the software or portions thereof marked with this legend must also reproduce the markings.

(End of legend)

(3) *Restricted rights markings. Software delivered or otherwise furnished to the Government with restricted rights shall be marked with the following legend:*

RESTRICTED RIGHTS

Contract No.

Contractor Name

Contractor Address

The Government's rights to use, modify, reproduce, release, perform, display, or disclose this software are restricted by paragraph (b)(3) of the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause contained in the above identified contract. Any reproduction of computer software or portions thereof marked with this legend must also reproduce the markings. Any person, other than the Government, who has been provided access to such software, must promptly notify the above named Contractor.

(End of legend)

*(4) Special license rights markings.*

*(i) Computer software or computer software documentation in which the Government's rights stem from a specifically negotiated license shall be marked with the following legend:*

SPECIAL LICENSE RIGHTS

The Government's rights to use, modify, reproduce, release, perform, display, or disclose these data are restricted by Contract No. _____(Insert contract number)____, License No. ____(Insert license identifier)____. Any reproduction of computer software, computer software documentation, or portions thereof marked with this legend must also reproduce the markings.

(End of legend)

*(ii) For purposes of this clause, special licenses do not include Government purpose license rights acquired under a prior contract (see paragraph (b)(5) of this clause).*

*(5) Pre-existing markings. If the terms of a prior contract or license permitted the Contractor to restrict the Government's rights to use, modify, release, perform, display, or disclose computer software or computer software documentation and those restrictions are still applicable, the Contractor may mark such software or documentation with the appropriate restrictive legend for which the software qualified under the prior contract or license. The marking procedures in paragraph (f)(1) of this clause shall be followed.*

*(g) Contractor procedures and records. Throughout performance of this contract, the Contractor and its subcontractors or suppliers that will deliver computer software or computer software documentation with other than Unlimited rights, shall—*

*(1) Have, maintain, and follow written procedures sufficient to assure that restrictive markings are used only when authorized by the terms of this clause; and*

*(2) Maintain records sufficient to justify the validity of any restrictive markings on computer software or computer software documentation delivered under this contract.*

*(h) Removal of unjustified and nonconforming markings.*

*(1) Unjustified computer software or computer software documentation markings. The rights and obligations of the parties regarding the validation of restrictive markings on computer software or computer software documentation furnished or to be furnished under this contract are contained in the Validation of Asserted Restrictions—Computer Software and the Validation of Restrictive Markings on Technical Data clauses of this contract, respectively. Notwithstanding any provision of this contract concerning inspection and acceptance, the Government may ignore or, at the Contractor's expense, correct or strike a marking if, in accordance with the procedures of those clauses, a restrictive marking is determined to be unjustified.*

*(2) Nonconforming computer software or computer software documentation markings. A nonconforming marking is a marking placed on computer software or computer software documentation delivered or otherwise furnished to the Government under this contract that is not in the format authorized by this contract. Correction of nonconforming markings is not subject to the Validation of Asserted Restrictions—*

*Computer Software or the Validation of Restrictive Markings on Technical Data clause of this contract. If the Contracting Officer notifies the Contractor of a nonconforming marking or markings and the Contractor fails to remove or correct such markings within sixty (60) days, the Government may ignore or, at the Contractor's expense, remove or correct any nonconforming markings.*

*(i) Relation to patents. Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government under any patent.*

*(j) Limitation on charges for rights in computer software or computer software documentation.*

*(1) The Contractor shall not charge to this contract any cost, including but not limited to license fees, royalties, or similar charges, for rights in computer software or computer software documentation to be delivered under this contract when—*

*(i) The Government has acquired, by any means, the same or greater rights in the software or documentation; or*

*(ii) The software or documentation is available to the public without restrictions.*

*(2) The limitation in paragraph (j)(1) of this clause—*

*(iii) Includes costs charged by a subcontractor or supplier, at any tier, or costs incurred by the Contractor to acquire rights in subcontractor or supplier computer software or computer software documentation, if the subcontractor or supplier has been paid for such rights under any other Government contract or under a license conveying the rights to the Government; and*

*(iv) Does not include the reasonable costs of reproducing, handling, or mailing the documents or other media in which the software or documentation will be delivered.*

*(k) Applicability to subcontractors or suppliers.*

*(3) Whenever any noncommercial computer software or computer software documentation is to be obtained from a subcontractor or supplier for delivery to the Government under this contract, the Contractor shall use this same clause in its subcontracts or other contractual instruments, and require its subcontractors or suppliers to do so, without alteration, except to identify the parties. No other clause shall be used to enlarge or diminish the Government's, the Contractor's, or a higher tier subcontractor's or supplier's rights in a subcontractor's or supplier's computer software or computer software documentation.*

*(4) The Contractor and higher tier subcontractors or suppliers shall not use their power to award contracts as economic leverage to obtain rights in computer software or computer software documentation from their subcontractors or suppliers.*

*(5) The Contractor shall ensure that subcontractor or supplier rights are recognized and protected in the identification, assertion, and delivery processes required by paragraph (e) of this clause.*

*(6) In no event shall the Contractor use its obligation to recognize and protect subcontractor or supplier rights in computer software or computer software documentation as an excuse for failing to satisfy its contractual obligation to the Government.*

(End of clause)

*Alternate I (Jun 1995)*

*As prescribed in 227.7203-6(a)(2), add the following paragraph (l) to the basic clause:*

*(l) Publication for sale.*

- *(1) This paragraph only applies to computer software or computer software documentation in which the Government has obtained Unlimited rights or a license to make an unrestricted release of the software or documentation.*
- *(2) The Government shall not publish a deliverable item or items of computer software or computer software documentation identified in this contract as being subject to paragraph (l) of this clause or authorize others to publish such software or documentation on its behalf if, prior to publication for sale by the Government and within twenty-four (24) months following the date specified in this contract for delivery of such software or documentation, or the removal of any national security or export control restrictions, whichever is later, the Contractor publishes that item or items for sale and promptly notifies the Contracting Officer of such publication(s). Any such publication shall include a notice identifying the number of this contract and the Government's rights in the published software or documentation.*
- *(3) This limitation on the Government's right to publish for sale shall continue as long as the software or documentation is reasonably available to the public for purchase.*

GENERAL RECOMMENDATIONS

This clause applies to Computer Software/Documentation. Review the complete text of DFARS 227.72 for:

- Specific uses of 252.227-7014
- Clauses used in conjunction with 252.227-7014.
- Clauses used instead of 252.227-7014

### 3.6.3 Section M - Evaluation

EXAMPLE 1

*In evaluating the Data Rights and Patent Rights, the Government will use information in the proposal to assess the extent to which the rights in technical data (TD), computer software (CS), computer software documentation (CSD), and inventions/patents offered to the Government ensure unimpeded, innovative, and cost effective production, operation, maintenance, and upgrade of the [SYSTEM NAME] throughout its life cycle; allow for open and competitive procurement of [SYSTEM NAME] enhancements; and permit the transfer of the [SYSTEM NAME] non-proprietary object code and source code to other contractors for use on other systems or platforms.*

### 3.6.4 Section L - Instructions to Offerors

### 3.7 Rights in Noncommercial Technical Data and Computer Software—Small Business Innovation Research (SBIR) Program

#### 3.7.1 Section C - SOW/SOO; Requirements

#### 3.7.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7018]

*As prescribed in 227.7104(a), use the following clause:*

Rights In Noncommercial Technical Data And Computer Software—Small Business Innovation Research (SBIR) Program

(Jun 1995)

*(a) Definitions. As used in this clause:*

*(1) "Commercial computer software" means software developed or regularly used for non-Governmental purposes which—*

*(i) Has been sold, leased, or licensed to the public;*

*(ii) Has been offered for sale, lease, or license to the public;*

*(iii) Has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this contract; or*

*(iv) Satisfies a criterion expressed in paragraph (a)(1)(i), (ii), or (iii) of this clause and would require only minor modification to meet the requirements of this contract.*

*(2) "Computer database means a collection of recorded data in a form capable of being processed by a computer. The term does not include computer software.*

*(3) "Computer program" means a set of instructions, rules, or routines, recorded in a form that is capable of causing a computer to perform a specific operation or series of operations.*

*(4) "Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer databases or computer software documentation.*

*(5) "Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.*

*(6) "Detailed manufacturing or process data" means technical data that describe the steps, sequences, and conditions of manufacturing, processing or assembly used by the manufacturer to produce an item or component or to perform a process.*

*(7) "Developed" means—*

*(i) (Applicable to technical data other than computer software documentation.) An item, component, or process, exists and is workable. Thus, the item or component must have been constructed or the process practiced. Workability is generally established when the item, component, or process has been analyzed or tested sufficiently to demonstrate to reasonable people skilled in the applicable art that there is a high probability that it will operate as intended. Whether, how much, and what type of analysis or testing is required to establish workability depends on the nature of the item, component, or process, and the state of the art. To be considered "developed," the item, component, or process need not be at the stage where it could be offered for sale or sold on the commercial market, nor must the item, component or process be actually reduced to practice within the meaning of Title 35 of the United States Code;*

*(ii) A computer program has been successfully operated in a computer and tested to the extent sufficient to demonstrate to reasonable persons skilled in the art that the program can reasonably be expected to perform its intended purpose;*

*(iii) Computer software, other than computer programs, has been tested or analyzed to the extent sufficient to demonstrate to reasonable persons skilled in the art that the software can reasonably be expected to perform its intended purpose; or*

*(iv) Computer software documentation required to be delivered under a contract has been written, in any medium, in sufficient detail to comply with requirements under that contract.*

*(8) "Developed exclusively at private expense" means development was accomplished entirely with costs charged to indirect cost pools, costs not allocated to a Government contract, or any combination thereof.*

*(i) Private expense determinations should be made at the lowest practicable level.*

*(ii) Under fixed-price contracts, when total costs are greater than the firm-fixed-price or ceiling price of the contract, the additional development costs necessary to complete development shall not be considered when determining whether development was at Government , private, or mixed expense.*

*(9) "Developed exclusively with Government funds" means development was not accomplished exclusively or partially at private expense.*

*(10) "Developed with mixed funding" means development was accomplished partially with costs charged to indirect cost pools and/or costs not allocated to a Government contract, and partially with costs charged directly to a Government contract.*

*(11) "Form, fit, and function data" means technical data that describe the required overall physical, functional, and performance characteristics (along with the qualification requirements, if applicable) of an item, component, or process to the extent necessary to permit identification of physically and functionally interchangeable items.*

*(12) "Generated" means technical data or computer software first created in the performance of this contract.*

*(13) "Government purpose" means any activity in which the United States Government is a party, including cooperative agreements with international or multi-national defense organizations or sales or transfers by the United States Government to foreign Governments or international organizations. Government purposes include*

*competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose technical data or computer software for commercial purposes or authorize others to do so.*

(14) *"License to use computer software" means the rights to use, modify, reproduce, release, perform, display, or disclose technical data, in whole or in part, within the Government. The Government may not, without the written permission of the party asserting License to use computer software, release or disclose the technical data outside the Government, use the technical data for manufacture, or permit the technical data to be used by another party, except that the Government may reproduce, release or disclose such data or permit the use or reproduction of the data by persons outside the Government if reproduction, release, disclosure, or use is—*

(i) *Necessary for emergency repair and overhaul; or*

(ii) *A release or disclosure of technical data (other than detailed manufacturing or process data) to, or use of such data by, a foreign Government that is in the interest of the Government and is required for evaluation or informational purposes;*

(iii) *Subject to a prohibition on the further reproduction, release, disclosure, or use of the technical data; and*

(iv) *The Contractor or subcontractor asserting the restriction is notified of such reproduction, release, disclosure, or use.*

(15) *"Minor modification" means a modification that does not significantly alter the non-Governmental function or purpose of computer software or is of the type customarily provided in the commercial marketplace.*

(16) *"Noncommercial computer software" means software that does not qualify as commercial computer software under paragraph (a)(1) of this clause.*

(17) *"Restricted rights" apply only to noncommercial computer software and mean the Government's rights to—*

(i) *Use a computer program with one computer at one time. The program may not be accessed by more than one terminal or central processing unit or time shared unless otherwise permitted by this contract;*

(ii) *Transfer a computer program to another Government agency without the further permission of the Contractor if the transferor destroys all copies of the program and related computer software documentation in its possession and notifies the licensor of the transfer. Transferred programs remain subject to the provisions of this clause;*

(iii) *Make the minimum number of copies of the computer software required for safekeeping (archive), backup, or modification purposes;*

(iv) *Modify computer software provided that the Government may—*

(A) *Use the modified software only as provided in paragraphs (a)(17)(i) and (iii) of this clause; and*

(B) *Not release or disclose the modified software except as provided in paragraphs (a)(17)(ii), (v) and (vi) of this clause;*

(v) *Permit contractors or subcontractors performing service contracts (see 37.101 of the Federal Acquisition Regulation) in support of this or a related contract to* *use computer software to diagnose and correct deficiencies in a computer program, to modify computer software to enable a computer program to be combined with, adapted to, or merged with other computer programs or when necessary to respond to urgent tactical situations, provided that—*

*(A) The Government notifies the party which has granted restricted rights that a release or disclosure to particular contractors or subcontractors was made;*

*(B) Such contractors or subcontractors are subject to the non-disclosure agreement at 227.7103-7 of the DFARS or are Government contractors receiving access to the software for performance of a Government contract that contains the clause at DFARS 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends;*

*(C) The Government shall not permit the recipient to decompile, disassemble, or reverse engineer the software, or use software decompiled, disassembled, or reverse engineered by the Government pursuant to paragraph (a)(17)(iv) of this clause, for any other purpose; and*

*(D) Such use is subject to the limitation in paragraph (a)(17)(i) of this clause; and*

*(vi) Permit contractors or subcontractors performing emergency repairs or overhaul of items or components of items procured under this or a related contract to use the computer software when necessary to perform the repairs or overhaul, or to modify the computer software to reflect the repairs or overhaul made, provided that—*

*(A) The intended recipient is subject to the non-disclosure agreement at DFARS 227.7103-7 or is a Government contractor receiving access to the software for performance of a Government contract that contains the clause at DFARS 252.227-7025, Limitations on the Use or Disclosure of Government Furnished Information Marked with Restrictive Legends; and*

*(B) The Government shall not permit the recipient to decompile, disassemble, or reverse engineer the software, or use software decompiled, disassembled, or reverse engineered by the Government pursuant to paragraph (a)(17)(iv) of this clause, for any other purpose.*

*(18) "SBIR data rights" mean a royalty-free license for the Government, including its support service contractors, to use, modify, reproduce, release, perform, display, or disclose technical data or computer software generated and delivered under this contract for any United States Government purpose.*

*(19) "Technical data" means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information.*

*(20) "Unlimited rights" means rights to use, modify, reproduce, release, perform, display, or disclose, technical data or computer software in whole or in part, in any manner and for any purpose whatsoever, and to have or authorize others to do so.*

(b) *Rights in technical data and computer software. The Contractor grants or shall obtain for the Government the following royalty-free, world-wide, nonexclusive, irrevocable license rights in technical data or noncommercial computer software. All rights not granted to the Government are retained by the Contractor.*

(1) *Unlimited rights. The Government shall have Unlimited rights in technical data, including computer software documentation, or computer software generated under this contract that are—*

(i) *Form, fit, and function data;*

(ii) *Necessary for installation, operation, maintenance, or training purposes (other than detailed manufacturing or process data);*

(iii) *Corrections or changes to Government-furnished technical data or computer software;*

(iv) *Otherwise publicly available or have been released or disclosed by the Contractor or a subcontractor without restrictions on further use, release or disclosure other than a release or disclosure resulting from the sale, transfer, or other assignment of interest in the technical data or computer software to another party or the sale or transfer of some or all of a business entity or its assets to another party;*

(v) *Data or software in which the Government has acquired previously Unlimited rights under another Government contract or through a specific license; and*

(vi) *SBIR data upon expiration of the SBIR data rights period.*

(2) *License to use computer software. The Government shall have License to use computer software in technical data, that were not generated under this contract, pertain to items, components or processes developed exclusively at private expense, and are marked, in accordance with the marking instructions in paragraph (f)(1) of this clause, with the legend prescribed in paragraph (f)(2) of this clause.*

(3) *Restricted rights in computer software. The Government shall have restricted rights in noncommercial computer software required to be delivered or otherwise furnished to the Government under this contract that were developed exclusively at private expense and were not generated under this contract.*

(4) *SBIR data rights.*

(i) *Except for technical data, including computer software documentation, or computer software in which the Government has Unlimited rights under paragraph (b)(1) of this clause, the Government shall have SBIR data rights in all technical data or computer software generated under this contract during the period commencing with contract award and ending upon the date five years after completion of the project from which such data were generated.*

(ii) *The Government may not release or disclose SBIR data to any person, other than its support services contractors, except—*

(A) *As expressly permitted by the Contractor;*

(B) *For evaluational purposes; or*

(C) *A release, disclosure, or use that is necessary for emergency repair or overhaul of items operated by the Government.*

(iii) *A release or disclosure of SBIR data to the Government's support services contractors, or a release or disclosure under paragraph (b)(4)(ii)(B) or (C) of* *this clause, may be made only if, prior to release or disclosure, the intended recipient is subject to the use and non-disclosure agreement at DFARS 227.7103-7 or is a Government contractor receiving access to the technical data or software for performance of a Government contract that contains the clause at DFARS 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends.*

*(5) Specifically negotiated license rights. The standard license rights granted to the Government under paragraphs (b)(1) through (b)(4) of this clause may be modified by mutual agreement to provide such rights as the parties consider appropriate but shall not provide the Government lesser rights in technical data, including computer software documentation, than are enumerated in paragraph (a)(14) of this clause or lesser rights in computer software than are enumerated in paragraph (a)(17) of this clause. Any rights so negotiated shall be identified in a license agreement made part of this contract.*

*(6) Prior Government rights. Technical data, including computer software documentation, or computer software that will be delivered, furnished, or otherwise provided to the Government under this contract, in which the Government has previously obtained rights shall be delivered, furnished, or provided with the pre-existing rights, unless—*

*(i) The parties have agreed otherwise; or*

*(ii) Any restrictions on the Government's rights to use, modify, release, perform, display, or disclose the technical data or computer software have expired or no longer apply.*

*(7) Release from liability. The Contractor agrees to release the Government from liability for any release or disclosure of technical data, computer software, or computer software documentation made in accordance with paragraph (a)(14), (a)(17), or (b)(4) of this clause, or in accordance with the terms of a license negotiated under paragraph (b)(5) of this clause, or by others to whom the recipient has released or disclosed the data, software, or documentation and to seek relief solely from the party who has improperly used, modified, reproduced, released, performed, displayed, or disclosed Contractor data or software marked with restrictive legends.*

*(c) Rights in derivative computer software or computer software documentation. The Government shall retain its rights in the unchanged portions of any computer software or computer software documentation delivered under this contract that the Contractor uses to prepare, or includes in, derivative software or documentation.*

*(d) Third party copyrighted technical data and computer software. The Contractor shall not, without the written approval of the Contracting Officer, incorporate any copyrighted technical data, including computer software documentation, or computer software in the data or software to be delivered under this contract unless the Contractor is the copyright owner or has obtained for the Government the license rights necessary to perfect a license or licenses in the deliverable data or software of the appropriate scope set forth in paragraph (b) of this clause and, prior to delivery of such—*

*(1) Technical data, has affixed to the transmittal document a statement of the license rights obtained; or*

*(2) Computer software, has provided a statement of the license rights obtained in a form acceptable to the Contracting Officer.*

*(e) Identification and delivery of technical data or computer software to be furnished with restrictions on use, release, or disclosure.*

*(1) This paragraph does not apply to technical data or computer software that was or will be generated under this contract or to restrictions based solely on copyright.*

*(2) Except as provided in paragraph (e)(3) of this clause, technical data or computer software that the Contractor asserts should be furnished to the Government with restrictions on use, release, or disclosure is identified in an attachment to this contract (the Attachment). The Contractor shall not deliver any technical data or computer software with restrictive markings unless the technical data or computer software is listed on the Attachment.*

*(3) In addition to the assertions made in the Attachment, other assertions may be identified after award when based on new information or inadvertent omissions unless the inadvertent omissions would have materially affected the source selection decision. Such identification and assertion shall be submitted to the Contracting Officer as soon as practicable prior to the scheduled date for delivery of the technical data or computer software, in the following format, and signed by an official authorized to contractually obligate the Contractor:*

Identification and Assertion of Restrictions on the Government's Use, Release, or Disclosure of Technical Data or Computer Software.

| **The Contractor asserts for itself, or the persons identified below, that the Government's rights to use, release, or disclose the following technical data or computer software should be restricted: Technical Data or Computer Software to be Furnished With Restrictions*** | **Basis for Assertion**** | **Asserted Rights Category***** | **Name of Person Asserting Restrictions****** |
|---|---|---|---|
| (LIST) | (LIST) | (LIST) | (LIST) |

*If the assertion is applicable to items, components, or processes developed at private expense, identify both the technical data and each such item, component, or process.

**Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions on the Government's rights to use, release, or disclose technical data or computer software. Indicate whether development was exclusively or partially at private expense. If development was not at private expense, enter the specific reason for asserting that the Government's rights should be restricted.

***Enter asserted rights category (e.g., License to use computer software, restricted rights, Government purpose rights, or Government purpose license rights from a prior contract, SBIR data rights under another contract, or specifically negotiated licenses).

****Corporation, individual, or other person, as appropriate.

| | |
|---|---|
| Date | _______________________________ |
| Printed Name and Title | _______________________________ |
| | _______________________________ |
| Signature | _______________________________ |

(End of identification and assertion)

(4) *When requested by the Contracting Officer, the Contractor shall provide sufficient information to enable the Contracting Officer to evaluate the Contractor's assertions. The Contracting Officer reserves the right to add the Contractor's assertions to the Attachment and validate any listed assertions, at a later date, in accordance with the procedures of the Validation of Asserted Restrictions—Computer Software and/or Validation of Restrictive Markings on Technical Data clauses of this contract.*

(f) *Marking requirements. The Contractor, and its subcontractors or suppliers, may only assert restrictions on the Government's rights to use, modify, reproduce, release, perform, display, or disclose technical data or computer software to be delivered under this contract by marking the deliverable data or software subject to restriction. Except as provided in paragraph (f)(6) of this clause, only the following markings are authorized under this contract: the License to use computer software legend at paragraph (f)(2) of this clause; the restricted rights legend at paragraph (f)(3) of this clause, the SBIR data rights legend at paragraph (f)(4) of this clause, or the special license rights legend at paragraph (f)(5) of this clause; and/or a notice of copyright as prescribed under 17 U.S.C. 401 or 402.*

(1) *General marking instructions. The Contractor, or its subcontractors or suppliers, shall conspicuously and legibly mark the appropriate legend to all technical data and computer software that qualify for such markings. The authorized legends shall be placed on the transmittal document or storage container and, for printed material, each page of the printed material containing technical data or computer software for which restrictions are asserted. When only portions of a page of printed material are subject to the asserted restrictions, such portions shall be identified by circling, underscoring, with a note, or other appropriate identifier. Technical data or computer software transmitted directly from one computer or computer terminal to another shall contain a notice of asserted restrictions. However, instructions that interfere with or delay the operation of computer software in order to display a restrictive rights legend or other license statement at any time prior to or during use of the computer software, or otherwise cause such interference or delay, shall not be inserted in software that will or might be used in combat or situations that simulate combat conditions, unless the Contracting Officer's written permission to deliver such software has been obtained prior to delivery. Reproductions of technical data, computer software, or any portions thereof subject to asserted restrictions shall also reproduce the asserted restrictions.*

(2) *License to use computer software markings. Technical data not generated under this contract that pertain to items, components, or processes developed exclusively at private expense and delivered or otherwise furnished with License to use computer software shall be marked with the following legend:*

LICENSE TO USE COMPUTER SOFTWARE

Contract No. ______________________________

Contractor Name ______________________________

Contractor Address ______________________________

______________________________

The Government's rights to use, modify, reproduce, release, perform, display, or disclose these technical data are restricted by paragraph (b)(2) of the Rights in Noncommercial Technical Data and Computer Software—Small Business Innovative Research (SBIR) Program clause contained in the above identified contract. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings. Any person, other than the Government, who has been provided access to such data must promptly notify the above named Contractor.

(End of legend)

(3) *Restricted rights markings. Computer software delivered or otherwise furnished to the Government with restricted rights shall be marked with the following legend:*

RESTRICTED RIGHTS

Contract No. ______________________________

Contractor Name ______________________________

Contractor Address ______________________________

______________________________

The Government's rights to use, modify, reproduce, release, perform, display, or disclose this software are restricted by paragraph (b)(3) of the Rights in Noncommercial Technical Data and Computer Software—Small Business Innovative Research (SBIR) Program clause contained in the above identified contract. Any reproduction of computer software or portions thereof marked with this legend must also reproduce the markings. Any person, other than the Government, who has been provided access to such software must promptly notify the above named Contractor.

*(End of legend)*

(4) *SBIR data rights markings. Except for technical data or computer software in which the Government has acquired Unlimited rights under paragraph (b)(1) of this clause, or negotiated special license rights as provided in paragraph (b)(5) of this clause, technical data or computer software generated under this contract shall be marked with the following legend. The Contractor shall enter the expiration date for the SBIR data rights period on the legend:*

*SBIR DATA RIGHTS*

Contract No. ________________________

Contractor Name ________________________

Contractor Address ________________________

______________________________________

Expiration of SBIR Data Rights Period ____________

The Government's rights to use, modify, reproduce, release, perform, display, or disclose technical data or computer software marked with this legend are restricted during the period shown as provided in paragraph (b)(4) of the Rights in Noncommercial Technical Data and Computer Software—Small Business Innovative Research (SBIR) Program clause contained in the above identified contract. No restrictions apply after the expiration date shown above. Any reproduction of technical data, computer software, or portions thereof marked with this legend must also reproduce the markings.

(End of legend)

*(5) Special license rights markings.*

*(i) Technical data or computer software in which the Government's rights stem from a specifically negotiated license shall be marked with the following legend:*

SPECIAL LICENSE RIGHTS

The Government's rights to use, modify, reproduce, release, perform, display, or disclose this technical data or computer software are restricted by Contract No. _____(Insert contract number)____, License No. ____(Insert license identifier)____. Any reproduction of technical data, computer software, or portions thereof marked with this legend must also reproduce the markings.

(End of legend)

*(ii) For purposes of this clause, special licenses do not include Government purpose license rights acquired under a prior contract (see paragraph (b)(6) of this clause).*

*(6) Pre-existing data markings. If the terms of a prior contract or license permitted the Contractor to restrict the Government's rights to use, modify, reproduce, release, perform, display, or disclose technical data or computer software, and those restrictions are still applicable, the Contractor may mark such data or software with the appropriate restrictive legend for which the data or software qualified under the prior contract or license. The marking procedures in paragraph (f)(1) of this clause shall be followed.*

*(g) Contractor procedures and records. Throughout performance of this contract, the Contractor, and its subcontractors or suppliers that will deliver technical data or computer software with other than Unlimited rights, shall—*

*(1) Have, maintain, and follow written procedures sufficient to assure that restrictive markings are used only when authorized by the terms of this clause; and*

*(2) Maintain records sufficient to justify the validity of any restrictive markings on technical data or computer software delivered under this contract.*

*(h) Removal of unjustified and nonconforming markings.*

*(1) Unjustified markings. The rights and obligations of the parties regarding the validation of restrictive markings on technical data or computer software furnished or to be furnished under this contract are contained in the Validation of Restrictive Markings on Technical Data and the Validation of Asserted Restrictions—Computer Software clauses of this contract, respectively. Notwithstanding any provision of this contract concerning inspection and acceptance, the Government may ignore or, at the Contractor's expense, correct or strike a marking if, in accordance with the applicable procedures of those clauses, a restrictive marking is determined to be unjustified.*

*(2) Nonconforming markings. A nonconforming marking is a marking placed on technical data or computer software delivered or otherwise furnished to the Government under this contract that is not in the format authorized by this contract. Correction of nonconforming markings is not subject to the Validation of Restrictive Markings on Technical Data or the Validation of Asserted Restrictions—Computer Software clause of this contract. If the Contracting Officer notifies the Contractor of a nonconforming marking or markings and the Contractor fails to remove or correct such markings within sixty (60) days, the Government may ignore or, at the Contractor's expense, remove or correct any nonconforming markings.*

*(i) Relation to patents. Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government under any patent.*

*(j) Limitation on charges for rights in technical data or computer software.*

*(1) The Contractor shall not charge to this contract any cost, including but not limited to, license fees, royalties, or similar charges, for rights in technical data or computer software to be delivered under this contract when—*

*(i) The Government has acquired, by any means, the same or greater rights in the data or software; or*

*(ii) The data are available to the public without restrictions.*

*(2) The limitation in paragraph (j)(1) of this clause—*

*(i) Includes costs charged by a subcontractor or supplier, at any tier, or costs incurred by the Contractor to acquire rights in subcontractor or supplier technical data or computer software, if the subcontractor or supplier has been paid for such rights under any other Government contract or under a license conveying the rights to the Government; and*

*(ii) Does not include the reasonable costs of reproducing, handling, or mailing the documents or other media in which the technical data or computer software will be delivered.*

*(k) Applicability to subcontractors or suppliers.*

*(1) The Contractor shall assure that the rights afforded its subcontractors and suppliers under 10 U.S.C. 2320, 10 U.S.C. 2321, and the identification, assertion, and delivery processes required by paragraph (e) of this clause are recognized and protected.*

*(2) Whenever any noncommercial technical data or computer software is to be obtained from a subcontractor or supplier for delivery to the Government under this contract, the Contractor shall use this same clause in the subcontract or other contractual instrument, and require its subcontractors or suppliers to do so, without alteration, except to identify the parties. The Contractor shall use the Technical Data—Commercial Items clause of this contract to obtain technical data pertaining to commercial items, components, or processes. No other clause shall be used to enlarge or diminish the Government's, the Contractor's, or a higher tier subcontractor's or supplier's rights in a subcontractor's or supplier's technical data or computer software.*

*(3) Technical data required to be delivered by a subcontractor or supplier shall normally be delivered to the next higher tier contractor, subcontractor, or supplier. However, when there is a requirement in the prime contract for technical data which may be submitted with other than Unlimited rights by a subcontractor or supplier, then said subcontractor or supplier may fulfill its requirement by submitting such technical data directly to the Government, rather than through a higher tier contractor, subcontractor, or supplier.*

*(4) The Contractor and higher tier subcontractors or suppliers shall not use their power to award contracts as economic leverage to obtain rights in technical data or computer software from their subcontractors or suppliers.*

*(5) In no event shall the Contractor use its obligation to recognize and protect subcontractor or supplier rights in technical data or computer software as an excuse for failing to satisfy its contractual obligation to the Government.*

(End of clause)

*Alternate I (Jun 1995)*

*As prescribed in 227.7104(d), add the following paragraph (l) to the basic clause:*

*(l) Publication for sale.*

*(1) This paragraph applies only to technical data or computer software delivered to the Government with SBIR data rights.*

*(2) Upon expiration of the SBIR data rights period, the Government will not exercise its right to publish or authorize others to publish an item of technical data or computer software identified in this contract as being subject to paragraph (l) of this clause if the Contractor, prior to the expiration of the SBIR data rights period, or within two years following delivery of the data or software item, or within twenty-four months following the removal of any national security or export control restrictions, whichever is later, publishes such data or software item(s) and promptly notifies the Contracting Officer of such publication(s). Any such publication(s) shall include a notice identifying the number of this contract and the Government's rights in the published data.*

*(3) This limitation on the Government's right to publish for sale shall continue as long as the technical data or computer software are reasonably available to the public for purchase.*

GENERAL RECOMMENDATIONS

This clause applies to both Technical Data and Computer Software/Documentation. Review the complete text of DFARS 227.71 and 227.72 for:

- Specific uses of 252.227-7018
- Clauses used in conjunction with 252.227-7018.
- Clauses used instead of 252.227-7018

### 3.7.3 Section M - Evaluation

### 3.7.4 Section L - Instructions to Offerors

## 3.8 Rights in Special Works

### 3.8.1 Section C - SOW/SOO; Requirements

### 3.8.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7020]

*As prescribed in 227.7105-3, 227.7106(a) or 227.7205(a), use the following clause:*

Rights In Special Works (Jun 1995)

*(a) Applicability. This clause applies to works first created, generated, or produced and required to be delivered under this contract.*

*(b) Definitions. As used in this clause:*

*(1) "Computer data base" means a collection of data recorded in a form capable of being processed by a computer. The term does not include computer software.*

*(2) "Computer program" means a set of instructions, rules, or routines recorded in a form that is capable of causing a computer to perform a specific operation or series of operations.*

*(3) "Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer data bases or computer software documentation.*

*(4) "Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.*

*(5) "License to use computer software " means the rights to use, modify, reproduce, perform, display, release, or disclose a work in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so.*

*(6) The term "works" includes computer data bases, computer software, or computer software documentation; literary, musical, choreographic, or dramatic compositions; pantomimes; pictorial, graphic, or sculptural compositions; motion pictures and other audiovisual compositions; sound recordings in any medium; or, items of similar nature.*

*(c) License rights.*

*(1) The Government shall have Unlimited rights in works first produced, created, or generated and required to be delivered under this contract.*

*(2) When a work is first produced, created, or generated under this contract, and such work is required to be delivered under this contract, the Contractor shall assign copyright in those works to the Government. The Contractor, unless directed to the contrary by the Contracting Officer, shall place the following notice on such works:*

*"© (Year date of delivery) United States Government, as represented by the Secretary of (department). All rights reserved."*

(3) *The Contractor grants to the Government a royalty-free, world-wide, nonexclusive, irrevocable license to reproduce, prepare derivative works from, distribute, perform, or display, and to have or authorize others to do so, the Contractor's copyrighted works not first produced, created, or generated under this contract that have been incorporated into the works deliverable under this contract.*

(d) *Third party copyrighted data. The Contractor shall not incorporate, without the written approval of the Contracting Officer, any copyrighted works in the works to be delivered under this contract unless the Contractor is the copyright owner or has obtained for the Government the license rights necessary to perfect a license of the scope identified in paragraph (c)(3) of this clause and, prior to delivery of such works—*

(1) *Has affixed to the transmittal document a statement of the license rights obtained; or*

(2) *For computer software, has provided a statement of the license rights obtained in a form acceptable to the Contracting Officer.*

(e) *Indemnification. The Contractor shall indemnify and save and hold harmless the Government, and its officers, agents and employees acting for the Government, against any liability, including costs and expenses, (1) for violation of proprietary rights, copyrights, or rights of privacy or publicity, arising out of the creation, delivery, use, modification, reproduction, release, performance, display, or disclosure of any works furnished under this contract, or (2) based upon any libelous or other unlawful matter contained in such works.*

(f) *Government-furnished information (GFI). Paragraphs (d) and (e) of this clause are not applicable to information furnished to the Contractor by the Government and incorporated in the works delivered under this contract.*

(End of clause)

GENERAL RECOMMENDATIONS

This clause applies to both Technical Data and Computer Software/Documentation. Review the complete text of DFARS 227.71 and 227.72 for:

- Specific uses of 252.227-7020
- Clauses used in conjunction with 252.227-7020
- Clauses used instead of 252.227-7020

### 3.8.3 Section M - Evaluation

### 3.8.4 Section L - Instructions to Offerors

## 3.9 Rights in Technical Data and Computer Software (Foreign)

### 3.9.1 Section C - SOW/SOO; Requirements

### 3.9.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7032]

As prescribed in 227.7103-17, use the following clause:

Rights In Technical Data And Computer Software (Foreign)

(Jun 1975)

*The United States Government may duplicate, use, and disclose in any manner for any purposes whatsoever, including delivery to other Government s for the furtherance of mutual defense of the United States Government and other Government s, all technical data including reports, drawings and blueprints, and all computer software, specified to be delivered by the Contractor to the United States Government under this contract.*

(End of clause)

GENERAL RECOMMENDATIONS

This clause applies to both Technical Data and Computer Software/Documentation. Review the complete text of DFARS 227.71and 272.72 for:

- Specific uses of 252.227-7032
- Clauses used in conjunction with 252.227-7032 .
- Clauses used instead of 252.227-7032

### 3.9.3 Section M - Evaluation

### 3.9.4 Section L - Instructions to Offerors

## 3.10 Technical Data or Computer Software Previously Delivered to the Government.

### 3.10.1 Section C - SOW/SOO; Requirements

### 3.10.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7028]

As prescribed in 227.7103-6(d), 227.7104(f)(2), or 227.7203-6(e), use the following provision:

Technical Data Or Computer Software Previously Delivered To The Government

(Jun 1995)

*The Offeror shall attach to its offer an identification of all documents or other media incorporating technical data or computer software it intends to deliver under this contract with other than Unlimited rights that are identical or substantially similar to documents or other media that the Offeror has produced for, delivered to, or is obligated to deliver to the Government under any contract or subcontract. The attachment shall identify—*

*(a) The contract number under which the data or software were produced;*

*(b) The contract number under which, and the name and address of the organization to whom, the data or software were most recently delivered or will be delivered; and*

*(c) Any limitations on the Government's rights to use or disclose the data or software, including, when applicable, identification of the earliest date the limitations expire.*

GENERAL RECOMMENDATIONS

Review the complete text of DFARS 227.71 and 227.72 for:

- Specific uses of 252.227-7028
- Clauses used in conjunction with 252.227-7028
- Clauses used instead of 252.227-7028

### 3.10.3 Section M - Evaluation

### 3.10.4 Section L - Instructions to Offerors

## 3.11 Third Party Development

### 3.11.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Contractor shall address how it will provide to the Government information needed to support third-party development and delivery of competitive alternatives of designs for software or other components or modules on an ongoing basis. The Contractor shall provide a list of those proprietary, vendor-unique elements that it requests be exempt from this review* [USN 2007a].

### 3.11.2 Section I - Contract Clauses

### 3.11.3 Section M - Evaluation

### 3.11.4 Section L - Instructions to Offerors

## 3.12 Validation of Asserted Restrictions - Computer Software

### 3.12.1 Section C - SOW/SOO; Requirements

### 3.12.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7019]

*As prescribed in 227.7104(e)(3) or 227.7203-6(c), use the following clause:*

*Validation Of Asserted Restrictions—Computer Software*

*(Jun 1995)*

*(a) Definitions.*

*(1) As used in this clause, unless otherwise specifically indicated, the term "Contractor" means the Contractor and its subcontractors or suppliers.*

*(2) Other terms used in this clause are defined in the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause of this contract.*

*(b) Justification. The Contractor shall maintain records sufficient to justify the validity of any markings that assert restrictions on the Government's rights to use, modify, reproduce, perform, display, release, or disclose computer software delivered or required to be delivered under this contract and shall be prepared to furnish to the Contracting Officer a written justification for such restrictive markings in response to a request for information under paragraph (d) or a challenge under paragraph (f) of this clause.*

*(c) Direct contact with subcontractors or suppliers. The Contractor agrees that the Contracting Officer may transact matters under this clause directly with subcontractors or suppliers at any tier who assert restrictions on the Government's right to use, modify, reproduce, release, perform, display, or disclose computer software. Neither this clause, nor any action taken by the Government under this clause, creates or implies privity of contract between the Government and the Contractor's subcontractors or suppliers.*

*(d) Requests for information.*

*(1) The Contracting Officer may request the Contractor to provide sufficient information to enable the Contracting Officer to evaluate the Contractor's asserted restrictions. Such information shall be based upon the records required by this clause or other information reasonably available to the Contractor.*

*(2) Based upon the information provided, if the—*

*(i) Contractor agrees that an asserted restriction is not valid, the Contracting Officer may—*

*(A) Strike or correct the unjustified marking at the Contractor's expense; or*

*(B) Return the computer software to the Contractor for correction at the Contractor's expense. If the Contractor fails to correct or strike the unjustified restriction and return the corrected software to the Contracting Officer within sixty (60) days following receipt of the*

*software, the Contracting Officer may correct or strike the markings at that Contractor's expense.*

*(ii) Contracting Officer concludes that the asserted restriction is appropriate for this contract, the Contracting Officer shall so notify the Contractor in writing.*

*(3) The Contractor's failure to provide a timely response to a Contracting Officer's request for information or failure to provide sufficient information to enable the Contracting Officer to evaluate an asserted restriction shall constitute reasonable grounds for questioning the validity of an asserted restriction.*

*(e) Government right to challenge and validate asserted restrictions.*

*(1) The Government, when there are reasonable grounds to do so, has the right to review and challenge the validity of any restrictions asserted by the Contractor on the Government's rights to use, modify, reproduce, release, perform, display, or disclose computer software delivered, to be delivered under this contract, or otherwise provided to the Government in the performance of this contract. Except for software that is publicly available, has been furnished to the Government without restrictions, or has been otherwise made available without restrictions, the Government may exercise this right only within three years after the date(s) the software is delivered or otherwise furnished to the Government, or three years following final payment under this contract, whichever is later.*

*(2) The absence of a challenge to an asserted restriction shall not constitute validation under this clause. Only a Contracting Officer's final decision or actions of an agency Board of Contract Appeals or a court of competent jurisdiction that sustain the validity of an asserted restriction constitute validation of the restriction.*

*(f) Challenge procedures.*

*(1) A challenge must be in writing and shall—*

*(i) State the specific grounds for challenging the asserted restriction;*

*(ii) Require the Contractor to respond within sixty (60) days;*

*(iii) Require the Contractor to provide justification for the assertion based upon records kept in accordance with paragraph (b) of this clause and such other documentation that are reasonably available to the Contractor, in sufficient detail to enable the Contracting Officer to determine the validity of the asserted restrictions; and*

*(iv) State that a Contracting Officer's final decision, during the three-year period preceding this challenge, or action of a court of competent jurisdiction or Board of Contract Appeals that sustained the validity of an identical assertion made by the Contractor (or a licensee) shall serve as justification for the asserted restriction.*

*(2) The Contracting Officer shall extend the time for response if the Contractor submits a written request showing the need for additional time to prepare a response.*

*(3) The Contracting Officer may request additional supporting documentation if, in the Contracting Officer’s opinion, the Contractor's explanation does not provide sufficient evidence to justify the validity of the asserted restrictions. The Contractor agrees to promptly respond to the Contracting Officer's request for additional supporting documentation.*

(4) *Notwithstanding challenge by the Contracting Officer, the parties may agree on the disposition of an asserted restriction at any time prior to a Contracting Officer's final decision or, if the Contractor has appealed that decision, filed suit, or provided notice of an intent to file suit, at any time prior to a decision by a court of competent jurisdiction or Board of Contract Appeals.*

(5) *If the Contractor fails to respond to the Contracting Officer's request for information or additional information under paragraph (f)(1) of this clause, the Contracting Officer shall issue a final decision, in accordance with the Disputes clause of this contract, pertaining to the validity of the asserted restriction.*

(6) *If the Contracting Officer, after reviewing the written explanation furnished pursuant to paragraph (f)(1) of this clause, or any other available information pertaining to the validity of an asserted restriction, determines that the asserted restriction has—*

(i) *Not been justified, the Contracting Officer shall issue promptly a final decision, in accordance with the Disputes clause of this contract, denying the validity of the asserted restriction; or*

(ii) *Been justified, the Contracting Officer shall issue promptly a final decision, in accordance with the Disputes clause of this contract, validating the asserted restriction.*

(7) *A Contractor receiving challenges to the same asserted restriction(s) from more than one Contracting Officer shall notify each Contracting Officer of the other challenges. The notice shall also state which Contracting Officer initiated the first in time unanswered challenge. The Contracting Officer who initiated the first in time unanswered challenge, after consultation with the other Contracting Officers who have challenged the restrictions and the Contractor, shall formulate and distribute a schedule that provides the Contractor a reasonable opportunity for responding to each challenge.*

(g) *Contractor appeal* - *Government obligation.*

(1) *The Government agrees that, notwithstanding a Contracting Officer's final decision denying the validity of an asserted restriction and except as provided in paragraph (g)(3) of this clause, it will honor the asserted restriction—*

(i) *For a period of ninety (90) days from the date of the Contracting Officer's final decision to allow the Contractor to appeal to the appropriate Board of Contract Appeals or to file suit in an appropriate court;*

(ii) *For a period of one year from the date of the Contracting Officer's final decision if, within the first ninety (90) days following the Contracting Officer's final decision, the Contractor has provided notice of an intent to file suit in an appropriate court; or*

(iii) *Until final disposition by the appropriate Board of Contract Appeals or court of competent jurisdiction, if the Contractor has:*

(A) *appealed to the Board of Contract Appeals or filed suit an appropriate court within ninety (90) days; or*

(B) *submitted, within ninety (90) days, a notice of intent to file suit in an appropriate court and filed suit within one year.*

(2) *The Contractor agrees that the Government may strike, correct, or ignore the restrictive markings if the Contractor fails to—*

*(i) Appeal to a Board of Contract Appeals within ninety (90) days from the date of the Contracting Officer's final decision;*

*(ii) File suit in an appropriate court within ninety (90) days from such date; or*

*(iii) File suit within one year after the date of the Contracting Officer's final decision if the Contractor had provided notice of intent to file suit within ninety (90) days following the date of the Contracting Officer's final decision.*

*(3) The agency head, on a nondelegable basis, may determine that urgent or compelling circumstances do not permit awaiting the filing of suit in an appropriate court, or the rendering of a decision by a court of competent jurisdiction or Board of Contract Appeals. In that event, the agency head shall notify the Contractor of the urgent or compelling circumstances. Notwithstanding paragraph (g)(1) of this clause, the Contractor agrees that the agency may use, modify, reproduce, release, perform, display, or disclose computer software marked with (i) Government purpose legends for any purpose, and authorize others to do so; or (ii) restricted or special license rights for Government purposes only. The Government agrees not to release or disclose such software unless, prior to release or disclosure, the intended recipient is subject to the use and non-disclosure agreement at 227.7103-7 of DFARS, or is a Government contractor receiving access to the software for performance of a Government contract that contains the clause at DFARS 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends. The agency head's determination may be made at any time after the date of the Contracting Officer's final decision and shall not affect the Contractor's right to damages against the United States, or other relief provided by law, if its asserted restrictions are ultimately upheld.*

*(h) Final disposition of appeal or suit. If the Contractor appeals or files suit and if, upon final disposition of the appeal or suit, the Contracting Officer's decision is:*

*(1) Sustained—*

*(i) Any restrictive marking on such computer software shall be struck or corrected at the Contractor's expense or ignored; and*

*(ii) If the asserted restriction is found not to be substantially justified, the Contractor shall be liable to the Government for payment of the cost to the Government of reviewing the asserted restriction and the fees and other expenses (as defined in 28 U.S.C. 2412(d)(2)(A)) incurred by the Government in challenging the restriction, unless special circumstances would make such payment unjust.*

*(2) Not sustained—*

*(i) The Government shall be bound by the asserted restriction; and*

*(ii) If the challenge by the Government is found not to have been made in good faith, the Government shall be liable to the Contractor for payment of fees and other expenses (as defined in 28 U.S.C. 2412(d)(2)(A)) incurred by the Contractor in defending the restriction.*

*(i) Flowdown. The Contractor shall insert this clause in all contracts, purchase orders, and other similar instruments with its subcontractors or suppliers, at any tier, who will be furnishing computer software to the Government in the performance of this contract. The clause may not be altered other than to identify the appropriate parties.*

(End of clause)

GENERAL RECOMMENDATIONS

This clause applies to both Technical Data and Computer Software/Documentation. Review the complete text of DFARS 227.71 and 227.72 for:

- Specific uses of 252.227-7019
- Clauses used in conjunction with 252.227-7019.
- Clauses used instead of 252.227-7019

### 3.12.3 Section M - Evaluation

### 3.12.4 Section L - Instructions to Offerors

### 3.13 Validation of Restrictive Markings on Technical Data

#### 3.13.1 Section C - SOW/SOO; Requirements

#### 3.13.2 Section I - Contract Clauses

EXAMPLE 1

[DFARS 252.227-7037]

*As prescribed in 227.7102-3(c), 227.7103-6(e)(3), 227.7104(e)(5), or 227.7203-6(f), use the following clause:*

*VALIDATION OF RESTRICTIVE MARKINGS ON TECHNICAL DATA (1999)*

*(a) Definitions. The terms used in this clause are defined in the Rights in Technical Data—Noncommercial Items clause of this contract.*

*(b) Contracts for commercial items—presumption of development at private expense. Under a contract for a commercial item, component, or process, the Department of Defense shall presume that a Contractor's asserted use or release restrictions are justified on the basis that the item, component, or process was developed exclusively at private expense. The Department shall not challenge such assertions unless information the Department provides demonstrates that the item, component, or process was not developed exclusively at private expense.*

*(c) Justification. The Contractor or subcontractor at any tier is responsible for maintaining records sufficient to justify the validity of its markings that impose restrictions on the Government and others to use, duplicate, or disclose technical data delivered or required to be delivered under the contract or subcontract. Except under contracts for commercial items, the Contractor or subcontractor shall be prepared to furnish to the Contracting Officer a written justification for such restrictive markings in response to a challenge under paragraph (e) of this clause.*

*(d) Pre-challenge request for information.*

*(1) The Contracting Officer may request the Contractor or subcontractor to furnish a written explanation for any restriction asserted by the Contractor or subcontractor on the right of the United States or others to use technical data. If, upon review of the explanation submitted, the Contracting Officer remains unable to ascertain the basis of the restrictive marking, the Contracting Officer may further request the Contractor or subcontractor to furnish additional information in the records of, or otherwise in the possession of or reasonably available to, the Contractor or subcontractor to justify the validity of any restrictive marking on technical data delivered or to be delivered under the contract or subcontract (e.g., a statement of facts accompanied with supporting documentation). The Contractor or subcontractor shall submit such written data as requested by the Contracting Officer within the time required or such longer period as may be mutually agreed.*

*(2) If the Contracting Officer, after reviewing the written data furnished pursuant to paragraph (d)(1) of this clause, or any other available information pertaining to the validity of a restrictive marking, determines that reasonable grounds exist to question the current validity of the marking and that continued adherence to the marking would make impracticable the subsequent competitive acquisition of the*

*item, component, or process to which the technical data relates, the Contracting Officer shall follow the procedures in paragraph (e) of this clause.*

(3) *If the Contractor or subcontractor fails to respond to the Contracting Officer's request for information under paragraph (d)(1) of this clause, and the Contracting Officer determines that continued adherence to the marking would make impracticable the subsequent competitive acquisition of the item, component, or process to which the technical data relates, the Contracting Officer may challenge the validity of the marking as described in paragraph (e) of this clause.*

(e) *Challenge.*

(1) *Notwithstanding any provision of this contract concerning inspection and acceptance, if the Contracting Officer determines that a challenge to the restrictive marking is warranted, the Contracting Officer shall send a written challenge notice to the Contractor or subcontractor asserting the restrictive markings. Such challenge shall—*

(i) *State the specific grounds for challenging the asserted restriction;*

(ii) *Require a response within sixty (60) days justifying and providing sufficient evidence as to the current validity of the asserted restriction;*

(iii) *State that a DoD Contracting Officer's final decision, issued pursuant to paragraph (g) of this clause, sustaining the validity of a restrictive marking identical to the asserted restriction, within the three-year period preceding the challenge, shall serve as justification for the asserted restriction if the validated restriction was asserted by the same Contractor or subcontractor (or any licensee of such Contractor or subcontractor) to which such notice is being provided; and*

(iv) *State that failure to respond to the challenge notice may result in issuance of a final decision pursuant to paragraph (f) of this clause.*

(2) *The Contracting Officer shall extend the time for response as appropriate if the Contractor or subcontractor submits a written request showing the need for additional time to prepare a response.*

(3) *The Contractor's or subcontractor's written response shall be considered a claim within the meaning of the Contract Disputes Act of 1978 (41 U.S.C. 601, et seq.), and shall be certified in the form prescribed at 33.207 of the Federal Acquisition Regulation, regardless of dollar amount.*

(4) *A Contractor or subcontractor receiving challenges to the same restrictive markings from more than one Contracting Officer shall notify each Contracting Officer of the existence of more than one challenge. The notice shall also state which Contracting Officer initiated the first in time unanswered challenge. The Contracting Officer initiating the first in time unanswered challenge after consultation with the Contractor or subcontractor and the other Contracting Officers, shall formulate and distribute a schedule for responding to each of the challenge notices to all interested parties. The schedule shall afford the Contractor or subcontractor an opportunity to respond to each challenge notice. All parties will be bound by this schedule.*

(f) *Final decision when Contractor or subcontractor fails to respond. Upon a failure of a Contractor or subcontractor to submit any response to the challenge notice, other than a failure to respond under a contract for commercial items, the Contracting Officer will issue a final decision to the Contractor or subcontractor in accordance with the Disputes clause of* *this contract pertaining to the validity of the asserted restriction. This final decision shall be issued as soon as possible after the expiration of the time period of paragraph (e)(1)(ii) or (e)(2) of this clause. Following issuance of the final decision, the Contracting Officer will comply with the procedures in paragraphs (g)(2)(ii) through (iv) of this clause.*

*(g) Final decision when Contractor or subcontractor responds.*

*(1) If the Contracting Officer determines that the Contractor or subcontractor has justified the validity of the restrictive marking, the Contracting Officer shall issue a final decision to the Contractor or subcontractor sustaining the validity of the restrictive marking, and stating that the Government will continue to be bound by the restrictive marking. This final decision shall be issued within sixty (60) days after receipt of the Contractor's or subcontractor's response to the challenge notice, or within such longer period that the Contracting Officer has notified the Contractor or subcontractor that the Government will require. The notification of a longer period for issuance of a final decision will be made within sixty (60) days after receipt of the response to the challenge notice.*

*(2)*

*(i) If the Contracting Officer determines that the validity of the restrictive marking is not justified, the Contracting Officer shall issue a final decision to the Contractor or subcontractor in accordance with the Disputes clause of this contract. Notwithstanding paragraph (e) of the Disputes clause, the final decision shall be issued within sixty (60) days after receipt of the Contractor's or subcontractor's response to the challenge notice, or within such longer period that the Contracting Officer has notified the Contractor or subcontractor of the longer period that the Government will require. The notification of a longer period for issuance of a final decision will be made within sixty (60) days after receipt of the response to the challenge notice.*

*(ii) The Government agrees that it will continue to be bound by the restrictive marking for a period of ninety (90) days from the issuance of the Contracting Officer's final decision under paragraph (g)(2)(i) of this clause. The Contractor or subcontractor agrees that, if it intends to file suit in the United States Claims Court it will provide a notice of intent to file suit to the Contracting Officer within ninety (90) days from the issuance of the Contracting Officer's final decision under paragraph (g)(2)(i) of this clause. If the Contractor or subcontractor fails to appeal, file suit, or provide a notice of intent to file suit to the Contracting Officer within the ninety (90)-day period, the Government may cancel or ignore the restrictive markings, and the failure of the Contractor or subcontractor to take the required action constitutes agreement with such Government action.*

*(iii) The Government agrees that it will continue to be bound by the restrictive marking where a notice of intent to file suit in the United States Claims Court is provided to the Contracting Officer within ninety (90) days from the issuance of the final decision under paragraph (g)(2)(i) of this clause. The Government will no longer be bound, and the Contractor or subcontractor agrees that the Government may strike or ignore the restrictive markings, if the Contractor or subcontractor fails to file its suit within one (1) year after issuance of the final decision. Notwithstanding the foregoing, where the head of an agency determines, on a nondelegable basis, that urgent or compelling circumstances will not permit waiting for the filing of a suit in the United States Claims Court,*

*the Contractor or subcontractor agrees that the agency may, following notice to the Contractor or subcontractor, authorize release or disclosure of the technical data. Such agency determination may be made at any time after issuance of the final decision and will not affect the Contractor's or subcontractor's right to damages against the United States where its restrictive markings are ultimately upheld or to pursue other relief, if any, as may be provided by law.*

*(iv) The Government agrees that it will be bound by the restrictive marking where an appeal or suit is filed pursuant to the Contract Disputes Act until final disposition by an agency Board of Contract Appeals or the United States Claims Court. Notwithstanding the foregoing, where the head of an agency determines, on a nondelegable basis, following notice to the Contractor that urgent or compelling circumstances will not permit awaiting the decision by such Board of Contract Appeals or the United States Claims Court, the Contractor or subcontractor agrees that the agency may authorize release or disclosure of the technical data. Such agency determination may be made at any time after issuance of the final decision and will not affect the Contractor's or subcontractor's right to damages against the United States where its restrictive markings are ultimately upheld or to pursue other relief, if any, as may be provided by law.*

*(h) Final disposition of appeal or suit.*

*(1) If the Contractor or subcontractor appeals or files suit and if, upon final disposition of the appeal or suit, the Contracting Officer's decision is sustained—*

*(i) The restrictive marking on the technical data shall be cancelled, corrected or ignored; and*

*(ii) If the restrictive marking is found not to be substantially justified, the Contractor or subcontractor, as appropriate, shall be liable to the Government for payment of the cost to the Government of reviewing the restrictive marking and the fees and other expenses (as defined in 28 U.S.C. 2412(d)(2)(A)) incurred by the Government in challenging the marking, unless special circumstances would make such payment unjust.*

*(2) If the Contractor or subcontractor appeals or files suit and if, upon final disposition of the appeal or suit, the Contracting Officer's decision is not sustained—*

*(i) The Government shall continue to be bound by the restrictive marking; and*

*(ii) The Government shall be liable to the Contractor or subcontractor for payment of fees and other expenses (as defined in 28 U.S.C. 2412(d)(2)(A)) incurred by the Contractor or subcontractor in defending the marking, if the challenge by the Government is found not to have been made in good faith.*

*(i) Duration of right to challenge. The Government may review the validity of any restriction on technical data, delivered or to be delivered under a contract, asserted by the Contractor or subcontractor. During the period within three (3) years of final payment on a contract or within three (3) years of delivery of the technical data to the Government, whichever is later, the Contracting Officer may review and make a written determination to challenge the restriction. The Government may, however, challenge a restriction on the release, disclosure or use of technical data at any time if such technical data—*

*(1) Is publicly available;*

*(2) Has been furnished to the United States without restriction; or*

(3) *Has been otherwise made available without restriction. Only the Contracting Officer's final decision resolving a formal challenge by sustaining the validity of a restrictive marking constitutes "validation" as addressed in 10 U.S.C. 2321.*

*(j) Decision not to challenge. A decision by the Government, or a determination by the Contracting Officer, to not challenge the restrictive marking or asserted restriction shall not constitute "validation."*

*(k) Privity of contract. The Contractor or subcontractor agrees that the Contracting Officer may transact matters under this clause directly with subcontractors at any tier that assert restrictive markings. However, this clause neither creates nor implies privity of contract between the Government and subcontractors.*

*(l) Flowdown. The Contractor or subcontractor agrees to insert this clause in contractual instruments with its subcontractors or suppliers at any tier requiring the delivery of technical data, except contractual instruments for commercial items or commercial components.*

(End of clause)

GENERAL RECOMMENDATIONS

This clause applies to both Technical Data and Computer Software/Documentation. Review the complete text of DFARS 227.71 and 227.72 for:

- Specific uses of 252.227-7037
- Clauses used in conjunction with 252.227-7037.
- Clauses used instead of 252.227-7037

### 3.13.3 Section M - Evaluation

### 3.13.4 Section L - Instructions to Offerors

# 4 Process and Product Support Activities

The Process and Product Support Activities section of this document provides RFP language examples that are used in the context of performing all projects. In general, these activities may address processes and their products that apply more generally to the organization. For example, quality assurance, configuration management, and measurement can be used to support all processes and products, and to provide objective evaluations of the processes and work products.

### 4.1 Automated Development and Support Environment

#### 4.1.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *An automated computer-based software life-cycle development and support environment will be used by the contractor. Development of the environment's requirements shall be the responsibility of the program office. The environment should provide the following capabilities: 1) specification of the life-cycle software development process and the monitoring/enforcement of that process, 2) integration of Computer-aided Software Engineering (CASE) and other tools supporting the various interphase activities of the life cycle, and 3) interphase support including program management, configuration management and baselining, document/specification generation, traceability and change impact analysis* [USAF 1996].

#### 4.1.2 Section M - Evaluation

#### 4.1.3 Section L - Instructions to Offerors

## 4.2 Certification and Accreditation Processes

### 4.2.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *Contractors must also warrant that proposed system and software product specifications and security and data access architectures have either been addressed in ongoing documentation required by the agency's certification and accreditation process [name the process, regulations governing the process, and specific documentation where this must be addressed] and are ready for evaluation in applicable phases of the process [list the specific phases of the process and specifically what is required in each phase]. Contractors must also address willingness to provide proposed equipment and engineering assistance as required, at no cost to the government, to the specified [name the testing facility] testing facility to obtain required certification of functionality* [DHS 2008].

EXAMPLE 2

> *Contractors must warrant that their products have been satisfactorily validated under common criteria or that products will be satisfactorily validated with the period of time specified in the contract and that such product validation will be maintained for updated versions or modifications by subsequent evaluation as required* [DHS 2009].

### 4.2.2 Section M - Evaluation

### 4.2.3 Section L - Instructions to Offerors

## 4.3 Configuration Management Audit

### 4.3.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The contractor shall conduct formal audits of the configuration management function, as provided for in the* Software Quality Assurance (SQA) *Plan, to ensure strict compliance with the requirements of the contract, the approved* Software Development Plan (SDP)*), and the approved Software Configuration Management Plan. The contractor's procedures shall ensure the effective configuration management of the developmental baseline from the time of contract award until final acceptance of the software and its associated documentation by the procuring agency. Also to be included in these procedures is the independent auditing of the status accounting system to assess effectiveness in tracking Software Trouble Reports. The contractor shall ensure that such procedures are integrated with the configuration management procedures addressing the total defense system when the software is only a portion of the total system development* [MIL-STD-QQQ].

### 4.3.2 Section M - Evaluation

### 4.3.3 Section L - Instructions to Offerors

## 4.4 Defect Prevention

### 4.4.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The Government's objective is for the supplier to define and mitigate the manufacturing process risks associated with the design solution through the development of producible designs, capable fabrication and assembly processes, and associated controls. This includes activities such as the following* [DOD 1998]:

*(1)* *Developing and implementing an approach for the identification of key product characteristics. Key product characteristics are the features of a material or part whose variation has a significant influence on product fit, performance, service life, or manufacturability* [DOD 1998].

*(2)* *Identifying manufacturing process risks (e.g., the risks related to developing stable and capable processes, to minimizing the need for engineering changes, to preventing defects) associated with the evolving design solution, and developing and implementing appropriate design alternatives and risk reduction efforts* [DOD 1998].

### 4.4.2 Section M - Evaluation

EXAMPLE 1

*Proposed approaches will be evaluated based upon* [DOD 1998]:

*(1)* *The extent to which they employ disciplined, structured processes (versus ad hoc or anecdotal) to identify and mitigate manufacturing process risks (e.g., the risks related to developing stable and capable processes, to minimizing the need for engineering changes, to preventing defects)* [DOD 1998].

*(2)* *The extent to which the processes for identifying key product characteristics and identifying/mitigating of manufacturing process risks are integrated with the overall systems engineering process* [DOD 1998].

*(3)* *The extent to which the proposed approaches reflect the integration of manufacturing process risk reduction efforts into the planning for this program* [DOD 1998].

### 4.4.3 Section L - Instructions to Offerors

EXAMPLE 1

*Propose and discuss any defect prevention practices to be employed for this acquisition. To facilitate Government evaluation methods, provide rationale for each such method, indicating how it helps to meet the SOO paragraphs on defect prevention* [DOD 1998].

*Describe how key product characteristics will be identified and how existing manufacturing process capabilities are considered in the assessment of manufacturing process risks associated with the evolving product design. Define how manufacturing process risk assessments are fed back to product design efforts to ensure that reducibility considerations are included in the evolving product design* [DOD 1998].

### 4.5 Measures

#### 4.5.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The System Development Plan (*Software Development Plan (SDP)*) shall specify the collection of the following minimum set of metrics, and the collection methodology* [Army 2006].

*a.* *Requirements volatility: total number of requirements at SSR and requirement changes over time after SSR.*

*b.* *Software size: planned and actual number of units, lines of code, or other size measurement over time.*

*c.* *Software staffing: planned and actual staffing levels over time.*

*d.* *Software progress: planned and actual number of software units designed, implemented, unit tested, and integrated over time.*

*e.* *Problem/change reports status: total number, number closed, number opened in the current reporting period, number by each software unit, age, and priority of open reports.*

*f.* *Computer hardware resource utilization: planned and actual use of computer hardware resources (e.g., processor capacity, memory capacity, input/output device capacity, communications/network equipment capacity, auxiliary storage device capacity, and bus bandwidth) over time and for the worst case operations scenario.*

*g.* *Milestone performance: planned and actual dates of software development activities and events (detailed Work Breakdown Structure (WBS) rate chart).*

EXAMPLE 2

*It is imperative that the operational* Reliability, Availability, and Maintainability (RAM) *metrics associated with the system are translated into contractual terms that become system RAM requirements within the RFP and contract. For acquisition of an overall weapons system, an overall RAM requirement including Integrated Diagnostics should be imposed in the contract and demonstrated* [DOD 2005].

EXAMPLE 3

*The contractor shall systematically collect and report actual contract costs to provide DoD cost analysts with needed data to estimate future costs. Contractor reports shall be prepared in accordance with the instructions contained in the most recently approved versions of DI-FNCL-81565, DI-FNCL-81566, and DI-FNCL-81567. The contractor as part of the response to the solicitation will* [DOD2008a]:

*a.* *Accept or propose changes to the approved Contract Cost and Software Data Reporting (CSDR) Plan, DD Form 2794, that includes the contract WBS using the approved Program Plan and the Contract Plan provided by the DoD program office as the baseline. The Contract CSDR Plan will include level 3 of the contract WBS and any lower level WBS elements designated by DoD as being high risk, high value, or high technical interest. The contractor may further extend the WBS for its own reporting purposes.*

b. *Negotiate, if appropriate, a revised Contract CSDR Plan that will be submitted by the DoD program office to the DCARC for review and the Cost Analysis Improvement Group (CAIG) Chair's approval. The final approved Contract CSDR Plan will be incorporated into the contract.*

c. *IAW DFAR 215.403-5, provide contract cost estimates on the DD Forms 1921, 1921-1 and 1921-2 using the contract CWBS dictionary proposed in subparagraph a above.*

*After contract award the contractor shall:*

d. *Provide the final contract WBS and dictionary IAW DI-MGMT-81334 within 60 days after contract award. Maintain and update the WBS and dictionary during contract execution. Submittals will be no more frequent than CCDR reports.*

e. *Prepare and provide CCDRs IAW DI-FNCL-81565, DI-FNCL- 81566, and DIFNCL-81567 and with the approved Contract CSDR Plan.*

f. *Flow down CCDR requirements to any lower tier contractor that will have a contract valued at over $50 million or any contracts valued at between $7 million and $50 million that are designated by the DoD program office as being high risk, high value, or high technical interest* [DOD 2008a].

EXAMPLE 4

*The metrics should clearly portray variances between planned and actual performance, enable early detection or prediction of situations that require management attention, and support the assessment of proposed changes on the program. All programs of record with any software, regardless of ACAT category, shall define, develop, and implement the following minimum set of core metrics specific to their program.*

- *Software Size*
- *Cost Schedule (WBS) focus on software)*
- *Software Quality*
- *Software Organization*

*The core metrics should be tailored and implemented consistent with both of the Program office's and the developer's internal tools and processes. Program offices and developers should establish and agree upon additional metrics or means of insight to identify and address software issues deemed critical or unique to the program* [USN 2008a]

GENERAL RECOMMENDATIONS

Specify the tracking and analysis of performance Metrics/measures in the RFP [SEI 2007a].

Establish clear performance thresholds for each performance measure [SEI Test 2007].

Performance Metrics/measures must be directly related to the risks you identify, and support the actions you take to mitigate those risks [SEI 2007a].

If you do not know what decision a measure supports, THROW IT OUT [SEI 2007a].

Your RFP should define the indicators and metrics the government needs to track progress, quality, schedule, cost, and maintainability. What you should look for when analyzing an offeror's Metrics Usage Plan is "control." Through measurement, the process's internal workings are defined and assessed. If an effective process improvement plan is executed (which requires that appropriate measurements are taken) data are collected and analyzed to predict process failures. Therefore, the offeror must have a corporate mechanism implemented in a systematic manner that performs orderly process control and methodical process improvement. This can be identified by the measurement methods the company uses to assess the development process, analyze the data collected, and feedback corrections for problems within the process [USAF 2000].

After you have identified your program issues (and before contract award) you and your future contractor must agree on entry and exit criteria definitions for the proposed software development process and products. Entry and exit criteria must also be defined for all data inputs, standards of acceptance, schedule and progress estimation, and data collection and analysis methods. For instance, there must be an agreement on the definition of source lines-of-code and how and when SLOC will be estimated or counted. The entire collection and analysis process—all definitions, decisions, and agreements—should be written into the contract [USAF 2000].

Make sure the software quality metrics and indicators they employ include a clear definition of component parts (e.g., SLOC), are accurate and readily collectible, and span the development spectrum and functional activities. They must identify metrics early and apply them at the beginning of the system engineering and software implementation process. They should also develop software Metrics Usage Plan before contract award [USAF 2000].

### 4.5.2 Section M - Evaluation

EXAMPLE 1

> *The contractor's customized SRDR and Data Dictionary will be evaluated on the extent to which (1) the report captures the Government's stated need and (2) the data provided is integrated with the contractor's normal oversight and management procedures* [DOD 2008].

### 4.5.3 Section L - Instructions to Offerors

EXAMPLE 1

> *The Government identifies software resources data on the elements identified within the attached CSDR Plan, DD Form 2794. The data for each marked element are contained in the most recently approved versions of the DI-MGMT-81739 and DI-MGMT-81740. The government objective is to collect a subset of the same data that the contractor normally collects to oversee and manage software development efforts. Therefore, the Government expects the contractor to customize or tailor the sample formats to be consistent with data it normally collects. The Government will approve the customized or tailored formats proposed by the contractor. The contractor shall provide a SRDR Data Dictionary with the customized formats.*

*The contractor shall submit the completed SRDR Initial Developer Report within 60 days after contract award for the entire software product, and within 60 days after initiation of each software release or build. The contractor shall submit a completed SRDR Final Developer Report within 60 days of delivery of each delivered software release. The contractor shall submit a completed SRDR Final Developer Report for the entire software product within 60 days of delivery of the final software element. Report format and other delivery requirements are specified in the attached CDR* [DOD 2008].

## 4.6 Quality Assurance Program General Requirements

### 4.6.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> ***General.*** *The contractor shall plan, develop, document and implement a* Software Quality Assurance (SQA) *Program to ensure that high levels of software quality are attained and all contractual requirements are complied with fully. Program reporting shall be part of the management reporting system during all phases of software development. The contractor's Program shall, as a minimum, utilize assessments, documentation reviews, design reviews, monitoring, auditing, and testing to ensure compliance with contractual requirements. The Program shall be applied to, but not limited to, the following: software requirements; software design; software engineering standards, practices and procedures; computer program implementation; software documentation, software testing; software library controls; configuration management; corrective action; and subcontractor control* [MIL-STD-QQQ].
>
> ***Management.*** *Effective Software Quality Assurance (SQA) management shall have sufficient, well-defined responsibility, authority, and the organizational freedom to identify and evaluate quality problems and to initiate, recommend and/or provide solutions. Contractor management regularly shall review the status and adequacy of the Program and realign the Program to insure that its requirements and those of contracts will be satisfied. The term "*Software Quality Assurance (SQA) *Program Requirements" are used herein includes the collective requirements of the Standard. The fulfillment of the requirements of this Standard are not intended to be responsibility of any single contractor organization, function, or person. However, the organizational groups responsible for the Program's implementation, monitoring and enforcement shall have, as a minimum, corporate reporting responsibility external to and independent of the software developing/engineering group to ensure an objective evaluation of the software quality, including compliance with contractual requirements* [MIL-STD-QQQ].
>
> ***Reporting.*** *The contractor's organization responsible for software* Quality Assurance *shall be provided a corporate reporting chain that is independent of the manager of the organization responsible for developing the software under contract* [MIL-STD-QQQ].
>
> *Results of all software* Quality Assurance *activities shall be documented in established formats and shall be promptly submitted to the proper authority. These reports shall be available for review by the procuring agency. Failure to report discovered discrepancies will be considered in non-conformance with contractual requirements* [MIL-STD-QQQ].

EXAMPLE 2

> *The Developer shall establish a* Software Quality Assurance (SQA) *Process IAW the Developer's Government approved* Software Quality Assurance (SQA) Process(SQAP, *or the* Software Development Plan (SDP) *when the* Software Quality Assurance Process(SQAP) *is incorporated into the* Software Development Plan (SDP). *The Developer shall document their processes in the* Software Quality Assurance Process(SQAP) *(see section 8.3.21), which may be included as part of the* Software Development Plan (SDP). *The* Software Quality Assurance (SQA) *process and life cycle objective evidence shall be recorded and made available to support contractual requirements. Provision shall be made to permit Government representatives to review procedures and data during all phases of the Developer's performance* [Army 2006].

*The Developer shall provide Software Quality indicators to report the status of software quality. The Developer's existing software quality data collection and reporting formats shall be made available to the Government for evaluation. The status of problem reports (open/closed) shall be provided electronically every two weeks* [Army 2006].

### 4.6.2 Section M - Evaluation

### 4.6.3 Section L - Instructions to Offerors

## 4.7 Quality Assurance Program Plan

### 4.7.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The contractor shall develop a* Software Quality Assurance (SQA) *Plan (hereafter referred to as the "Plan") to document the application of the Program to a specific contract. The Plan shall identify Organizational responsibilities and authorities for its execution and the events critical to its implantation* [MIL-STD-QQQ].

### 4.7.2 Section M - Evaluation

### 4.7.3 Section L - Instructions to Offerors

## 4.8 Quality Assurance Reviews and Audits

### 4.8.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The contractor shall establish procedures for the preparation and execution of independent software* Quality Assurance *reviews and audits. These procedures shall be subject to the review and approval by the procuring agency. The procedures shall include provisions for assessing software and its associated documentation's conformance with standards and technical/contractual requirements and shall establish traceability of the original contractual performance requirements throughout the software development. The Plan shall identify the schedule and the persons responsible for the conduct of such audits throughout the software development from time of contract award through final software acceptance by the procuring agency* [MIL-STD-QQQ].

EXAMPLE 2

> *Subcontractor Quality Assurance Audits. The contractor is responsible for imposing the software quality requirements on any and all subcontractors that he may employ for the development of defense department software. Accordingly, the contractor shall conduct periodic audits of his subcontractors' software* Quality Assurance *program, plan, and execution thereof to ensure that all requirements are being satisfied and that the software being developed possesses the highest degree of quality feasible* [MIL-STD-QQQ].

### 4.8.2 Section M - Evaluation

### 4.8.3 Section L - Instructions to Offerors

### 4.9 Risk Identification and Mitigation Approach

#### 4.9.1 Section C - SOW/SOO; Requirements

#### 4.9.2 Section M - Evaluation

EXAMPLE 1

Proposal Requirement #X: Risk Identification/Mitigation [USAF 2005]

> *The proposal requirement will be met when the Offeror proposes specific, cost effective, and technically sound risk mitigation activities for the prioritized list of risks submitted, including burndown plans coordinated to program milestones, for significant risks such that risks are mitigated prior to the appropriate program milestone. The risk information exhibits an understanding of the risk levels (probability of occurrence and severity of consequence), implementation of an approach to address inter/intra-segment and external interface risks, and implementation of an approach to mature technologies deemed critical to the proposed architecture. The risk analysis adequately justifies these risks and includes isolation of causes and determination of effects. The risk information should identify organizational responsibilities and provide a realistic work schedule in the IMS and effort in the WBS which is consistent with objectives for TSAT/TMOS milestones.*

#### 4.9.3 Section L - Instructions to Offerors

EXAMPLE 1

Proposal Requirement #X: Risk Identification/Mitigation [USAF 2005]

> *Propose risk mitigation/burn down activities for those risks identified below as well as significant contractor identified risks. Mitigation approaches may include, but are not limited to, technology development, prototypes, field demonstrations, engineering models and simulations. The burn down plans should include the required tasks and allocated resources and should be consistent with the IMP and IMS. Based on your assessment of the TMOS TRD, in the context of the overall TMOS program, provide a detailed description of the critical management and systems engineering risk areas for the TMOS Segment, with associated rationale. Provide a prioritized list of all significant technical and management risks. Consider risks for all program phases. At a minimum this information should:*
>
> > *Describe your approach to establish technical maturity of Policy Based Management (PBM) consistent with the deployment schedule.*
> >
> > *Describe the risk associated with ensuring interoperability with GIG networks.*
> >
> > *Describe the risks associated with ensuring certification and accreditation of the TSAT network and TMOS elements.*
> >
> > *Describe the risk associated with accommodating mobile (COTM) terminals.*
> >
> > *Describe the risk associated with the use of COTS/GOTS/NDI components including the risk of integrating multiple products.*

## 4.10 Risk Management

### 4.10.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The RFP should state that the offeror's approach be organized around identified software development risks and how they will exploit risk mitigation opportunities throughout contract performance* [USAF 2000].

### 4.10.2 Section M - Evaluation

### 4.10.3 Section L - Instructions to Offerors

| GENERAL RECOMMENDATIONS |
| --- |
| The offeror should document the approach to be used in managing risk in developing software and integrating it in the system. The offeror should be required to quantify performance, support, cost, and schedule risk factors (this should be part of the offeror's Software Development Plan (SDP) [USAF 1996]. |

## 4.11 Risk Program Approach

### 4.11.1 Section C - SOW/SOO; Requirements

### 4.11.2 Section M - Evaluation

### 4.11.3 Section L - Instructions to Offerors

EXAMPLE 1

Proposal Requirement #X: Risk Program [USAF 2005]

> *Describe your risk program that identifies, plans for, tracks, and controls risks. Identify and establish the quantified acceptable risk levels that need to be achieved prior to transitioning to deployment, including definitions of the criteria used to determine the acceptability of the risk levels and justification for the selection of those criteria.*

### 4.12 Securely Configuring Proprietary Commercial Software

#### 4.12.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*Vista™ and Windows XP™ Standard Secure Configuration* [DHS 2008]

(a) *The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For Windows XP settings, see: <http://csrc.nist.gov/itsec/guidance_WinXP.html>, and for the Windows Vista settings, see: <http://csrc.nist.gov/itsec/guidance_vista.html>* [DHS 2008].

*(b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to default "program files" directory and should be able to silently install and uninstall* [DHS 2008].

*(c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges* [DHS 2008].

#### 4.12.2 Section M - Evaluation

#### 4.12.3 Section L - Instructions to Offerors

## 4.13 Security Controls and Standards

### 4.13.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*(a) When mitigating or remediating risks to confidentiality, integrity, and availability of Federal Information Systems, National Security Systems, contractor assets that enable possession, control, or otherwise enable access to Federal Information or National Security Systems, the Contractor shall implement controls and standards as effective or more effective than those implemented by the Agency for the same or substantially similar risks with the same or substantially similar potential measure of harm* [DHS 2008].

(b) *When selecting appropriate controls and standards for protecting confidentiality, integrity, and availability of Federal Information and National Security Systems, the Contractor shall use the analyses, processes, and standards established for Federal Government systems established by the [current organization/agency and other applicable standards] publications* [DHS 2008].

### 4.13.2 .Section M - Evaluation

### 4.13.3 Section L - Instructions to Offerors

### 4.14 Software Assurance Case Submission

#### 4.14.1 Section C - SOW/SOO; Requirements

#### 4.14.2 Section M - Evaluation

#### 4.14.3 Section L - Instructions to Offerors

EXAMPLE 1

> *In order for the Acquirer to evaluate the proposed software assurance capabilities, the potential suppliers must submit an initial Software Assurance Case in accordance with ISO/IEC 15026, Systems and software engineering—Systems and software assurance—Part 2: Assurance Case . Paragraph 3.2 below identifies the minimum that should be included in the initial assurance case. The initial Software Assurance Case shall subsequently become a part of the contract and be used by the Acquirer as initial acceptance conditions* [DHS 2008].
>
> *It is understood that the initial Software Assurance Case will be broad in nature because potential suppliers will not know all the details of safety and security until contract performance. However, the assurance case should be comprehensive enough to convey a clear understanding of the safety and security requirement of this RFP. As a minimum, the initial Software Assurance Case shall include the following* [DHS 2008]:
>
> *3.2.1 Top-level claims (and sub-claims as appropriate). These claims shall include all the characteristics of claims defined in ISO/IEC 15026.*
>
> *3.2.2 Arguments for the top-level claims and subclaims. These arguments shall include all the characteristics of arguments defined in ISO/IEC 15026.*
>
> *3.2.3 Evidence and explicit assumptions supporting the arguments. The evidence shall include all the characteristics of evidence defined in ISO/IEC 15026.*
>
> *3.2.4 Approving authority for the assurance case. The approving authority resume shall be included. The resume should include evidence of the authority's experience and education in software assurance and developing and managing software assurance cases.*

## 4.15 Software Security Acceptance and Measurement Criteria

### 4.15.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

(a) *The Supplier shall provide all operating system, middleware, and application software to the Acquirer security configured by Supplier in accordance with the FAR requirement based on 44 USC 3544 (b) (2) (D) (iii)* [DHS 2008].

(b) *The Supplier shall demonstrate that all application software is fully functional when residing on the operating system and on middleware platforms used by the Acquirer in its production environment, configured as noted above.*

(c) *The Supplier shall NOT change any configuration settings when providing software updates unless specifically authorized in writing by the Acquirer.*

(d) *The Supplier shall provide the Acquirer with software tools that the Acquirer can use to continually monitor software updates and the configuration status.*

(e) *At specified intervals by the Buyer, the Supplier shall provide the Acquirer with a comprehensive vulnerability test report for the suite of applications and associated operating system and middleware platforms used by the Acquirer in its production environment, configured as noted above.*

(f) *The Acquirer and Supplier agree to work together to establish appropriate measures to quantify and monitor the supplier's performance according to the contract requirements. Specific guidance should include types of measures to be used, measures reporting frequency, measures refresh and retirement, and thresholds of acceptable performance.*

(g) *The Supplier shall provide all operating system, middleware, and application software to the Acquirer free of common vulnerabilities as specified by the Common Vulnerabilities and Exposures (CVE®)—The Standard for Information Security Vulnerability Names that can be retrieved from http://cve.mitre.org/*

(h) *The Supplier shall provide all operating system, middleware, and application software to the Acquirer free of common weaknesses as specified in the Common Weakness Enumeration, A Community-Developed Dictionary of Software Weakness Types that can be retrieved from http://cwe.mitre.org/* [DHS 2008].

### 4.15.2 Section M - Evaluation

### 4.15.3 Section L - Instructions to Offerors

### 4.16 Trustworthy Software

#### 4.16.1 Section C - SOW/SOO; Requirements

GENERAL RECOMMENDATIONS

1.0 Trustworthy Software [DHS 2008]

1.1 Key definitions [DHS 2008]

"Security controls" mean the management, operational, and technical controls (that is, safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information [NIST SP 800– 53]. This definition includes software.

"Security category" means the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals [FIPS Pub 199].

"Security objectives" mean confidentiality, integrity, and availability [44 USC, Sec. 3542].

"Assurance" means grounds for justified confidence that a claim has been or will be achieved. (ISO/IEC 15026).

"Assurance Case" means representation of a claim or claims, and support for these claims (ISO/IEC 15026). A Software Assurance Case includes (software assurance) claims and evidence that support those (software assurance) claims. Include other appropriate definitions.

1.2 Security Category (NOTE: This is an example. Also see [FIPS 199] and [DODI 8500.2, Enclosure 4)

This software system is used for large procurements in a contracting organization and contains both sensitive and proprietary supplier information and routine administrative information. For the sensitive supplier information, the potential impact from a loss of confidentiality is moderate (for example, the loss may result in a significant financial loss), the potential impact from a loss of integrity is moderate (for example, the loss may result in the effectiveness of the contracting mission is significantly reduced and there is significant damage to the information asset), and the potential impact from a loss of availability is low (for example, the loss may result in downtime, but there is backup). For the routine administrative information, the potential impact from a loss of confidentiality is low, the impact from a loss of integrity is low, and the impact from a loss of availability is low. Based on 1.2, the resulting security category of the software system is {(confidentiality, moderate), (integrity, moderate), (availability, low)} [DHS 2008].

1.3 Software Security Requirements.

Based on the security category for the software system, the minimum security requirements specified in (NOTE: Reference the external document(s)) are required. (NOTE: Minimum security controls may be specified in this paragraph or in an external document similar to FIPS Pub 200; National Institute of Standards and Technology (NIST) SP 800–53; and DODI 8500.2, Enclosure 4) [DHS 2008].

1.4 Software Assurance Case.

The Software Assurance Case shall be the primary instrument for refining and monitoring software assurance during the life of this contract. The Software Assurance Case shall be developed and conform to the requirements of ISO/IEC 15026, Systems and software engineering—Systems and software assurance—Part 2: Assurance Case. The supplier shall refine the Software Assurance Case throughout the development process and should be based on the software assurance requirements of this contract. The contractor shall submit the case for review. (NOTE: Specify when the case should be reviewed, such as with the submission of the software design) Lastly, the successful execution of the Software Assurance Case shall be a condition for final acceptance of the software product/service [DHS 2008].

#### 4.16.2 Section M - Evaluation

#### 4.16.3 Section L - Instructions to Offerors

# 5 Project Management

The Project Management section of this document provides RFP language examples to assist acquiring organizations with visibility into contractor activities such as planning, monitoring, and controlling the project. Examples address multiple points in the life cycle and include establishing and maintaining plans, managing commitments, monitoring progress against plans, and taking corrective action.

## 5.1 Contractor Monitoring

### 5.1.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Statement of Work for the procurement must address requirements that the functional processes of Software Acquisition Planning, Requirements Development, Management, Project Management and Oversight, and Risk Management must be demonstrated and exercised by the developer in a continuous manner and be equivalent to that articulated by CMMI Capability Level 3* [USN 2006].

### 5.1.2 Section M - Evaluation

### 5.1.3 Section L - Instructions to Offerors

GENERAL RECOMMENDATIONS

The purpose of this activity is to ensure that Section L of the Request for Proposal contains appropriate instructions that allow for an adequate government review of the offeror's approach to satisfying the system performance requirements s well as adequate evaluation of the offeror's software development processes and planned development approach [SMC 2004].

Currently, the SEI Capability Maturity Model— Integrated (CMMI) model and methodology can serve as a representative set of mature software development and management processes. Other appraisal models or methodologies may currently be in use on DoD programs [SMC 2004].

## 5.2 Contractor Statement of Work (CSOW)

### 5.2.1 Section C - SOW/SOO; Requirements

### 5.2.2 Section M - Evaluation

### 5.2.3 Section L - Instructions to Offerors

EXAMPLE 1

Attachment CDX to Volume X: Contractor Statement of Work (CSOW) and Annexes [USAF 2005]

> *A Statement of Objectives (SOO) is provided as Attachment x to the solicitation. The SOO represents the Government's minimum objectives for TMOS. The Offeror shall use the SOO to propose a WBS-structured SOW, which expands upon these minimum objectives to the extent necessary to perform this effort. The proposed CSOW shall define the tasks required for TMOS, ensuring all minimum requirements of the Government provided SOO and preliminary WBS have been addressed. The proposed CSOW shall consist of tasking statements. Each tasking statement shall reference the CDRL items that will be delivered by that task. The proposed CSOW shall not contain informational notes, as the Mission Capability volume provides ample opportunity for discussion and description of the Offeror's approach, and the IMP and IMS provide the mechanisms for describing specific details of the Offeror's approach. The tasking statements in the CSOW, elements of the CWBS, and the IMP and IMS sections shall use a common numbering system. The proposed CSOW, when accepted by the Government, shall be put on contract at award.*

**CSOW Tasks**

> *The proposed CSOW shall, at a minimum, include all SOO items and the following tasks:*
>
> *Implement a seamless Electronic Data Interchange (EDI) with the Government utilizing Web-based technology at the unclassified and Secret level. EDI processes shall be referenced in the IMP, as applicable. The EDI shall establish and maintain the capability for electronic mail, scheduling, and access to CDRLs. It shall provide access to all other data to include subcontractor data in the prime's possession and working draft data (classified up to DoD Secret) developed to support the management and engineering efforts of the program and this data shall be included in the Data Accession List. This shall include, but not be limited to, the latest requirement allocation status traced from technical and capability requirements documents to subordinate segment hardware and software requirements.*
>
> *Conduct a multi-day program startup workshop, monthly program management reviews, and quarterly risk reduction reviews. Conduct a quarterly review (in place of that month's program management review) that has increased external segment emphasis and representation from other program segments and users. Structure these reviews to provide insight into the technical design, risk, cost and schedule progress, and management issues.*
>
> *Conduct Integrated Baseline Reviews. Such reviews shall be scheduled as early as practicable and should be conducted within 180 calendar days after (1) contract award, (2) the exercise of significant contract options, or (3) the incorporation of major modifications. The objective of the integrated baseline review is for the Government and*

*the Contractor to jointly assess areas, such as the Contractor's planning, to ensure complete coverage of the statement of work, logical scheduling of the work activities, adequate resourcing, and identification of inherent risks.*

*Develop and document a time-phased TMOS Segment Integration, Test, and Evaluation (IT&E) strategy, concept and master plan. Support development of key T&E documentation developed within Government IPTs. Provide support, as needed, to Operational Test Agencies. Perform box/component/software item/segment/inter-segment/system level testing to ensure end-to-end verification of TMOS and TSAT network requirements and capabilities. Support the TSAT Multi-Service Initial Operational Test and Evaluation (MOT&E) certification process. Maintain compliance with the Government Deficiency Reporting (DR) System described by Technical Order (TO) 00-35D-54. Integrate deficiency resolution and IT&E activities with the program management, systems engineering, and risk management processes as well as hardware/software development and sustainment activities.*

*Develop and conduct logistics and supportability analysis concurrent with and as an integral part of the overall systems engineering process compatible with Government infrastructure and in accordance with the MIL-PRF-49506—Logistics Management Information Performance Specification. Assist the Government as a partner in determining Depot Source of Repair Assignment Process (SORAP).*

*Develop safety requirements and conduct a comprehensive Environmental, Safety and Occupational Health (ESOH) Analysis complying with all Federal, state, and local laws and regulations and provide compliance documentation.*

*Provide conceptual designs, LCC updates, program management planning and Risk Mitigation status.*

*Map the Government supplied TSAT CONOPS to the TMOS TRD by TMOS post-award System Requirements Review (approximately 1.5 – 2 months after contract award).*

*Develop and stabilize the user interface early in accordance with Human Factors Engineering standards, using the TMOS Demonstrator as appropriate. Identify schedule and functionality of TMOS Demonstrator incremental capability deliveries. TMOS Demonstrator deliveries will be in advance of relevant PMP's incremental deliveries. TMOS Demonstrator deliveries will be in advance of relevant TMOS major IMP events (see the section below Attachment CD2 to Volume IV: Integrated Master Plan (IMP)).*

*Support the Government in determining the compliance requirements for DOD Information Technology Standards Registry (DISR) standards, including updates to appropriate TRDs. In addition, the contractor shall generate DISR profiles (i.e., standards profiles, DoDAF TV-1) through the use of the DISR online tool.*

*Support the Government in the implementation of the program's Modular Open Systems Approach (MOSA).*

*Provide all necessary data and support for implementation of applicable Net-Ready KPP requirements.*

*Implement an accredited EVM system in accordance with ANSI/EIA-748 to actively and effectively manage cost, schedule, and performance through the life of the program. Conduct quarterly EAC updates and provide the Government with sufficient documentation to support estimates. CPR data should be submitted in accordance with CDRL A003 and each task shall be loaded individually to correspond to its appropriate resource.*

*Develop and demonstrate a functional CAIV model, and conduct a TMOS CAIV trade analyses, based upon your design and corresponding LCC estimate (which includes risk reduction and design development and acquisition/operations). The model shall include the Basis of Estimate (BOE) by WBS element and a complete risk analysis (cost, schedule & technical) in 10% confidence intervals (10%, 20%, 30%, etc.). All cost deliverables shall include a clear trace between the LCC WBS and all plans that relate to the risk reduction and system development phases of the program. The model shall identify time-phased costs (then year and base year). The contractor shall participate in the Cost/Performance IPT (CPIPT) and conduct meetings to present results to and answer questions from the CPIPT.*

*Participate in the TSAT program giver/receiver forum to build an IMS that integrates all segments of the TSAT program. Deliver the IMS in an electronic format compatible with the Government's IMS. Coordinate with the Government in defining and mapping data fields within the IMS in order to facilitate data exchange.*

*Verify TMOS requirements, including hardware and software integration and maintenance, network integration and test, and support to TSAT requirements in accordance with the TSAT and TMOS TRDs.*

*Data Accession List items shall be readily and electronically accessible by the Government with revision control.*

*The contractor shall identify all software that shall require NSA certification. This software shall be segregated such that it can be delivered separately. In addition the documentation for this software shall be easily separated from, or easily identified as a separate section within, the software-related CDRLs.*

*Contractors will operate in accordance with contractor-generated, Government-approved plans including but not limited to: Software Development Plan, Systems Engineering Master Plan, Information Assurance Plan and test plans.*

*The contractor shall work with the government through the post-award System Design Review to update and finalize the list of applicable compliance and reference documents.*

#### *TMOS Contractor Roles and Responsibilities at the TSAT System Level*

*The proposed CSOW must also cover tasks related to TSAT system and segment IPT activities and products. Table 6.2.1 summarizes TMOS contractor roles and responsibilities in this regard. Using this table as guidance, the following tasks at a minimum must be addressed in the CSOW:*

A. *Lead network architecture coordination within the TSAT Network IPT to ensure payload and terminal constraints are accommodated and proper trades completed; address user and operator needs; coordinate with external network programs and activities (e.g. GIG E2E; GIG/BE; tactical networks).*

B. *Lead NM and OM coordination within Network IPT working groups, including extensive coordination with TSAT segments and external network management and mission planning organizations.*

C. *Support the TSAT System Requirements IPT, including recommending and coordinating changes to system requirements for the TSAT network based upon the approved TSAT network architecture and changes to TSAT NM/OM requirements as appropriate. Provide recommended network requirement updates for the System TRD (sections 3.2.x’s and impacted sections 3.7.x’s for all segments) and TMOS*

*TRD (sections 3.7.x's) based upon the approved network architecture and design. For these requirements, provide and update verification plans (VCRM entries and RVPs), including verification plans to allocated segments. These will be used as inputs and recommendations to the Program T&V IPT to integrate into system level plans. Maintain traceability of TSAT TRD sections 3.2.x's and 3.7.x for the network requirements.*

D. *Support the TSAT System CAIV IPT, including performing TMOS CAIV studies and coordinating cross-segment trades.*

E. *Support the TSAT System Test and Verification IPT, including a leadership role in TSAT network testing. Within the T&V IPT intersegment and system test working groups, lead E2E network (packet services) system testing, including selected test case development, planning, test requirement development and the development of selected simulated test scenario external inputs. Provide input data for RVPs involved with network system level requirements verification and provide appropriate data for verification of other system level requirements. Coordinate on all suggested changes to network VCRMs and RVPs, including allocations to all segments. This work will be consistent with the SE&I developed System Test and Verification Plan (STVP) and done within the structure of the SE&I Integration, Test and Verification IPT. Provide support for other system level (circuit services) integration and test activities as well as network end to end testing with the GIG and any other external networks. Prepare test reports for TMOS segment level testing and E2E network testing for TSAT for use in the SE&I requirement verification process. Identify appropriate risk reduction tests for TMOS and the TSAT network along with support requirements.*

F. *Support the TSAT System Interfaces and Standards IPT, including a leadership role in producing ICDs listed in Table 6.2-1, as well as playing a major role in the TMOS to Space ICD and Payload to Terminal ICD.*

G. *Support the TSAT System Integration IPT, including a leadership role in developing a TSAT network integration plan, coordinating with TSAT segments and external networks (e.g. terrestrial GIG, tactical networks).*

H. *Support the TSAT System Terminal ILT, including a leadership role in developing the TMOS to terminal interface, coordinating with TSAT segments and terminal programs (JTEO and service terminal programs).*

I. *Support, lead, or coordinate with additional IPT and working group activities listed in Table 6.2-1. In addition, participate in external activities, including GIG E2E working groups, test activities, operational planning groups, and similar activities.*

J. *Perform network level (E2E) modeling and simulation activity, including model development and/or integration as required.*

K. *Support the program office in the development of a plan for the transition to operations, to include transition of AEHF to TSAT.*

*Table 6.2-1: TMOS Contractor Roles and Responsibilities*

| | TMOS Contractor Role | TMOS Products |
|---|---|---|
| System - Network | CL | Network Architecture (CDRL) |
| System - System Requirements | S, CL for network requirements | TSAT network requirements recommendations |
| System - CAIV | S | CAIV Study Reports |
| System - Software | S | |
| System - Test and Verification | S, CL for network testing; Verify Network Requirements | Network test plan; Network test report (CDRLs); RVP Inputs |
| System - Mission Systems Engineering | S | |
| System - Interfaces and Standards | S, CL for network, OM, NM ICDs | (all CDRLs) TMOS-Terminal ICD; Common MNE ICD; TMOS to External NMS ICD; TMOS to KMI/SMI ICD; TMOS to external planning ICD; TMOS to AEHF MCS ICD* |
| System - IA | S | |
| System - Risk Management | S | Segment Risks & Burn Down Plans |
| System - Modeling and Simulation | S | Network modeling and simulation |
| System - Integration | S, CL for network, OM, NM integration | Network Integration Plan (CDRL) |
| System - Terminal | S | |
| TMOS - SEIT | CL | |
| TMOS - IA/Crypto | CL | |
| Space - Payload | S | |
| Space - SEIT | C | |
| Space - IA/Crypto | C | |

Role Legend: CL - Contractor Lead; S - Support IPT; C - Coordinate with IPT

* If needed, based upon Offeror's proposed approach to AEHF integration

### 5.3 Contractor Work Breakdown Structure (CWBS)

#### 5.3.1 Section C - SOW/SOO; Requirements

#### 5.3.2 Section M - Evaluation

#### 5.3.3 Section L - Instructions to Offerors

EXAMPLE 1

Attachment CDX to Volume X: CWBS [USAF 2005]

> *A Government Work Breakdown Structure (WBS) for the TMOS Segment program has been provided as Attachment 12 of the solicitation. The reference document for developing the WBS and dictionary is DoD Military Handbook 881/MIL-HBK-881 – Work Breakdown Structure. The Offeror shall develop a Contractor Work Breakdown Structure (CWBS) and dictionary, which reflects their view of the contract effort. The CWBS shall serve as the framework for organizing the TMOS Segment Program in-house, inter-divisional, subcontractor, and associate contractor activities. The Offeror may re-arrange and/or combine the WBS elements shown but must still maintain the visibility of the government-provided elements within the contractor's EVMS deliverables. The Offeror should also develop depth (level) and breadth sufficient to accurately describe the Offeror's understanding of the effort required for the TMOS Segment Program as reflected in the SOW. A mapping of CLINs to WBS elements shall be completely consistent with that shown in Section B of the Model Contract.*

## 5.4 Corrective Action

### 5.4.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The contractor shall establish a corrective action system for reporting, correcting, and analyzing problems/failures occurring during all phases of software development. The contractor shall provide for the conduct of periodic audits of this system to ensure its continuous effectiveness* [MIL-STD-QQQ].
>
> *The contractor shall perform periodic analysis of all software trouble reports for the purpose of identify trends which may disclose generic problem areas. The trend analysis shall include the study of the causes, magnitude of impact, frequency of occurrence, and preventive measures* [MIL-STD-QQQ].

### 5.4.2 Section M - Evaluation

### 5.4.3 Section L - Instructions to Offerors

### 5.5 Cost and Schedule

#### 5.5.1 Section C - SOW/SOO; Requirements

#### 5.5.2 Section M - Evaluation

#### 5.5.3 Section L - Instructions to Offerors

EXAMPLE 1

*Factor ( ): Cost Proposal (Open Architecture Related)* - *The Government will evaluate the following costs with respect to how they further XXX Open Architecture goals:* [USN 2007a]

- *Supplemental Information Concerning Cost/Price of Noncommercial Technical Data (TD), Noncommercial Computer Software (CS), and Noncommercial Computer Software Documentation (CSD)*
- *Supplemental Information Concerning Cost/Price of Commercial Computer Software (CS), and Commercial Computer Software Documentation (CSD) and Commercial Technical Data (TD)*
- *Supplemental Information Concerning Cost/Price of Background Inventions*

GENERAL RECOMMENDATIONS

The RFP should require offerors to provide a development schedule appropriate to the known requirements, showing all major milestones, audits, reviews, inspections, and deliverables. It is expected that this schedule will change as requirements become better defined. Evaluate this schedule to determine if the offeror understands the need for presenting detailed schedule information and for tying that information to detailed program requirements. Determine whether the program tracking system being proposed is part of the company's normal management practices or if it is new for this program. Also, you will want to ensure schedule needs and types are described and included in the Software Development Plan (SDP) [USAF 2000].

Problems are often created when schedule baselines are established before software requirements are well defined and understood. government RFP preparers may include schedule information based on factors that do not account for the system development process or software requirements. Offerors then inadvertently accept RFP schedule information as a requirement for a responsive proposal, and prepare their response based on these so-called requirements. This practice causes offerors to bid to untenable schedules affecting the viability of their submissions, decreasing the probability they will complete tasks as proposed. One solution – provide minimum schedule guidance, and require offerors to propose development schedules based on program requirements and their development approach [USAF 2000].

Where users remain adamant that arbitrary delivery dates must be met, you will do well to work with them on the concept of evolutionary or incremental deliveries versus a full scope capability. Even then, it is recommended that you use every persuasive power at your command to educate them on the exceedingly high failure rate for programs with unrealistic schedules [USAF 2000].

### 5.6 Design Information Documentation

#### 5.6.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Contractor shall document and model the system or component (e.g., software, hardware, middleware) design information using industry standard formats, (e.g., Unified Modeling Language or UML), and how it will use tools that are capable of exporting model information in a standard format (e.g., Extensible Markup Language Metadata Interchange (XMI) and AP233/ISO 10303). The Contractor shall identify the proposed standards and formats to be used. The contractor shall maintain the design information, including any models used, so that it is current with the as-built system* [USN 2007a].

#### 5.6.2 Section M - Evaluation

#### 5.6.3 Section L - Instructions to Offerors

## 5.7 Information Development Environment (IDE)

### 5.7.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*Upon contract award, the contractor shall establish a program-wide integrated information development environment (IDE) that:*

*(a) Contains all program development information, including intermediate and final artifacts, both in-work and completed, developed and used as a part of the development activity, to include, at a minimum, all design data items, review materials (briefings and reports), technical reports and briefings, all software Metrics/measures reports, peer review reports, program schedules, and all Software Development Folders (SDF) (including all requirements, design documents, code, test cases, test results, and other items).*

*(b) Provides a web-enabled interface allowing continuous, real-time access (remote and local) to all items contained in the Integrated information development environment (IDE).*

*(c) For information maintained in special formats (such as within database tools used to manage requirements), access will be provided either via web-enabled tool interfaces or via remote tool invocation, or both, ensuring minimal user access delays.*

*(d) Provides continuous, real-time access for all stakeholders, including Government staff, contractor staff, subcontractors, Independent Verification and Validation (IV&V) activities, and others as necessary and appropriate.*

*(e) Segregates information according to need-to-know and security levels, protecting the enclaves using access controls and, if necessary, separate networks. For example, restricted and proprietary information can be kept private from subcontractors.*

*(f) Upon contract completion, the Integrated information development environment (IDE) shall be delivered to the Government as a CDRL* [USN 2008].

GENERAL RECOMMENDATION

If the Prime proposes a distributed development facility with each major subcontractor using their own processes, the risk resides in the ability of the prime to deploy an Integrated information development environment (IDE) and to integrate its overarching processes with the subcontractors' through an organizational and technical interface structure. If the Prime intends to execute a distributed development environment, its productivity will be lower at the start of the program unless it plans to implement the Information development environment (IDE) prior to award and train its subcontractors on the tools that it intend to use [SEI 2007b].

It is important for the acquirer to know and understand the risks arising from prime contractor / subcontractor process integration to properly monitor and manage these risks. As the two previous paragraphs indicate, there is a risk of lowered productivity early in the program for either approach. The RFP should request a plan from the prime contractor addressing this subject, and ensure that all activities and risks are captured in the Integrated Master Plan (IMP), Integrated Master Schedule (IMS), and Risk Management Plan (RMP) [SEI 2007b].

Process compatibility topics involve [SEI 2007b]

- ensuring a common vocabulary (i.e., what is the meaning of a HIGH risk exposure)
- ensuring consistent and compatible process goals
- ensuring efficient and clear bi-directional communication of process information
- ensuring a clear understanding of each other's processes

### 5.7.2 Section M - Evaluation

### 5.7.3 Section L - Instructions to Offerors

### 5.8 Integrated Master Plan Approach

#### 5.8.1 Section C - SOW/SOO; Requirements

#### 5.8.2 Section M - Evaluation

#### 5.8.3 Section L - Instructions to Offerors

EXAMPLE 1

Attachment CD2 to Volume IV: Integrated Master Plan (IMP) [USAF 2005]

*The IMP shall clearly and concisely state the Offeror's plans for executing the TMOS program from Authority To Proceed (ATP) through deployment. It will include descriptions of how management and systems engineering efforts will be conducted, how program tasks will be controlled and who, organizationally, will accomplish each task. It should identify key management and engineering tasks, their relationships to program milestones, and the specific criteria that will be used to track and measure successful task completion. Criteria to measure technical progress should include a set of Technical Performance Measures (TPMs). The IMP should provide top-to-bottom traceability from the CLINs to Level 4 of the CWBS, except for Software Development which shall be traced to Level 5. The IMP shall describe: a) key events and accomplishments to be achieved by the Offeror under the contract; b) the associated criteria for the events and accomplishments; and c) the processes to be used in performing and reporting the tasks required by the contract. The IMP shall also include a glossary. The Offeror shall prepare the IMP in a format which clearly and succinctly conveys to the Government the information requested above. Offeror format is encouraged for this document.*

*The IMP identifies the necessary Events, Significant Accomplishments, and associated Accomplishment Criteria to meet the intent of the Contractor Statement of Work (CSOW). As an event driven document, the IMP tracks program maturity and represents up-front planning and commitment, provides the basis for lower-tier planning, instills balanced design discipline, and provides a measure of progress in accomplishing TMOS Segment objectives. The IMP shall contain selected Narratives to correlate the required processes to the achievement of the Significant Accomplishments and Accomplishment Criteria. The IMP shall be a single plan for the entire effort, including associate and/or major subcontractor activities. The SOO, CSOW, IMP, IMS, and CWBS shall be consistent. This is a contractual document and can only be changed by mutual agreement of the parties.*

*The Integrated Master Schedule (IMS) provides the schedule information for execution of the IMP. The IMS is a contract deliverable item under the CDRL and is to be updated "as required" (to maintain schedule flexibility) in accordance with the requirements of the Offeror's CDRL.*

<u>*Events:*</u> *An Event is defined to be the initiation/conclusion of an interval of major program activity. It represents a decision point related to the system maturity with continued system development. Events may be identified in the format of entry and exit events (e.g. Initiate CDR and Complete CDR) or they may use entry and exit criteria for each event. As decision points for continued activity, Events shall clearly define expected maturity at a specific point in the program. Events shall be logically sequenced and may include demonstration milestones, major reviews, modeling and simulation results, product deliveries, and other*

*key decision points. The Contractor shall include definitions of each Event at the beginning of the IMP. The Offeror is encouraged to identify additional Key Events that best reflect the proposed program approach. Monthly Program Management Reviews, consisting of technical and management aspects, are held to keep the Government informed and facilitate timely problem resolution. Software Design Reviews (PDR and CDR) for software development shall be scheduled to reflect the Master Software Build Plan and delivery of major functionality. Likewise software testing events shall be similarly addressed. For each IMP event, there shall be one or more entry or exit Significant Accomplishments (entry or exit). The minimum set of Events identified by the Government are:*

1. *TMOS Post-Award Requirements Review*
2. *TMOS Segment Design Review*
3. *TSAT Phase B IPR-2*
4. *TMOS Preliminary Design Review (PDR)*
5. *TSAT Key Decision Point C*
6. *TMOS Critical Design Review (CDR)*
7. *TMOS Test Readiness Reviews (TRR) – Conducted at the prior to each major test to determine that test procedures are complete and to assure that the Offeror is prepared for formal testing.*
8. *TMOS Developmental Test and Evaluation*
9. *TMOS Operational Test and Evaluation*
10. *TMOS Acceptance Review for Deployment*
11. *TSAT IOC*
12. *TSAT FOC*

*Significant Accomplishments: A Significant Accomplishment is a specified result substantiating an event that indicates the level of progress or maturity directly related to each product/process. Accomplishments shall be measurable. Significant Accomplishments are interim or final critical efforts that must be completed prior to entering or exiting an event. Entry accomplishments reflect what must be completed to initiate an event. Exit accomplishments reflect what must be done for the event to be successfully closed and to demonstrate that the project is ready for the next event. Within each Event, Significant Accomplishments are grouped to ensure the IMP correctly addresses the interrelationships among functional disciplines. Significant Accomplishments shall provide sufficient Government insight into the process for achieving objectives of the SOO and CSOW. Significant Accomplishments shall be sequenced in a manner that ensures a logical path is maintained throughout the IMP. One or more Accomplishment Criteria shall define each Significant Accomplishment.*

*Significant Accomplishments may include:*

1. *A desired result at a specified Event, which indicates a level of design maturity (or progress) directly related to each product and process*
2. *A discrete step in a process.*
3. *A description of interrelationship between different functional disciplines.*

*Accomplishment Criteria:* *Accomplishment Criteria are definitive indicators of system maturity required to declare completion of a Significant Accomplishment. Accomplishment Criteria shall be tied to the completion of detailed tasks, shall be measurable, shall avoid the use of "percent complete," and shall avoid citing completion of data reports rather than results of data reports. Accomplishment Criteria shall include the use of Technical Performance Measures (TPM) and metrics to track detailed tasks in the IMS. The TPM and metrics information should include which measures will be flowed down to subcontractors and unless otherwise stated, the Government will have access to data on the TPMs and metrics listed in the IMP. Accomplishment Criteria may include:*

1. *The completion of specific detailed tasks.*
2. *The confirmation of the value of significant technical parameters.*
3. *The completion of documents, which provide results of in-process verification (successfully completed analysis or other testing activities).*
4. *The completion of critical activities required by the Contractor's program plans/operating instructions.*

*Narratives:* *Narratives are concise summaries providing visibility into the Offeror's key functional and management processes and procedures, how they relate to the integrated product development process, and an overview of the efforts required to implement them. The Narratives shall address only the key elements of implementing or developing a process/procedure (i.e. what the process will be and how it will be implemented and tracked). The Narratives facilitate Offeror and Government understanding of and commitment to critical processes/procedures prior to contract award. The Narratives shall complement the respective Significant Accomplishment and Accomplishment Criteria sections by indicating where in the particular process the criteria apply. Each narrative subject area shall include a brief objective statement of desired results traceable to the CSOW, the processes applicable to that objective, a listing of any Government, industry, national and international specifications and standards to be used achieve the objective. The Offeror shall clearly state which of these documents are compliance and which are reference and if they will be tailored. Compliance documents are contractually binding, while reference documents are for guidance only. The Software Development Plan will be a compliance document. Narratives shall not include rationale for using particular processes. The Narrative shall be consistent with applicable technical and management approaches described in the Mission Capability volume of the proposal.*

*The Offeror shall include the following process Narratives in the IMP (not listed in order of importance) and any others deemed critical to successful execution of the program. Each process Narrative shall include, as a minimum, processes encompassing all work tasks contained in the applicable WBS element:*

1. *Program Management. Define the processes to be used to plan, execute, track and control overall program progress with respect to cost and schedule to include staff allocation and EVMS planning. Provide decision-making flow within the team to include subcontractor management. Describe your communications strategy that discusses how information will be shared effectively across your team and with the Government, other TSAT segments and associate contractor teams. Outline the infrastructure (tools, Electronic Data Interchange (EDI), personnel, processes) necessary to accomplish the*

*strategy, including a team readiness assessment. Provide details of how classified information will be exchanged physically and electronically if proposed.*

2. *Systems Engineering. Define the processes to be used for conducting requirements analyses, performing functional analyses, allocating performance requirements, providing bi-directional requirements traceability, synthesizing design solutions, performing systems analysis and trade-off studies, and system test /requirements verification. Describe the methodologies that will be used in measuring progress, evaluating alternatives, selecting preferred alternatives, and documenting data and decisions. Include the processes to be used for conducting technical evaluations on critical products/documents to include government participation. Include Software Systems Engineering as part of the systems engineering processes as follows: Describe the role of software in TMOS design, development, test, operations and maintenance and your commitment to following the Software Development Plan.*
3. *Information Assurance Planning and Implementation. Define the processes to be used to design and integrate information assurance into the overall TMOS system. Include detailed plans and processes for certification activities.*
4. *Environmental Compliance. Define the processes to be used for integrating environmental protection considerations into the overall TMOS system architecture and engineering processes.*
5. *System Safety and Health. Define the processes to be used to develop a system-wide safety and health program that will ensure that safety and health requirements are identified and factored into the design of TMOS.*
6. *Network Architecture and Design. Define processes to be used for leveraging standards (IETF/ANSI), design processes (including prototyping and concept validation), following commercial best practices for service provider networks, and managing responsiveness to changes in GIG standards and Services network architectures.*
7. *Network Testing. Define processes to validate design and external interfaces throughout development, including the validation of elements of the network developed by other segments.*
8. *Mission Assurance. Define the processes to be used in conducting the mission assurance program for system hardware and software during design, development and test.*
9. *Development Test and Evaluation: Define the processes to be used in planning, conducting, and reporting Development Test and Evaluation.*
10. *Data Management. Define the processes to be used by which all program data (both technical and cost data) will be developed, maintained, and made available to the Government electronically. Include the processes for classified data.*
11. *Risk Management: Define the processes used across the project team to manage, identify, mitigate and track risks.*
12. *Integrated Logistic Support. Describe the logistics support analysis approach and how these processes will be used in developing supportable systems.*
13. *Configuration Control: Describe the processes for implementing configuration control throughout the program, to include subcontractors. Include information on interfaces to Government configuration management processes.*

*Each narrative subject area shall include, as a minimum, the following items:*

1. *Process Title*
2. *Objective: A brief statement of desired results, which is traceable to the Events.*
3. *Governing Documentation: The Governing Documentation lists the Government documents and/or established Offeror practices or procedures to be used to achieve the objective. The Offeror shall clearly state whether Government documents will be tailored and will reference, as required, the Applicable Documents section of the CSOW for tailoring.*
4. *Description of the processes.*
5. *Process owner (organization responsible for maintaining and training).*
6. *Process metrics that will be used to monitor the execution of the process. Unless otherwise stated, the government will have access to any of the metrics cited in this section.*
7. *Training given and planned to be given to support execution of the process.*

### 5.9 Management Plan Approach

#### 5.9.1 Section C - SOW/SOO; Requirements

#### 5.9.2 Section M - Evaluation

EXAMPLE 1

The proposal requirement will be met when the Offeror [USAF 2005]

> *Proposes an effective management/subcontractor team structure and plan that integrates the management/subcontractor team structure for successful program execution.*
>
> *Proposes a plan to obtain, and more importantly keep, highly skilled, effective personnel on the program, especially key personnel. The Offeror provides resumes of personnel in key positions that reflect experience needed to perform successfully.*
>
> *Proposes effective communications and collaboration with the Government and other segment contractor teams to manage program-wide integration and risk reduction efforts. The Offeror's strategy promotes near real-time information exchange, including access to all technical data (including classified data), within the TMOS contractor team and with the Government.*
>
> *Provides consistent program contract documentation. The IMS identifies critical paths and clearly provides buffer time to accommodate unexpected program events. The IMP should include details of metrics (including metrics from team members) that will be used to monitor contract performance and details which metrics will be available for government use. The Software Development Capability Evaluation (SDCE) responses must be consistent with the contents of the IMP.*
>
> *Proposes a plan to ensure the entire TMOS contractor team maintains a disciplined product development approach consistent with Capability Maturity Model Integration (CMMI) Maturity Level 3 or higher, including a plan to ensure this performance continues throughout the life of the contract. The tasks for ensuring this should be included in the IMP and the IMS. The plan should include which model you plan to use (e.g. CMMI-SE/SW, CMMI-SE/SW/IPPD/SS)* [USAF 2005].

#### 5.9.3 Section L - Instructions to Offerors

EXAMPLE 1

Proposal Requirement #x: Management Plan [USAF 2005]

> *Provide your overall management approach to successfully execute this program. Describe the proposed plan to monitor and evaluate overall program progress across all disciplines and team members. At a minimum, address the following topics: top level schedule, budget, earned value, resource allocation (including management of key personnel), funding perturbations, overall risk management approach, issue tracking and resolution, assumptions management, and near real time information exchange. Cite the management tools used to monitor and provide Government insight into the progress of the team's performance. Include an explanation for each tool proposed, explaining its intended utility, heritage, and expected benefit.*
>
> *Describe, in detail, the team structure, including the following:*

*Provide the team organizational chart(s) that show where all team members fit in the organization and the interdependencies, key relationships, and communication channels. Provide information on the IPT structure you plan to implement (to include government and other TSAT segments as appropriate). The IPT structure should include the structure you plan to employ to effectively lead the system level activities that have been allocated to TMOS for leadership. Within the team, identify key management and technical personnel (to include commercial network experience: see Section H, clause SMC-H017 for a definition of key personnel). Provide your plan for maintaining equivalent level of expertise for these positions throughout contract duration.*

*Describe your team's product development approach, including milestones. This approach should be disciplined and consistent with Capability Maturity Model Integration (CMMI) Level 3 or higher. Include your plan to integrate processes across team members and a description of and schedule for internal and/or external team-wide appraisals. The appraisals plan must include a team-wide Standard CMMI Appraisal Method for Process Improvement (SCAMPI) B level assessment to be performed no later than 9 months after contract award. This appraisal must be led by a Software Engineering Institute (SEI) authorized Lead Appraiser, external to the contractor's business unit, division, site, or program office. The plan should also include the approach for managing and resolving risks and weakness identified during the appraisals. For any appraisals already completed, include the Appraisal Disclosure Statement (ADS) that identifies the business unit/location appraised, the team conducting the appraisal, the credentials of the lead appraiser, a statement illustrating the independence of the team from the unit appraised, and the date of the appraisal. Also include any strengths or weaknesses identified during the appraisal and the plans/schedule for addressing the weaknesses.*

*Provide your subcontractor, associate contractor, and interdivisional team member management plan which identifies all team members in Atch MC3. Include at a minimum, their roles and responsibilities, location, leadership, capabilities/expertise of each to show why they were chosen to serve in that role and how they will be managed to ensure an effective program team.*

*Fully depict all Organizational Conflict of Interest (OCI) at Prime and Subcontractor levels. In Atch MC3 provide a comprehensive Organizational Conflict of Interest (OCI) integration plan including protective methods to prevent OCI with other TSAT-associated contractors.*

*Provide an Integrated Master Schedule (IMS), Integrated Master Plan (IMP), Contractor Work Breakdown Structure (CWBS), and Contractor Statement of Work (CSOW). Provide a mapping of the CSOW to the CWBS as requested in Atch MC1. Identify critical path(s) in the IMS including the relationship between any spiral (or incremental) builds and the risk reduction activities and milestone reviews. The IMP should include details of metrics that will be collected and made available to the Government, to include Technical Performance Measures (TPMs).*

## 5.10 Modular Open Systems Support Plan

### 5.10.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Contractor shall provide a modular open systems support plan for supporting the proposed* Modular Open Systems Approach (MOSA), *including, but not limited to, plans for integrating the systems under development both internally and externally, a strategy for maintaining the currency of the technology (through Commercial off-the-shelf software (COTS) and other reusable Non-Developmental Items (NDI) insertion, technology refresh strategies, and other appropriate means) and creation of different processes necessary to support* Modular Open Systems Approach (MOSA) [USN 2007a].

### 5.10.2 Section M - Evaluation

### 5.10.3 Section L - Instructions to Offerors

## 5.11 Operations and Maintenance

### 5.11.1 Section C - SOW/SOO; Requirements

### 5.11.2 Section M - Evaluation

### 5.11.3 Section L - Instructions to Offerors

| GENERAL RECOMMENDATION |
| --- |
| Include in the RFP the operations and maintenance requirement to deliver the test tools, drivers, and test data to the O&M organization [SMC 2004]. |

## 5.12 Past Performance Qualifications

### 5.12.1 Section C - SOW/SOO; Requirements

### 5.12.2 Section M - Evaluation

EXAMPLE 1

*Subfactor 1. Offeror's Open Architecture Past Performance Submissions* [USN 2007a]

*In assessing the Offeror's past performance submissions on similar contracts, the Government will consider how well the Offeror implemented XXX Open Architecture principles and used a modular open system approach, including:*

- *The degree to which the Offeror demonstrated that its design approach, plans for technology insertion, and sustainment strategy were consistent with the modular open systems requirements.*
- *The degree to which the Offeror managed the impact of changing requirements and evolving technology on the system's ability to continue to satisfy improved capabilities over time.*
- *The degree to which the Offeror's test and evaluation planning contained the means for testing the conformance to open standards to ensure the openness of key interfaces throughout the system life cycle.*
- *The degree to which the Offeror's approach contains capabilities to easily and quickly update, revise, and change the system as threats (warfighting and information assurance threats) or technologies Commercial off-the-shelf software (COTS) or reusable) evolve;* [USN 2007a].

EXAMPLE 2

*Past performance is a measure of the Government's confidence in the Offeror's, teaming partners, and major and critical subcontractors' performance on relevant contracts. The evaluation is based on, but not limited to, systems engineering, network design, information assurance (IA), network operations, ground control systems, protected and secure military communications, digital communications, past and present performance questionnaire, and software development capability such as the Software Engineering Institute's (SEI) Software Capability Evaluation (SCE) and the (Air Force Materiel Command) AFMC Software Development Capability Evaluation (SDCE) or equivalent, and commercial efforts.*

*Past performance will be evaluated by reviewing Contractor Performance Assessment Reports (CPARs) and information included by the Offeror on recent and relevant contracts. The Government may communicate with any other sources on any contract deemed relevant.*

*The main purpose of the past performance evaluation is to appropriately consider each Offeror's demonstrated record of contract compliance by supplying products and services that meet customer's needs, including cost and schedule.*

*(a) The recency and relevancy of the past performance information is critical in determining what contracts/programs should be evaluated and should be individually tailored to this acquisition. Recent performance will have greater impact on the performance confidence assessment than older performance. Recency is normally performance occurring within the last five (5) years. In determining relevancy, Offerors should make every effort to submit references from efforts*

*similar to the projected TMOS content. Offeror's contracts will receive a relevancy rating for each of the four subfactors. Subcontracts will receive a relevancy rating for the subfactor(s) identified in the proposal. Contracts focusing on experience with protected and secure, survivable communications systems and military/commercial network management will have the greatest weight.*

(b) *Offerors will be given the opportunity to address any negative or derogatory past performance information received during this evaluation (subject to the restrictions of FAR 15.306(e)(4)).*

*Past performance will be assigned one of the following ratings by the evaluation team:*

| ***TABLE 3 - PERFORMANCE CONFIDENCE ASSESSMENTS*** | |
|---|---|
| ***Rating*** | ***Description*** |
| *HIGH CONFIDENCE* | *Based on the Offeror's performance record, the government has high confidence the Offeror will successfully perform the required effort.* |
| *SIGNIFICANT CONFIDENCE* | *Based on the Offeror's performance record, the government has significant confidence the Offeror will successfully perform the required effort.* |
| *SATISFACTORY CONFIDENCE* | *Based on the Offeror's performance record, the government has confidence the Offeror will successfully perform the required effort. Normal contractor emphasis should preclude any problems.* |
| *UNKNOWN CONFIDENCE* | *No performance record is identifiable. See FAR 15.305(a)(2)(iii) and (iv).* |
| *LITTLE CONFIDENCE* | *Based on the Offeror's performance record, substantial doubt exists that the Offeror will successfully perform the required effort.* |
| *NO CONFIDENCE* | *Based on the Offeror's performance record, extreme doubt exists that the Offeror will successfully perform the required effort.* |

*In determining relevance, consideration will be given to similar technology, type of effort (development, maintenance, contract scope, schedule and type). Tables M4.5.1 thru M4.5.4 will be used as a guide for determining relevancy by Subfactor. These tables outline the criteria for evaluating contract relevance and provide performance assessment focus areas.*

### 5.12.3 Section L - Instructions to Offerors

EXAMPLE 1

> *Offerors shall also submit, as a part of their proposal, an* Software Development Plan (SDP) *rationale which describes why their specific approach is appropriate for the system to be procured and how their proposed processes are equivalent to those articulated by CMMI capability level 3* [USN 2007a].
>
> *Offerors shall submit a description of previous experience in developing software using the same or similar processes and approaches as proposed for this solicitation. Offerors shall describe the extent to which personnel who contributed to these previous efforts will be supporting this solicitation. Offerors shall also describe any previous CMMI or equivalent model-based process maturity appraisals performed. As a part of this description, offerors shall identify the organizational entity and location where the appraisal was performed, the type of evaluation, the organization performing the evaluation, and the level earned* [USN 2007a].

EXAMPLE 2

Relevant Past and Present Performance [USAF 2005]

General

> *Past and present performance information is required of the Offeror, major & critical subcontractors, and teaming partners proposed to perform key aspects of the effort the Offeror considers essential to overall successful performance.*
>
> *The information provided to the Performance Confidence Assessment Group (PCAG) in Volume V and responses to the Performance Questionnaire are two means used by the PCAG to obtain relevant past and present performance information. The Government reserves the right to obtain information from any other sources (e.g., Air Force CPARS) to assess Offeror's past and present performance. Problems not mentioned by the Offeror, but found by the PCAG during the course of assessing relevant past performance, may be addressed by the PCAG.*
>
> *Each Offeror with relevant performance information must send a Past Performance Questionnaire (Attachment 2) to at least two (2) points of contact (POCs) for each contract submitted with the Past Performance Volume. Preferred points of contact are, in order of descending preference: program or project manager, PCO, technical or engineering lead, or Administrative Contracting Officer (ACO). For Government programs, if the subcontractor's direct customer was another contractor, then the questionnaire shall be sent to the Government customer where applicable. For commercial contracts, the following order of precedence is suggested: program or project manager then contract manager. The Offeror shall send a standard transmittal letter (Attachment 2) to request that all POCs complete the Questionnaire. The points of contact shall return completed questionnaires via the instructions identified in the questionnaire.*
>
> *Past Performance information concerning subcontractors and/or teaming partners cannot be disclosed to a private party without the subcontractor's or teaming partner's consent. Because a prime contractor is a private party, the Government will need that consent before disclosing subcontractor/teaming partner past performance information to the prime during exchanges. In an effort to assist the PCAG in assessing the past performance relevancy and confidence, the Government requests that a consent form (Attachment 2) be completed by*

*each major and critical subcontractor and teaming partner identified in your proposal. The completed consent forms should be submitted as part of your Past Performance Volume V, Section 1 (not subject to page count limitation).*

*A separate copy of the client authorization letter(s) (Attachment 2) sent to each commercial POC, shall be included in Volume V (not subject to page count limitation) for the PCAG's use in case additional questionnaires need to be sent after submission of this volume. Copies of all remaining client authorization letter(s) shall be submitted within one week of proposal submission.*

*Early Proposal Information*

*Each Offeror is required to submit the Past Performance Volume, two (2) weeks prior to the date set for receipt of proposals.*

*Relevant Contracts*

*Submit Past Performance information on a maximum of five (5) recent contracts that the Offeror considers most relevant in demonstrating their ability to perform the proposed effort. Offeror's contracts will receive a relevancy rating for each of the four subfactors. Also, include information on a maximum of three (3) recent contracts performed by each of the Offeror's major & critical subcontractors and teaming partners that the Offeror considers most relevant in demonstrating their ability to perform the proposed effort. Include rationale supporting the assertion of relevance. The PCAG will assess an Offeror's relevant demonstrated performance as it relates to Mission Capability sub-factors, wherever possible: (Subfactor 1) Program Management and Systems Engineering, (Subfactor 2) Network Functions and Architecture, (Subfactor 3) Network Management and Operations, (Subfactor 4) Software Engineering, Development, and Management. The PCAG will assess performance for high, medium-high or medium relevance contracts only. Subcontracts will receive a relevancy rating for the subfactor(s) identified in the proposal. Additional details relating to how the PCAG will conduct its assessment and determine relevance are contained in Section M. – Evaluation Criteria, paragraph 4.5, Factor 3: Past Performance.*

*Note that the Government generally will not consider performance on a newly awarded contract without a performance history or on an effort that concluded more than 5 years prior to this source selection. If no relevant past or present performance information exists, do not submit a Volume V. Instead, explain in the proposal transmittal letter that no relevant past or present performance exists. We will treat an Offeror's lack of past performance as an unknown performance risk, having no positive or negative evaluative significance.*

*For the purpose of this solicitation, relevant past or present performance may be a part of any Federal, state, and local Government or their agencies' contract, or a commercial contract or subcontract.*

*Specific Content*

*Offerors are required to explain what aspects of the contracts are deemed relevant to the proposed effort and to what aspects of the proposed effort they relate. This may include a discussion of efforts accomplished by the Offeror to resolve problems encountered on prior contracts as well as past efforts to identify and manage program risk. The Offeror is required to clearly demonstrate management actions employed in overcoming problems and the effects of those actions, in terms of improvements achieved or problems rectified. For example, submittal of quality performance indicators or other management indicators that clearly support that an Offeror has overcome past problems is required. Categorize the relevance information into the specific Mission Capability sub-factors used to evaluate the proposal. Organize relevant past/present performance information in the following manner:*

*Section 1 – Volume Introduction*

*Provide a brief introduction to the volume and overview its organization.*

*Organizational Structure and Responsibilities. Describe the organizational structure for the participating divisions within the prime contractor and the submitted major & critical subcontractors and teaming partners. Summarize the responsibilities of each organizational member. Provide an estimate of the total dollar value each participant will expend.*

*Organizational Structure Change History. Many companies have acquired, been acquired by, or otherwise merged with other companies, and/or reorganized their divisions, business groups, subsidiary companies, etc. In many cases, these changes have taken place during the time of performance of relevant present or past efforts or between conclusion of recent past efforts and this source selection. As a result, it is sometimes difficult to determine what past performance is relevant to this acquisition. To facilitate this relevancy determination, provide a "roadmap" describing all such changes in the last 5 years, including all current and previous CAGE & DUNS codes, in the organization of the company, team partners and major subcontractors. As part of this explanation, show how these changes impact the performance of any efforts the Offeror identifies for past performance evaluation/performance confidence assessment. Since the Government intends to consider present and past performance information provided by other sources as well as that provided by the Offeror(s), the "roadmap" should be both specifically applicable to the efforts the Offeror identifies and general enough to apply to efforts on which the Government receives information from other sources.*

*Contract Data Matrix. Provide the following data for each relevant contract in matrix/data table form*

> *Contractor name and location of performing organization, including all current and previous CAGE codes and DUNS numbers.*
>
> *Name, address, telephone number, fax numbers and initial tracking status for: Procuring Contracting Officers, Contract Administrators, or Administrative Contracting Officers, Program, Project, or Subcontract Managers, Technical Representatives, and Other Cognizant Authorities (e.g. previous program managers, POCs, technical leads)*
>
> *Contract or subcontract number, name, type, and award date.*
>
> *Awarded cost/price and final (or projected) cost/price.*
>
> *Original delivery schedule and final (or projected) delivery schedule.*
>
> *Percentage of fee for each major period during the last 5 years for Fee or Incentive-type awards, together with rating and rationale.*
>
> *Questionnaire Tracking Record. Provide status of Past Performance Questionnaires.*
>
> *Consent/Authorization Forms. Insert consent forms and client authorization forms on all subcontractors and/or teaming partners.*

*Section 2 – Relevant Past and Present Performance (Prime Offeror)*

*This section contains relevant past/present performance, as described in Section L, paragraph 7.3, pertaining to the Prime Offeror. Limit this portion to five pages or less per contract or subcontract using the formatting instructions for the Offeror's proposal.*

*Description of Work: Provide a brief narrative for each contract or subcontract listed. Explain the nature of the work performed and how it is relevant to the TMOS effort in terms of technology, type of effort (development, production, maintenance), contract scope, schedule, and risk.*

*Relevancy Matrix. Complete a matrix for each contract or subcontract as shown in the example below. The left-hand column of the matrix contains rows for each of the critical Mission Capability (MC) sub-factors (SF1 Program Management and Systems Engineering, SF2 Network Functions and Architecture, SF3 Network Management and Operations, and SF4 Software Engineering, Development, and Management. The middle column rates the degree of relevance (Not Relevant = 0, Low = 1, Medium = 3, Medium-High = 4 or High = 5) that the Offeror feels the contract or subcontract has to the Mission Capability for this solicitation. Use the relevancy criteria described in Section M, paragraph 2.3, Factor 3: Past Performance, to do this rating. Leave the rating blank for any sub-factors that have no relevance. The right-hand column summarizes in two or three bullets the rationale for the relevancy rating. Text narrative in this section can be used to amplify the entries in the matrix.*

| ***TABLE 7.2 - RELEVANCY MATRIX*** | | |
|---|---|---|
| *MC Subfactor* | *Rating* | *Rationale for Rating* |
| *SF1* | *L* | *(2 or 3 bullets substantiating rating)* |
| *SF2* | *H* | *(2 or 3 bullets substantiating rating)* |
| *SF3* | *M* | *(2 or 3 bullets substantiating rating)* |
| *SF4* | *H* | *(2 or 3 bullets substantiating rating)* |

a) *Contract Performance. Describe contract performance in terms of the items listed in the Past Performance Questionnaire (Attachment 2). If the contract in question includes an Award Fee provision, provide award fee data for the entire period of performance. For any work that did not meet original cost, schedule, or technical performance and requirements, explain the reason(s) for the disparity and any corrective actions taken to avoid recurrence. Provide rationale as to why the price or delivery at the end varied from the beginning.*

b) *Lessons Learned/Best Practices. Describe any significant problems encountered on the subject contract, root cause of the problem, corrective action instituted, objective evidence that the corrective action worked, and preventive actions proposed for use on TMOS. If applicable, describe any unique or innovative approaches (Best Practices) used on this contract that proved to be effective.*

*<u>Section 3 – Relevant Past and Present Performance (Major and Critical Subcontractors)</u>*

*This section contains the same information on subcontractors as listed above for Section 2. However, the relevancy of each subcontractor past performance will be based on an assessment only against the Subfactor element(s) consistent with their role on the TMOS Offeror's Team.*

### 5.13 Process Maturity

#### 5.13.1 Section C - SOW/SOO; Requirements

#### 5.13.2 Section M - Evaluation

EXAMPLE 1

> *Factor x – Software development process experience* [USN 2007a]
>
> *Description: The Government will evaluate the offeror's previous experience in developing software using the same or similar approach as proposed for this solicitation. The results of any standard model-based process maturity appraisals performed within 24 months prior to proposal submission, and the number of proposed staff experienced in using these processes will be part of the evaluation criteria* [USN 2007a].

EXAMPLE 2

> *The Government will evaluate the software process by reviewing the offeror's Software Process Improvement Plan and by using the Software Engineering Institute (SEI) developed technique, the Standard CMMI Appraisal Methodology for Process Improvement (SCAMPI). The Government will determine the software process capability by investigating the offeror's current strengths and weaknesses in key process areas defined in the SEI report CMU/SEI-2006-TR-008 "CMMI for Development, Version 1.2"* [USAF 1996].
>
> *The Government will perform a SCAMPI on each offeror by reviewing current programs at the site proposed on this contract. The evaluation will be an organizational composite. It will be substantiated through individual interviews and reviews of documentation, of the offeror strengths and weaknesses in process areas relative to Maturity Level 3 (i.e., the extent to which an offeror meets or exceeds Maturity Level 3 criteria. The on-site appraisers may be separate and distinct from the proposal evaluation team and may include a Government contracting representative. The appraisal team will have been trained and experienced in the SCAMPI methods* [USAF 1996].

GENERAL RECOMMENDATIONS

Include capability evaluation as a criterion for selection [SEI SASS].

A SCAMPI can be used to support the Management Factor evaluation [SEI SASS].

Assure software processes defined by the offeror are reflected in the draft Software Development Plan (SDP), and in the submitted Integrated Master Plan (IMP) and Integrated Master Schedule (IMS), and that they include processes for handling (NDI) software, software as government furnished materials (GFM), and commercial off-the-shelf software (COTS)) software [SMC 2004]

To ensure the software process enacted for your program is predictable, repeatable, and manageable in terms of quality, cost, schedule, and performance, you should evaluate the offeror's software development capabilities prior to (or during) source selection. Remember, you are buying the process as well as the product! Performing a software development capability assessment will help you identify risks associated with the offeror's approach.

Risk identification is possible, since you will have:

1. An understanding of how the organization managed software development efforts in the past; and
2. The opportunity to compare past performance with the proposed software development process.

Therefore, you must pay due attention to the offeror's software development processes, starting with overall assessments, which focus on the details of tools, metrics, personnel facilities, management control, and language experience. Based on the maturity level of the selected contractor, you should consider customizing your contract to adapt that offeror's strengths and weaknesses. For example, if the contractor has achieved a high level of maturity (3 or above), you may decide that online access to the contractor's development environment and management status reports (e.g., cost, schedule, risk management and metrics data) is an effective alternative to the traditional oversight mechanisms of formal reviews and submission/approval of data items. Alternatively, if an offeror's process for coordinating the efforts of different engineering disciplines and stake holders is relatively weak, you may add a requirement for an on-site liaison to support coordination with users and the contractors developing interfacing systems [USAF 2000].

### 5.13.3 Section L - Instructions to Offerors

EXAMPLE 1

> *Offerors shall submit a description of previous experience in developing software using the same or similar processes and approaches as proposed for this solicitation. Offerors shall describe the extent to which personnel who contributed to these previous efforts will be supporting this solicitation. Offerors shall also describe any previous CMMI or equivalent model-based process maturity appraisals performed. As a part of this description, offerors shall identify the organizational entity and location where the appraisal was performed, the type of evaluation, the organization performing the evaluation, and the level earned* [USN 2007a].

GENERAL RECOMMENDATIONS

It is better to not list specific maturity levels from a specific model. Consider including information on the Process Areas instead [SEI SASS].

The five key software RFP elements are [USAF 2000]

- software development process
- contractor documentation and formats
- contractor control of baselines
- direct technical visibility
- proactive risk management

Software development process: A mature contractor process helps ensure that the contractor will produce supportable, quality software on schedule in a predictable, consistent manner. The contractor's practices must also be documented, maintained current by the development team, and be available for government review. This supports the need for continuous verification of process maturity and effectiveness [USAF 2000].

Contractor documentation and formats: Documentation deliverables should maximize the use of information in the form and format used to develop the software [USAF 2000].

Contractor control of baselines: Allowing the contractor to retain configuration and engineering control of baselines until they are stable, frees the developer from the government review and approval cycle which also supports partnering [USAF 2000].

Direct technical visibility: This may be implemented with the following requirements [USAF 2000]:

- The contractor must plan and implement a means for sharing software development information with the Government. The contractor should be required to provide access to current working documentation in the language and format normally used for software development. This includes Government access to software engineering tools and databases.
- Documentation, where possible, should reside in electronic format in the automated software engineering environment.
- The contractor must plan the information sharing mechanism so that little or no contractor assistance is required for Government personnel to access information. The information can be used as a basis for formal Government recommendations to the contractor, and whenever practical, should be used to simplify the formal technical review process. Thus, you need not provide formal approval of shared information on a day-to-day basis.

Proactive risk management: In the past, risk was reduced by requiring the delivery of a series of documents. Each deliverable was typically reviewed and approved by the Government to ensure quality and to independently verify contractor adherence to schedule. In principle, this document-driven contract monitoring was an efficient way to manage software development risk and perform program oversight. In practice, the oversight role progressively removed the developer from responsibility for design as each new document was approved. Since the Government performed the review and found the errors, the contractor only had to deliver a product on schedule and correct any errors the Government found. This approach too often led to increased reliance on testing and diffused the responsibility for quality problems, which often remained hidden until system delivery [USAF 2000].

### 5.14 Program Protection Plan and Information Assurance (IA)

#### 5.14.1 Section C - SOW/SOO; Requirements

#### 5.14.2 Section M - Evaluation

EXAMPLE 1

*The proposal requirement will be met when the Offeror:*

*Demonstrates a sound approach to implementing TSAT/TMOS Program Protection Planning as applied to the TMOS Segment, including the TSAT network, TGBE, TNOM element and TSAT Network Services element.*

*Proposes an effective approach for requirements identification, development, implementation, test, verification, and sustainment of IA, including key management planning. The proposal should reflect an understanding of how to document and operate a system that implements the Government's IA policies and Directives (DoD 8500 series).*

*Proposes an effective approach for the IA certification and accreditation processes.*

#### 5.14.3 Section L - Instructions to Offerors

EXAMPLE 1

Proposal Requirement #X: Program Protection Planning And Information Assurance (IA) [USAF 2005]

*Provide a detailed description of the Program Protection Planning (PPP) approach (with emphasis on Information Assurance and Systems Security Engineering (SSE)) for TMOS segment responsibilities, including the TSAT network design, TNOM design, and TSAT interfaces. Describe the approach for identifying candidate Critical Program Information (CPI) and Critical System Resources (CSR) for the TMOS segment. Describe the concept and processes for identifying, developing, implementing, and verifying IA (PPP and SSE) system and component requirements in the TMOS segment. Describe your approach for estimating, monitoring, and managing life cycle costs for PPP and SSE components throughout the TMOS segment.*

*Describe your approach for implementing the Government's PPP policies and directives that are applied to the TMOS segment. Describe candidate trade studies that may reduce identified vulnerabilities and mitigate risk(s) to the TMOS segment.*

*Describe your plans for IA certification and accreditation processes to include integrating IA vulnerability alerts (IAVAs), for the TSAT network and TMOS elements, including test and verification, and how certification and accreditation will be successfully achieved. Describe the resources needed to support security testing and verification. Include plans for interfacing with NSA and other Government personnel and organizations.*

*Describe your approach and rationale for the development of Information Assurance functions (including key management planning) for the TSAT network, TNOM, TGBE and TSAT Network Services.*

### 5.15 Software Development Plan (SDP)

#### 5.15.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*Within the SOW, there shall be a "Technical Approach" section. This section describes the XXX's expectations regarding the technical approach to be taken by the offerors. It is recommended that these expectations be based on the characteristics of the system to be developed and not mandate any specific approach, but rather define the criteria with which proposed approaches will be evaluated. In some cases, however, specific approaches may be required based on XXX needs and the system to be acquired* [USN 2007a].

*Within the "Technical Approach" section, there shall be a subsection titled "Software Engineering Approach," containing at a minimum the following language* [USN 2007a]:

*Software Engineering*

*The contractor shall define a software development approach appropriate for the computer software effort to be performed under this solicitation. This approach shall be documented in a (*Software Development Plan (SDP)*). The contractor shall follow this* Software Development Plan (SDP) *for all computer software to be developed or maintained under this effort* [USN 2007a].

*The* Software Development Plan (SDP) *shall define the offeror's proposed life cycle model and the processes used as a part of that model. In this context, the term "life cycle model" is as defined in IEEE/EIA Std 12207.O. The* Software Development Plan (SDP) *shall describe the overall life cycle and shall include primary, supporting, and organizational processes based on the work content of this solicitation. In accordance with the framework defined in IEEE/EIA Std. 12207.O, the* Software Development Plan (SDP) *shall define the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks. Because IEEE/EIA Std. 12207 does not prescribe how to accomplish the task, the offeror must provide this detailed information so the XXX can assess whether the offeror's approach is viable* [USN 2007a].

*The* Software Development Plan (SDP) *shall contain the information defined by IEEE/EIA Std. 12207.1, section 5.2.1 (generic content) and the Plans or procedures in Table 1 of IEEE/EIA Std. 12207.1. In all cases, the level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted. Information provided must include, as a minimum, specific standards, methods, tools, actions, strategies, and responsibilities associated with development and qualification* [USN 2007a].

#### 5.15.2 Section M - Evaluation

EXAMPLE 1

*At a minimum, the following three evaluation factors relating to the offeror's software development process shall be included in Section M* [USN 2007a].

Factor x – Software development approach [USN 2007a]

*Description: The Government will evaluate the offeror's proposed software development approach to ensure it is appropriate for the system to be developed and meets standard levels of completeness and process quality. For this evaluation, the Government will rely* *primarily on the draft* Software Development Plan (SDP) *and the* Software Development Plan (SDP) *rationale.*

*Criteria: IEEE/EIA Std. 12207.1, Section 4.2.3, H.3 – Characteristics of Life Cycle Data.*

Factor x – Software development experience [USN 2007a]

*Description: The Government will evaluate the offeror's previous experience in developing software of the same nature as that being acquired with this solicitation.*

Factor x – Software development process experience [USN 2007a]

*Description: The Government will evaluate the offeror's previous experience in developing software using the same or similar approach as proposed for this solicitation. The results of any standard model-based process maturity appraisals performed within 24 months prior to proposal submission, and the number of proposed staff experience in using these processes will be part of the evaluation criteria* [USN 2007a].

### 5.15.3 Section L - Instructions to Offerors

EXAMPLE 1

*The XXX shall request offerors to submit a draft version of their* Software Development Plan (SDP) *as part of their proposal package as well as a rationale for how the XXX justifies their process selection* [USN 2007a].

*"As part of the proposal, offerors shall submit a draft version of their* Software Development Plan (SDP) *in accordance with the content defined in the SOW. The* Software Development Plan (SDP) *may be formatted as desired by the offeror but must contain the information described but the* Software Development Plan (SDP) *DID. The* Software Development Plan (SDP) *is not page limited. An* Software Development Plan (SDP)*, if it is to-the-point and appropriate, may be preferable to a* Software Development Plan (SDP) *that is excessively wordy and contains non-essential material* [USN 2007a].

*"Offerors shall also submit, as a part of their proposal, an* Software Development Plan (SDP) *rationale which describes why their specific approach is appropriate for the system to be procured and how their proposed processes are equivalent to those articulated by CMMI capability level 3* [USN 2007a].

*Offerors shall submit a description of previous experience in developing software of the same nature as this solicitation. As a part of this description, the offerors shall describe the extent to which personnel who contributed to these previous efforts will be supporting this solicitation"* [USN 2007a].

*Offerors shall submit a description of previous experience in developing software using the same or similar processes and approaches as proposed for this solicitation. Offerors shall describe the extent to which personnel who contributed to these previous efforts will be supporting this solicitation. Offerors shall also describe any previous CMMI or equivalent model-based process maturity appraisals performed. As a part of this description, offerors shall identify the organizational entity and location where the appraisal was performed, the type of evaluation, the organization performing the evaluation, and the level earned"* [USN 2007a].

EXAMPLE 2

*Content for acquisition of systems software should be included in the RFP, such as* [SMC 2004]:

*For the acquisition of mission critical and support software, Section L of the RFP should require submittal of a draft (*Software Development Plan (SDP) *that defines the offeror's proposed software development processes to be applied during the program life cycle* [SMC 2004].

*Assure software processes defined by the offeror are reflected in the draft* Software Development Plan (SDP), *and in the submitted Integrated management Plan (IMP ) and Integrated Master Schedule (IMS), and that they include processes for handling NDI software, software as Government Furnished Materials (GFM), and Commercial off-the-shelf software (COTS)* [SMC 2004].

*The draft* Software Development Plan (SDP) *must cover the following topics:* [SMC 2004]

- *Organization – Who is responsible for each software development task (e.g., design, code, test, etc.) and what is the reporting chain of people and organizational groups* [SMC 2004]*?*
- *Management and Technical Controls – How will the software development be management and what management controls will be employed* [SMC 2004]*?*
- *Schedule and Milestones – What are the detailed schedule and specific milestones for the software development effort, and how do they relate to the overall systems development schedule* [SMC 2004]*?*
- *Status Monitoring – How will management know where the project is with regard to the schedules* [SMC 2004]*?*
- *Documentation – What documents will be produced and when? What formats will be employed and what automated facilities will be used? How will the documents be review and approved* [SMC 2004]*?*
- *Standards, Practices, and Guidelines – What specific internal standards, practices and guidelines will be followed in the design, code and test activities? How will this policy be enforced and how will the documents be reviewed and approved* [SMC 2004]*?*
- *Development and Test Resources – What support software and hardware is required and how will this software and hardware be obtained, maintained, and documented? Which of this software and hard is deliverable to the acquisition agency and how and when will it be delivered* [SMC 2004]*?*
- *Software Quality Assurance – What methods will be used for ensuring the integrity and quality of all software processes and products (e.g., reviews and walkthroughs, structured testing, automated analysis, etc* [SMC 2004]*?*
- *Error Reporting- How will errors in software products be documented? What accountability approaches will be used to make certain that all detected errors are corrected* [SMC 2004]*?*
- *Configuration Management – What software products will go under configuration control and when* [SMC 2004]*?*
    - *What configuration control boards will be established and who will make up these boards* [SMC 2004]*?*

- – *Will there be internal change control before formal Government change control* [SMC 2004]*?*

  *How will software configuration management interact with other system configuration management activities* [SMC 2004]*?*
- *Security – How will classified data and software products be controlled? How will hardware facilities be installed, controlled and operated to enable the processing of classified data* [SMC 2004]*?*

## 5.16 Software Documentation

### 5.16.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*Software documentation shall be utilized to plan, direct, explain, define, record, or provide information pertaining to the software development. The Developer shall prepare and maintain the software documentation and provide these documents electronically. In the event that the Government is unable to read the electronic media at the Government site, the Developer shall provide an alternate means for the Government to read the data* [Army 2006].

### 5.16.2 Section M - Evaluation

### 5.16.3 Section L - Instructions to Offerors

EXAMPLE 1

*The offeror shall also provide examples of software documentation (e.g., software specifications, source code listings, and software test report(s) prepared on other software development efforts* [SEI SASS].

### 5.17 Software Integrated Process Team

#### 5.17.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*Upon contract award, the Contractor and the Government shall jointly establish a Software Integrated Process Team. This team shall consist of contractor and Government representatives, and shall be co-chaired by the program office Chief Software Engineer and the contractor Chief Software Engineer (to include subcontractor Chief Software Engineers as appropriate). The Software Integrated Process Team should be tasked to define, document, monitor, and improve the software development approach being used for the software effort. Specifically, the Software Integrated Process Team shall:*

- *Define and document the software development approach to be used for the work effort. The approach is to be documented in the contractors' Software Development Plan* (SDP)*, which is to be based on the proposed* Software Development Plan (SDP) *submitted with the offeror's proposal.*
- *Secure Government approval for the* Software Development Plan (SDP)*. Approval is facilitated by having Government representatives serving on the Software Integrated Process Team.*
- *Identify and make process improvements to the software approach, and document these in the* Software Development Plan (SDP)*. These improvements are to be based on lessons-learned, suggestions from staff, industrial advancements, and other sources.*
- *Control all changes to the* Software Development Plan (SDP)*.*
- *Monitor development progress, assess effectiveness of the development approach, and monitor adherence to the defined process. One key mechanism for monitoring is attendance at technical reviews conducted in accordance with the* Software Development Plan (SDP) *and the Navy Technical Review process. Another is the use of a separately-scheduled process assessment review (Independent Technical Assessment (ITA)), conducted specifically to determine degree of adherence to the* Software Development Plan (SDP) *process and to assess the effectiveness of the* Software Development Plan (SDP) *as it is being applied.*
- *Monitor industry-wide lessons-learned, evolution of standards, advances in relevant technology, tool utility and availability, and other information that may prove to be valuable for the software work effort.*
- *Advise program management in areas relating to the software effort.*

*The Software Integrated Process Team is not responsible for management of the software effort, for performing software quality assurance, or for acting as an Independent Verification and Validation (IV&V) agent. The IPT however shall rely on existing program management and on the QA/IV&V function to provide sufficient information to facilitate their monitoring of progress and adherence to plan* [USN 2008].

#### 5.17.2 Section M - Evaluation

#### 5.17.3 Section L - Instructions to Offerors

## 5.18 Subcontractor Control

### 5.18.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The contractor is responsible for ensuring that the quality of all software, documentation, and programming materials procured from his subcontractors conform to the contract requirements* [MIL-STD-QQQ].

### 5.18.2 Section M - Evaluation

### 5.18.3 Section L - Instructions to Offerors

## 5.19 Support Planning

### 5.19.1 Section C - SOW/SOO; Requirements

GENERAL RECOMMENDATIONS

The SOW/SOO should define an objective for efficient, life-cycle software support consistent with total system requirements and should state that software supportability requirements and support characteristics are to be managed as an integral part of system development [SEI SASS].

Support planning addresses the development acquisition and entails request for proposal (RFP) development that provides for delivery of full documentation, data rights, and delivery of the software engineering environment (SEE used by the developer [USAF 2000].

The SOO defines an objective for efficient life-cycle software support consistent with total system requirements. The SOO states that software supportability requirements and support characteristics are to be managed as an integral part of system development [USAF 2000].

You should specify the following characteristics to ensure your software acquisition is supportable [USAF 2000]:

- Module size. Module size affects software supportability. Module size (a typical computer software component [CSC]) should generally not exceed 100 source lines of code (SLOC).
- Complexity. Application complexity affects software supportability. One generally accepted complexity measure is McCabe's Cyclomatic Complexity Measure, which should not exceed 10 for a given module.
- Programming language. The use of widely-accepted, higher-order programming languages to develop software enhances software supportability.
- Spare memory. The availability of installed spare memory improves software supportability. Spare memory permits the incorporation of enhancements and the correction of latent deficiencies. The effect of spare memory on supportability was calculated for the E-3 AWACS where two similar radars were delivered with 9 percent spare and 34 percent spare memory, respectively for the APY-1 and the APY-2. Measurements revealed a 3 to 1 difference in cost and schedule impact when making the same change to both E-3 radars.
- Spare computer throughput. The availability of installed spare throughput affects the software supportability by permitting the incorporation of enhancements and the correction of latent deficiencies.
- Spare computer system input/output. The availability of installed spare input/output affects software supportability.

### 5.19.2 Section M - Evaluation

GENERAL RECOMMENDATIONS

Consider making support a selection criteria [SEI SASS].

If licensing is an issue, this can be included as evaluation criteria [SEI SASS].

The higher the quality of the initial system, the easier it will be to support. Therefore, the offeror's approach to supportability must be a major source selection criterion [USAF 2000].

To ensure a prospective offeror's systems engineering and software development processes adequately address the supportability of software, it is imperative you carefully evaluate the offeror's software development processes during source selection [USAF 2000].

Software Development Plan (SDP). Require the submission of a Software Development Plan (SDP) with offerors' proposals that states how they intend to ensure their development process addresses supportability relative to the systems engineering process. This plan is evaluated during source selection [USAF 2000].

The way you structure the RFP to acquire and develop your initial software can profoundly impact the availability and usefulness of the required support environment. Therefore, you must require that all offerors describe their plans for supportability as part of their proposal submission [USAF 2000].

### 5.19.3 Section L - Instructions to Offerors

GENERAL RECOMMENDATIONS

The following supportability issues must be covered in the Instructions to Offerors [USAF 1996]:

- the methodology used to perform software sizing and cost estimating and the approach to be followed during software development
- the rationale used for computer resource timing and sizing estimates and description of how spare I/O utilization (channels or data rates), CPU throughput utilization, memory utilization requirements will be met
- a description of any teaming and subcontractor arrangements
- the skill levels required for computer resources development and their availability within the corporate structure
- the method to be used for risk control
- any planned use of firmware

- any plans for reusing or modifying existing software
- a clear definition of all assumptions used during proposal preparation
- plans for the development of prototype software
- plans and procedures for generating and using software metrics
- a disclosure statement of defect removal efficiency. This should include their definition of defects and what defects are included in the metric and the method of calculating the metric [USAF 1996].

Instructions to Offerors (ITO). The ITO and source selection evaluation criteria must specifically address those areas you consider critical processes. The evaluation criteria should describe what is required of the offerors' proposal and how it will be evaluated. The Aeronautical Systems Center has developed an RFP template which provides general and specific guidance on preparing the RFP for software-intensive systems [USAF 2000].

Your RFP must require that offerors plan for supportability by stipulating that the software be developed with a supportable architecture that anticipates change, uses accepted protocols and interfaces, and has documentation consistent with the code. This can only be achieved during initial software development and must be addressed upfront in the development contract. The higher the quality of the initial system, the easier it will be to support. Therefore, the offeror's approach to supportability must be a major source selection criterion [USAF 2000].

Whether a contractor maintains the software, or it is transitioned to in-house government maintainers, the maintainer must have the original developer's SEE and other essential tools for proper code maintenance. The following deliverables must be required [USAF 2000]:

- data rights to make and install changes
- source code and documentation adequate to understand the code
- computer resources (SEE, computers, compilers, etc.) needed to modify the source code and produce object code
- equipment and support software to test the subject code, to diagnose problems, and to test solutions, enhancements, and modifications
- equipment needed to distribute and install the new software
- a workable system to identify problems, resolve new requirements, and manage the support workload
- skilled personnel to perform required maintenance tasks [USAF 2000]

### 5.20 Systems Engineering Approach

#### 5.20.1 Section C - SOW/SOO; Requirements

#### 5.20.2 Section M - Evaluation

EXAMPLE 1

*The proposal requirement will be met when the Offeror proposes:*

*An effective approach for leading the effort to flow down and track network requirements, including updates, for the TSAT system. This should include ensuring the proper flow to the space, TMOS and terminal segment, to preliminary/revised interface control documents, and to segment and system test plans. The Offeror proposes comprehensive systems engineering supporting the generation of network requirements updates and the flowdown of TMOS segment requirements across and down to the elements, supportable components and associated interfaces.*

*Comprehensive systems engineering processes for development of TGBE (TSAT GIG Border Element) functions and interfaces.*

*Effective configuration management for maintaining a TMOS program baseline, including the TMOS specification tree.*

*Modeling and Simulation (M&S) plans that effectively address design, development, system integration and test, risk, and evolving requirements. The Offeror proposes an effective approach to validating models and disseminating program modeling results and simulation analysis with external segments and programs, including Space Segment and SE&I. The Offeror clearly explains an effective approach to performing system level network M&S.*

*Effective use of demonstration and prototyping to provide early risk reduction of requirements uncertainty, to evaluate TMOS concept and design alternatives, to evaluate TNOM user interfaces, and to obtain feedback from TSAT users and TNOM operators. The Offeror clearly explains, in the SEMP, a comprehensive and effective requirements maturation process used to manage the specification life cycle, from initial proposal through maturation into final specification(s). The plan explains how the maturation process effectively incorporates user feedback and technical performance assessment of demonstrations and prototypes. The plan clearly explains how requirements deficiencies are promptly identified, fully characterized, and appropriately remedied. The plan comprehensively identifies and characterizes existing requirements deficiencies, including those related to timing and performance.*

*The Offeror provides plans and processes for a test and verification program that address at a minimum: 1) The leadership of system level test activities for the network verification effort, including providing inputs and coordinating changes to the system level Verification Cross Reference Matrix / Requirements Verification Plans (VCRM/RVPs); 2) Support for TSAT SE&I test and verification planning, including support for development of the System Test and Verification Plan (STVP); 3) Development of TMOS segment and lower level VCRM/RVPs which support the system TRD and the TMOS TRD; 4) early systems integration testing; 5) The TMOS portion of TSAT to GIG interoperability testing and the TMOS portion of the Space and Terminal segment testing; and 6) Plans for testing COTS products.*

*An integrated logistics effort leading to an operationally suitable, sustainable support system infrastructure. The Offeror should demonstrate comprehensive planning for each element of*

*Integrated Logistics Support (ILS), placing special emphasis on the following topics: potential depot level maintenance in partnership with Government facilities, life cycle spare parts availability, and pre-operational support planning. The logistics effort should encompass all phases of the program, and be fully integrated into the System Engineering Management Plan (SEMP).*

*An effective systems engineering process describing the activities to be used on the program to ensure all TRD requirements translate into a TSAT network architecture and TMOS component systems and software architectures (TNOM, TGBE and TSAT Network Services). The systems engineering process should also describe the activities to flow these architectures into implementation, COTS selection, integration, and maintenance.*

### 5.20.3 Section L - Instructions to Offerors

EXAMPLE 1

Proposal Requirement #xx: System Engineering [USAF 2005]

*Describe your approach for effectively leading the effort to flow and track network requirements for the TSAT system, including providing recommended network requirement updates for the system TRD based on the approved network architecture. Include your processes for working with the SE&I, the other segments and other government organizations to perform this effort.*

*Provide in Attachment MC4 an initial Systems Engineering Management Plan (SEMP). Attachment MC4 should be prepared in accordance with paragraph 4.2.5.4. The SEMP will be evaluated in accordance with criteria in Section M, paragraph 4.3.1.*

*Describe your approach to defining and implementing intrasegment, intersegment, and TSAT external interfaces. The approach should include your processes for leading identified interface development tasks and for working with SE&I, other segments, and other government organizations. Describe your approach to leading the development of the following interfaces: common protocols and services, common managed network entity (MNE), TMOS to external Network Management System (NMS), TMOS to KMI/SMI, TMOS to GIG, and TMOS to external planning. Describe your approach to supporting development of the following interfaces (as required): TMOS to Space, TMOS to Terminal, TMOS to AEHF MCS (MPE), and Payload to Terminal.*

*Describe the approach to performing Modeling and Simulation (M&S) and analysis activities in support of TSAT network design, TNOM, TGBE and Network Services. For each of these components:*

> *Describe modeling, simulation, prototypes, test beds, executable demonstrations and other analysis tools necessary to perform systems engineering.*
>
> *Describe portions and/or characteristics to be simulated, the level of detail to which they will be simulated, and the specific M&S tools used to simulate and evaluate them.*
>
> *Explain how the tool set (including simulators) will be integrated and used to support evaluation of alternate architectures, requirements clarification and verification, performance prediction, technical trades, CONOPS development, risk reduction, design and development (including operational system testing) and human-machine interface design. Explain how modeling, demonstration, and prototype tools will be used to elicit user feedback and support the Offeror's proposed engineering analyses. Explain the*

*process by which such feedback and analyses will contribute to the delivery of complete, mature specifications.*

*Provide details regarding the processes, tools, and criteria used to monitor, assess, and validate the models.*

*Discuss your approach to integrating your M&S analysis activities with other segments and external interfaces.*

*Describe your plans for supporting SE&I verification of system level network requirements, architecture, and design. Describe your approach to leading TSAT edge-to-edge network (packet services) system integration, testing and verification as well as TMOS segment level testing. Describe your approach to provide support for Space and Terminal segment network testing. Describe your approach to supporting GIG interoperability testing.*

*Describe the systems engineering process for development of TSAT GIG Border Element (TGBE) functions and interfaces. This systems engineering process must include coordination with relevant external organizations including Space Segment, DISA, and GIG E2E working groups.*

*Describe your process for supporting the SE&I Test and Verification processes including, but not limited to, support of developing the STVP (including early inter-segment integration tests identified), system level VCRM/RVPs requiring TMOS support, and TMOS segment and below VCRM/RVPs that support system verification. This should include plans for any specific testing related to COTS products.*

## 5.21 Technical Management Process

### 5.21.1 Section C - SOW/SOO; Requirements

### 5.21.2 Section M - Evaluation

### 5.21.3 Section L - Instructions to Offerors

EXAMPLE 1

*This factor (subfactor) is met when the Offeror's proposal demonstrates* [DOD 2006]:

1. *The program tasks in the SOW are fully identified and include the technical tasks.*
2. *Technical planning is complete and supports implementation of the program's technical approach and accomplishment of the requirements and objectives contained in the RFP.*
3. *Technical and technical management processes are implemented across the program team, using appropriate and adequate tools.*
4. *The Offeror has implemented a technical baseline approach (functional, allocated, and product baselines) that support the program's technical approach. Data and software rights are clearly explained.*
5. *Technical processes are mature and stable and represent the Offeror's application of corporate enterprise processes and lessons learned.*
6. *Approach, tasks, processes, and procedures are flowed down to the subcontractors, vendors, and lowest level suppliers, as appropriate.*
7. *A trained workforce (familiar with the processes, practices, procedures, and tools) is available and in place to ensure accomplishment of the work.*
8. *Required professional certifications (such as IA required by DoD 8570.1) are held by offered personnel.*
9. *Technical events are included in the IMP/IMS and reflect the technical approach.*
10. *The IMP narratives include the technical and technical management processes and sub-processes (as appropriate).*
11. *The IMS clearly indicates the program's critical path(s) and has acceptable schedule risk.*
12. *Technical reviews are identified; explicit entry and exit criteria; participation established; and have the timing and frequency necessary to monitor and control technical baseline maturity and risk mitigation.*
13. *There is a single technical authority that is responsible for program technical direction. The lines of responsibility and authority are clearly established.*
14. *Key personnel are assigned and personnel resources identified.*
15. *The role of the Government (program office, supporting Government organizations, and user) along with the key subcontractors has been identified.*
16. *Program Integrated Product Team (IPT) is established that involves program participants and stakeholders for all Life Cycle phases and identify roles and responsibilities.*
17. *Program-specific plans represent a sound integrated technical approach. The plans are flowed down to the teammates, subcontractors, vendors, and lowest level suppliers on*

*the program. The planning is integrated across the SOW, SEP, IMP/IMS, and other program management plans and processes to support critical path analysis, EVM, and risk management.*

18. *The Offeror's SEP should thoroughly document the Offeror's technical approach to the integrated set of program requirements, technical staffing and organization planning, technical baseline management planning, technical review planning, and the integration with overall management of the program. It should clearly show how it is integrated, consistent, and aligned (but more detailed) with respect to the Government's SEP.*
19. *Proactive, disciplined SE technical management process leading indicators that provide a picture of future course that a program is likely to follow. The indicators should be measurable, map to incentive strategies and result in early identification and mitigation of risk* [DOD 2006].

## 5.22 Transition Plan

### 5.22.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall develop a Software Transition Plan (STRP) IAW DI-IPSC-81429A, and deliver IAW CDRL xxx. The plan shall address all aspects of transition from the development environment to a post-production life cycle support environment. The Developer shall provide the necessary user manuals, licenses, and training. The complete software engineering environment (the environment as it exists 30 days after the last two production units are produced) used in development of the software/firmware identified in the transition plan shall be transitioned to the Government for its ownership and use, or use by a third party, in performing software maintenance of the system. The Developer shall implement transition of the software IAW the Government approved Software Transition Plan* [Army 2006].

### 5.22.2 Section M - Evaluation

### 5.22.3 Section L - Instructions to Offerors

## 5.23 Treatment of Proprietary or Vendor Unique Elements

### 5.23.1 Section C - SOW/SOO; Requirements

### 5.23.2 Section M - Evaluation

### 5.23.3 Section L - Instructions to Offerors

EXAMPLE 1

*The Offeror shall justify any use of proprietary, vendor-unique, or closed components, including but not limited to Commercial off-the-shelf software (COTS)), and interfaces in current or future designs. This justification shall include documentation of the decision leading to the selection of specific Commercial off-the-shelf software (COTS) products (e.g. with test results, architectural suitability, "best value" assessments, etc.). The Offeror shall define its process for identifying and justifying proprietary, vendor unique or closed interfaces, code modules, hardware, firmware, or software to be used* [USN 2007a].

a. *The Offeror shall describe how it will employ hardware and/or software partitioning or other design techniques to isolate all proprietary, vendor unique portions of interfaces, hardware, firmware and modules – at the lowest subsystem or component level.*

b. *The proposal shall include documentation to support the rationale for a decision to integrate a proprietary, vendor unique or closed system hardware and/or software functions within the proposed system.*

c. *The Offeror shall describe how the integration of closed or proprietary, vendor-unique equipment, interfaces, data systems or functions due to a unique or specific system requirement will not preclude or hinder other component or module developers from interfacing with or otherwise developing, replacing, or upgrading open parts of the system.*

d. *The Offeror shall identify and take steps to prevent the open elements of the system from intertwining with proprietary or vendor-unique elements in a manner that restricts or limits the ability to replace or upgrade the open elements using an open competitive selection process.*

e. *The Offeror shall describe and demonstrate that the modularity of the system design promotes identification of multiple sources of supply and/or repair, and supports flexible business strategies that enhance subcontractor competition.*

   i. *The Offeror shall conduct a market survey to identify candidate Commercial off-the-shelf software (COTS) and other reusable NDI, including Government Intellectual Property (IP) assets, capable of achieving the performance requirements of solutions that it has proposed to custom build. Commercial off-the-shelf software (COTS) and other NDI selection criteria shall, at a minimum, address the following factors:*

      - *Electrostatic Sensitive Device (ESD) immunity;*
      - *Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC);*
      - *Integrated Logistics Support requirements;*
      - *Safety; Reliability (to include the hardware's designed-in ability to accommodate such stresses as electrical power fluctuation (voltage, current, frequency)), temperature, shock, vibration, operating time (duration),*

*changes in atmospheric pressure, and humidity consistent with the environment described in the System Specification;*

- *Maintainability;*
- *Subsystem performance trade-offs;*
- *Power, cooling, and physical form factors;*
- *Open system architecture break out compatibility;*
- *Cost;*
- *Manufacturer's* Quality Assurance *provisions;*
- *Market acceptability;*
- *Obsolescence;*
- *Adequacy of available technical and intellectual property data and re-procurement data rights on the product; and*
- *Merits of the software supported by the product.*

*The Offeror shall provide documentation of the decision leading to the selection of specific Commercial off-the-shelf software (COTS) products (e.g. test results, architectural suitability, "best value" assessments, etc.).*

*ii. The Offeror shall identify those pre-existing items (Government Intellectual Property (IP) assets, NDI, Open Source Software, and Commercial off-the-shelf software (COTS)) it intends to evaluate for reuse. At a minimum, the Offeror shall describe what artifacts from the repositories/libraries that will be made available to Offerors will be inserted] it intends to use within its proposed solution. Exceptions regarding reuse of pre-existing items must be accompanied by justification, such as cost (both of adoption and life cycle support), schedule, functional and non-functional performance, etc.*

*f. The Offeror shall address how it will provide information needed to support third party development and delivery of competitive alternatives or designs for software or other components or modules on an ongoing basis. This information may be used as part of peer review processes, to support the Integrated Product Team (IPT), and to facilitate competition for component suppliers. The Offeror will provide a list of those proprietary or vendor-unique elements that it requests be exempt from this review* [USN 2007a].

# 6 Safety-Critical Software

The Safety Critical Software section provides RFP language examples that ensure that safety-related appropriate processes, technical methods, and engineering are implemented during the system design and development (SD&D) phase. It will identify the data and artifacts (documents, code, etc.) required by the Software Engineering Directorate (SED) to assess software safety, and make a software-safety recommendation for system testing or deployment. The SED Software Safety Assessment Process recommended in the Program Manager Handbook for Software Safety (PMHSS) is based upon the numerous standards and procedures utilized by government agencies and industry that are concerned with safety-critical systems [Army 2006].

## 6.1 Flight Readiness Review (FRR)

### 6.1.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*An Flight Readiness Review(FRR) shall be conducted no later than 60 days prior to the first flight, prior to any subsequent flight for which the configuration of the air vehicle or software has significantly changed, and prior to conducting flight test activities for purposes that have not been approved in previous flight readiness reviews. The FRR shall ensure that all airworthiness prerequisites have been addressed and met, hardware and software are sufficiently mature to warrant proceeding with flight testing, and no undue risks are apparent in early flights. The detail of the data shall be such that it supports issuance of a Contractor Flight Release (CFR) and/or Airworthiness Release (AWR) by the Government. Agenda items to be addressed in the Flight Readiness Review (FRR) include but are not limited to the following* [Army 2003]*:*

1. *Evaluation of component and subsystem tests, test failures, and corrective actions.*
2. *Evaluation of management procedures for flight operation.*
3. *Evaluation of emergency operational procedures.*
4. *Evaluation of established flight abort criteria*
5. *Evaluation and assurance that the prerequisites for first flight have been met.*
6. *Evaluation of test instrumentation.*
7. *Evaluation of ground and flight Safety practices and procedures.*
8. *Evaluation of test objectives.*
9. *Evaluation of the software updating process during flight testing.*
10. *Software Version Description.*
11. *Software Test Report.*
12. *System Integration Test Results.*
13. *System Safety Hazard Analysis Report.*
14. *Safety Assessment Report.*
15. *Software Failure Modes, Effects, and Criticality Analysis Results* [Army 2003]

### 6.1.2 Section M - Evaluation

### 6.1.3 Section L - Instructions to Offerors

## 6.2 Hazard and SFMECA Testing

### 6.2.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall perform unit level Hazard and Software Failure Modes, Effects, and Criticality Analysis (SFMECA) test analysis to determine whether the software responds correctly to postulated hardware anomalies as documented and agreed upon during the design Hazard and SFMECA analysis. The Developer shall conduct hazard testing analysis to ensure that all system hazards that trace to software have been tested and that the software performs as specified in the SRSs (Note: in some cases this analysis may be deferred to system testing). The Developer shall perform Flight Qualification Test (FQT), or system testing to determine that the software correctly responds to postulated hardware anomalies, as agreed upon during the design and coding Hazard and SFMECA analysis, if the testing is not performed during code and unit test. The Developer shall prepare and document the methods to accomplish the hazard and SFMECA testing in the STP and* Software Test Description (STD), *and document the results of this hazard and SFMECA testing in the Software Test Report (STR)* [Army 2006].

### 6.2.2 Section M - Evaluation

### 6.2.3 Section L - Instructions to Offerors

## 6.3 Hazard Criticality Matrix

### 6.3.1 Section C - SOW/SOO; Requirements

### 6.3.2 Section M - Evaluation

### 6.3.3 Section L - Instructions to Offerors

**Software Hazard Criticality Matrix**

| Control Category | Severity | | | |
|---|---|---|---|---|
| | Catastrophic | Critical | Marginal | Negligible |
| (A) Software exercises autonomous control over potentially hazardous systems / components without intervention to preclude the occurrence of a hazard. Failure of software or a failure to prevent an event leads directly to a hazards occurrence (including critical information provided to the pilot). | 1 | 2 | 3 | 5 |
| (B) Software exercises control over potentially hazardous hardware systems / components allowing time for intervention by independent safety system to mitigate the hazard. However, these systems by themselves are not considered adequate. | 1 | 2 | 3 | 5 |
| (C) Software item displays information requiring immediate operator action to mitigate hazard. Software failure will allow or fail to prevent the hazard's occurrence (disabling an aiding function). | 2 | 3 | 4 | 5 |
| (D) Software items issues command over potentially hazardous hardware system or components requiring human action to complete the function. There are several redundant, independent safety measures for each hazardous event. | 3 | 3 | 5 | 5 |
| (E) Software generates information of a safety critical nature to make safety critical decisions. There are several redundant safety measures for each hazardous event | 3 | 4 | 5 | 5 |
| (F) Software does not control safety critical hardware systems or components and does not provide safety critical information. | 5 | 5 | 5 | 5 |

High Risk - Significant Analyses and Testing Resources (SHCI = 1)

Medium Risk - Requirements and Design Analyses and Depth Testing Required (SHCI = 2)

Moderate Risk - High Levels of Analysis and Testing Acceptable With Managing Activity (SHCI = 3)

Minor Risk - High Level of Analysis and Testing Acceptable With Managing Activity Approval (SHCI = 4)

Low Risk – Acceptable (SHCI = 5)

[Army 2006]

### 6.4 Safety-Critical Software - Developer Design Reviews

#### 6.4.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The Developer shall conduct periodic reviews with the Government during the program to establish a foundation for Safety substantiation and assure compliance with all Safety requirements. A proposed agenda shall be transmitted to the Government No Later Than (NLT) 15 days prior to each review. The following reviews are suggested. Proposed alternatives are encouraged if greater efficiency can be achieved. The Contractor shall prepare minutes IAW DI-ADMN-81505 and deliver IAW CDRL xxx for all software reviews* [Army 2006].

*Kick-Off Meeting. The Developer will host the Kick-Off Meeting at their facility. This meeting will take place approximately 30 (NLT 45) days after contract award. Agenda items to be addressed in the Kick-Off Meeting include but are not limited to the following* [Army 2006]:

1. *Draft System Specification for the ABC.*
2. *Draft* Software Development Plan (SDP).
3. *Technology Readiness Report and Technology Transition Plans.*
4. *Software Safety Program Plan.*
5. *Preliminary Hazard Analysis.*
6. *Baseline IMS.*

*Software Specification (Requirements) Review. The Software Specification (Requirements) Review (SSR) is intended to define the system requirements in detail that have been allocated to the software configuration items in the System/Subsystem Design Description (SSDD). The SSR shall be held NLT XY days after contract award to* [Army 2006]*:*

1. *Ensure that the software requirements correctly and completely specify the system requirements allocated to the software.*
2. *Identify each Computer Software Configuration Item (CSCI)/Partition (as defined by ARINC 653-1) that implements system Safety requirements.*
3. *Identify and justify the Software Hazard Criticality Index (SHCI) value for each CSCI/Partition.*
4. *Identify any software hazards resulting from the specification of derived software requirements and secure agreement that the software mitigation of hazards is appropriate.*
5. *Assess the requirements with respect to their compliance with the system and subsystem hazards mitigation and system Safety requirements.*

*Agenda items to be addressed in the SSR include but are not limited to the following:*

1. *Preliminary Software Requirements Specification (SRS).*
2. *Preliminary Interface Requirements Specification (IRS) .*
3. *System/Subsystem Design Description (SSDD).*

4. *The updated technology readiness assessment and technology transition plans.*
5. *Requirements Compliance Matrix.*
6. *Requirements Verification Matrix.*
7. *Interface Control Document (ICD).*

*Preliminary Design Review. The Preliminary Design Review (PDR) is intended to finalize the architecture of the software documented in the Software Design Document for the ABC. The Developer will host the PDR at their facility. The PDR shall be held to* [Army 2006]*:*

1. *Ensure the design approach complies with performance specification requirements, design criteria, airworthiness qualification, and other contract requirements.*
2. *Provide an understanding of the design and its implementation of the SRS.*
3. *Provide the Government access to the software trouble report database as applicable.*

*Agenda items to be addressed in the PDR include but are not limited to the following* [Army 2006]:

1. *Baseline ABC Displays.*
2. *Design Detail and Interface Issues.*
3. *Preliminary System Safety Hazard Analysis (SSHA) Report.*
4. *Draft Derived Safety Requirements.*
5. *Revised (as required) Software Hazard Criticality Index (SHCI) values for the CSCI/Partition.*
6. *Requirements Compliance Matrix (Software and Hardware).*
7. *Requirements Verification Matrix.*
8. *Top Level Hardware/Software Design.*
9. *Updated technology readiness assessment and technology transition plans.*
10. *Final SRS Review.*
11. *Final IRS Review.*
12. *Draft Software Design Description (SDD).*
13. *Draft Interface Design Document (IDD).*
14. *Draft Software Test Plan (*Software Test Plan (STP)*).*
15. *Top Level Software Safety Critical Functional Analysis (SSCFA).*
16. *Status and presentation of resolutions for all Software Specification (Requirements) Review (SSR) action items.*
17. *Explanation of any open ECRs and PCRs against software requirements.*
18. *Software architecture, including top-level CSCI structure and evidence that the following considerations are incorporated in the software design:*

    *a. compatibility with the high-level requirements,*

    *b. consistency,*

    *c. compatibility with the target computer,*

    *d. verifiability,*

*e. conformance to standards,*

*f. partitioning integrity, and*

*g. incorporation of necessary logic affecting system Safety.*

19. *Computer resource allocation, including:*

    *a. timing,*

    *b. sequencing requirements,*

    *c. relevant equipment constraints used in determining allocation, and*

    *d. tasking strategy/process control prioritization scheme and diagrams.*

20. *Executive control and start/recovery features of each CSCI.*
21. *Computer software development facilities, software development tools, test tools.*
22. *Design features providing for life-cycle software supportability.*
23. *Review of all software management and quality metrics.*
24. *Update of software milestone schedule.*
25. *Update of identified risk areas and risk mitigation measures.*
26. *Results of software quality and process audits and measurement of software quality metrics as provided for in the* Software Quality Assurance (SQA) *Plan.*

*In-Process Reviews (IPR). The Developer shall present the status of the ABC development effort during scheduled in-process reviews (IPR) ) beginning after SSR. Software development activities, metrics, and status will be presented at the IPR* [Army 2006].

*Critical Design Review. The Critical Design Review (CDR) is intended to finalize the software detailed design, and establish Developer's release of the detailed SDD for the ABC. Agenda items to be addressed in the CDR include but are not limited to the following* [Army 2006]:

1. *Preliminary Safety Assessment Data.*
2. *Final version of software design documentation that includes the SDD and the detailed software IDD.*
3. *Identification of all system hazards with software impacts and their resolution.*
4. *Updated software/system hazard analysis and causal factor analysis.*
5. *Final version of the SFMECA.*
6. *Detailed SSCFA at Computer Software Unit level.*
7. *Status and presentation of resolutions for all PDR action items.*
8. *Explanation of any open PCRs against software requirements.*
9. *Software architecture, including assignment of CSCI requirements to specific lower-level software components and units.*
10. *Updated technology readiness assessment and technology transition plans.*
11. *Overall information and control flow between software units, and sequencing of software operations.*

12. *Language standards; specifically Language Safe Subsets Analysis and Standards.*
13. *Evidence that the following considerations are incorporated in the software design* [Army 2006]*:*

    *a. compatibility with the high-level requirements,*

    *b. consistency,*

    *c. compatibility with the target computer,*

    *d. verifiability,*

    *e. conformance to standards,*

    *f. partitioning integrity,*

    *g. incorporation of necessary logic affecting system Safety, and*

    *h. data coupling and control coupling analysis.*
14. *Results of activities to determine processor throughput, memory, and bus utilization with respect to computer resource allocations, including* [Army 2006]*:*

    *a. timing,*

    *b. sequencing requirements,*

    *c. relevant equipment constraints used in determining allocation, and*

    *d. tasking strategy/process control prioritization scheme.*
15. *Computer software development facilities, software development tools, test tools* [Army 2006].
16. *Design features providing for life-cycle software supportability* [Army 2006].
17. *Review of all software management and quality metrics* [Army 2006].
18. *Update of IMS* [Army 2006].
19. *Update of software development schedule* [Army 2006].
20. *Update of identified risk areas and risk mitigation measures* [Army 2006].
21. *Results of software quality and process audits and measurement of software quality metrics as provided for in the* Software Quality Assurance Process (SQAP) [Army 2006].

*The CDR date shall be identified on the IMS. The Developer will host the CDR at their facility. The CDR shall be conducted prior to release for hardware production and/or prior to the initiation of software coding. The CDR shall be conducted to determine the characteristics of the design, and to ensure incorporation of requirements prior to commitment for implementation* [Army 2006].

*Test Readiness Review (TRR). The Test Readiness Review (TRR) is intended to determine that the software has reached a state of maturity to make it worthy of completion and that the Flight Qualification Test (FQT) environment is suitable for performing a successful FQT. The TRR shall be held NLT 30 days prior to the start of FQT. Agenda items to be addressed in the TRR include but are not limited to the following* [Army 2006]:

1. *Test results of software integration, informal Flight Qualification Test (FQT), software hazards, and SFMECA testing.*

2. *Status of the Software Test Plan (STP) and Software Test Description (STD) and detailed procedures.*
3. *Status of user manuals (e.g., Firmware User's Manual, Software User's Manual, etc.).*
4. *Status of software adaptation and calibration data.*
5. *Status of the SRSs, SDDs, ICDs, IRSs, IDDs, and all associated change proposals.*
6. *System and Software Hazard Tracking Report.*
7. *Status of the Flight Qualification Test (FQT environment including FQT required test data, data generation capabilities, all data and test environment simulation capabilities, and System Integration Laboratories.*
8. *Review of the applicable Software Development Plan (SDP) and STP, including discussion of any changes affecting sequence of testing leading up to and including Flight Qualification Test (FQT, and Structural Coverage Analysis/Testing report.*
9. *Status of the Software Test Description (STD), including detailed procedures.*
10. *Test results of software integration, software hazards, and SFMECA testing.*
11. *Status of the test environment, including FQT required test data, data generation capabilities, all data and test environment simulation capabilities, and system integration laboratories.*
12. *Results of software quality and process audits and measurement of software quality metrics as provided for in the Software Quality Assurance Process(SQAP).*
13. *Presentation of evidence that required levels of structural coverage analysis and hazard testing is provided for in the unit, integration, FQT, and/or system tests.*
14. *Final Technology Readiness Assessment Report and status of the Technology Transition Plans efforts.*

*Safety Assessment Review. A Safety Assessment Review (SAR) shall be conducted no later than 60 days prior to the first Integration, Operations, Test, and Evaluation (IOT&E), prior to any subsequent IOT&E for which the configuration of the system or software has significantly changed, and prior to conducting IOT&E test activities for purposes that have not been approved in previous SARs. The SAR shall ensure that all Safety prerequisites have been addressed and met, hardware and software are sufficiently mature to warrant proceeding with IOT&E testing, and no undue risks are apparent in previous tests. The detail of the data shall be such that it supports the approval of the PMO Safety Officer. Agenda items to be addressed in the SAR include but are not limited to the following* [Army 2006]*:*

1. *Evaluation of component and subsystem tests, test failures, and corrective actions.*
2. *Evaluation of management procedures for system operation.*
3. *Evaluation of emergency operational procedures.*
4. *Evaluation of established system abort criteria.*
5. *Evaluation of test instrumentation.*
6. *Evaluation of Safety practices and procedures.*
7. *Evaluation of test objectives.*
8. *Software Version Description.*

9. *Software Test Report.*
10. *System Integration Test Results.*
11. *Software/Subsystem Hazard Analysis (SSHA) Report.*
12. *Hazard Causal Factor Analysis (HCFA Report).*
13. *SFMECA Results.*
14. *Status of Engineering Change Proposals and Software Problems.*
15. *Evidence of certification for software not developed or modified under this contract but certified under some other contract or by another authority.*

*Production Readiness Review. The Production Readiness Review (PRR) is intended to obtain the Government's approval of the developed product. The Developer will host the PRR at their facility per the Integrated Master Schedule (IMS). Agenda items to be addressed in the PRR include but are not limited to the following* [Army 2006]*:*

1. *Changes in ABC Design.*
2. *Developer's release of the Technical Data Package (including source code, executable system, initialization, and calibration data) and related CDRL Documentation.*
3. *Any Changes to Interface or Detail Specifications.*
4. *Qualification Results from Government Testing.*
5. *System Test Results.*
6. *Developer Test Results.*
7. *Functional Configuration Audit Results.*
8. *Physical Configuration Audit Results.*
9. *Software Version Description.*
10. *Updated Technology Readiness Assessment Report and the Implementation Results of the Technology Transition Plan(s).*
11. *Hazard Analysis Report.*

### 6.4.2 Section M - Evaluation

### 6.4.3 Section L - Instructions to Offerors

## 6.5 Safety-Critical Software - Failure Analysis

### 6.5.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall implement a Failure Reporting, Analysis, and Corrective Action System (FRACAS) to track test failures during qualification testing, in-house testing, and production. FRACAS reports shall be detailed down to the lowest level necessary to determine the true root cause of a failure and to assure adequate corrective action has been instituted. The Government shall be notified of a test failure within three days of the subject failure. The Developer shall prepare the FRACAS report IAW DI-RELI-81315 and deliver IAW CDRL xxx. During production, ABC units scheduled for delivery shall be held until the FRACAS Report is approved by the Government* [Army 2006].

### 6.5.2 Section M - Evaluation

### 6.5.3 Section L - Instructions to Offerors

### 6.6 Safety-Critical Software - Hazard Causal Factor Analysis

#### 6.6.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The Developer shall prepare a Hazard Causal Factor Analysis (HCFA) IAW DI-MISC-80711A and deliver IAW CDRL. The purpose of the HCFA is to* [Army 2006]*:*

1. *Identify each specific cause which contributes to the hazard, including hardware, software, human error, and software influenced error potential causes.*
2. *Identify which hazard causes(s) are contributors to the hazard from across interface boundaries (across subsystem interfaces and between contractors).*
3. *Identify specific functional requirements to mitigate each causal factor to a level of acceptable risk. This includes hardware, software, protective equipment, warnings and cautions, training, and technical manual requirements.*
4. *Identify specific design, test, and verification requirements to provide evidence that the original design requirements have been successfully implemented in the design and code.*

*The System Safety Analysis Handbook (SSS-SSAH-1997) may be used as a guide in performing the analysis and preparation of the Hazard Causal Factor Analysis (HCFA)* [Army 2006].

#### 6.6.2 Section M - Evaluation

#### 6.6.3 Section L - Instructions to Offerors

### 6.7 Safety-Critical Software - Identification

#### 6.7.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall identify the software elements that perform functions related to system hazards and specify these elements as Safety critical. In addition, the Software Requirements Specification (SRS) shall specify those system Safety requirements allocated to the software elements, as well as derived software requirements related to system and subsystem hazards* [Army 2003].
>
> *The Developer shall perform a software hazard analysis and identify the Software Hazard Risk Index (SHRI) value for each software element (Computer Software Configuration Item (CSCI) and Computer Software Unit/Package) that implements Safety Requirements in the SRS. The SHRI analysis shall be performed as specified in FSAQAP, Appendix L. Each software element that has been assigned an SHRI value of 1 through 4 shall be defined as being Safety critical. In addition, each software element that has been assigned an SHRI value of 5 shall be defined as Safety critical if it* [Army 2003]:
>
> 1. *Provides data or performs a function required by software elements that have been assigned an SHRI value of 1 through 4, or*
> 2. *Is not partitioned such that it can interfere with the reliable and correct operation of software elements that have been assigned an SHRI value of 1 through 4* [Army 2003].

#### 6.7.2 Section M - Evaluation

#### 6.7.3 Section L - Instructions to Offerors

## 6.8 Safety Critical Software - Incremental SW Product Delivery

### 6.8.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall deliver incremental drops (Builds) of the latest software products for evaluations IAW DI-MCCR-80700 and deliver IAW CDRL xxx. The Developer shall coordinate with the Government to establish incremental submittals of documentation/code to meet program milestones. These drops shall be incorporated into the master schedule. The Developer shall provide a report that defines the capabilities and limitations of each Build* [Army 2006].

### 6.8.2 Section M - Evaluation

### 6.8.3 Section L - Instructions to Offerors

## 6.9 Safety-Critical Software - Interface Requirements Specification

### 6.9.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall develop an Interface Requirements Specification (IRS) IAW DI-IPSC-81434A and deliver IAW CDRL xxx. The IRS shall distinguish (e.g., flag) all software Safety requirements from the other software requirements. The Software IRS shall specify the requirements imposed on the Hardware/Software Interface, and the interfaces between software. An IRS is required for each CSCI to be integrated into the platform and each platform CSCI that was modified for the integration* [Army 2006].

### 6.9.2 Section M - Evaluation

### 6.9.3 Section L - Instructions to Offerors

### 6.10 Safety-Critical Software - Preliminary Hazard Analysis

#### 6.10.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall prepare a Preliminary Hazard Analysis (PHA) IAW MIL-STD-882D and deliver IAW CDRL xxx. The PHA shall document which hazards are associated with the ABC design and operational concept. This provides the initial framework for a listing of hazards and associated risks that require tracking and resolution during program design and development. The PHA shall be used to identify potential Safety-critical issues in hardware and/or software. The PHA will be maintained and updated throughout the development process* [Army 2006].

#### 6.10.2 Section M - Evaluation

#### 6.10.3 Section L - Instructions to Offerors

## 6.11 Safety-Critical Software - Required RFP Items for Airworthiness

### 6.11.1 Section C - SOW/SOO; Requirements

**GENERAL RECOMMENDATIONS**

RFP Required Items [Army 2003]

1. PMO System Safety Policies.
2. Preliminary Hazards List (see FSAQAP Appendix D, C.1.3).
3. PMO System Safety Management Plan (see FSAQAP Appendix B, 4.2.1.1).
4. PMO Specified Safety Requirements.
5. Airworthiness Qualification Plan (see FSAQAP Appendix E).
6. A Requirement for the development organization to perform and maintain the Software Safety Criticality Functional Analysis (SSCFA) as part of their development process.
7. A Requirement for the development organization to implement Safety oriented:
    a. Process Methods and Standards (see FSAQAP Table 2.3.2).
    b. Design and Engineering Standards (see FSAQAP Table 2.3.3).
    c. Techniques (see FSAQAP Table 2.5.1 – 2.5.7).
    d. Products (see FSAQAP Table 2.1.1 – 2.1.2).

In addition, the RFP should request the bidders to provide in their proposal an assessment of the software Safety criticality, the rationale for the assessment, a proposed Safety process and System/Software Safety Plan, software/system Safety design approaches and standards, and software/system Safety validation methods and procedures [Army 2003].

### 6.11.2 Section M - Evaluation

### 6.11.3 Section L - Instructions to Offerors

## 6.12 Safety-Critical Software - Required RFP Items for Safety

### 6.12.1 Section C - SOW/SOO; Requirements

**GENERAL RECOMMENDATIONS**

List of Required Items [Army 2006]

1. PMO System Safety Policies [Army 2006]
2. Preliminary Hazards List.
3. PMO System Safety Management Plan.
4. PMO Specified Safety Requirements.
5. A Requirement for the development organization to perform and maintain the Software Safety Criticality Functional Analysis (SSCFA) as part of their development process.
6. A Requirement for the development organization to implement Safety oriented:
    a. Process Methods and Standards.
    b. Design and Engineering Standards.
    c. Techniques.
7. Standard Software Development Artifacts/Data.
8. Standard Safety Oriented Artifacts/Data.

In addition, the RFP should request the bidders to provide in their proposal an assessment of the software Safety criticality, the rationale for the assessment, a proposed Safety process and System/Software Safety Plan, software/system Safety design approaches and standards, and software/system Safety validation methods and procedures. The typical standard software development artifacts/data and Safety oriented artifacts/data, together with the recommended submittal date [Army 2006].

### 6.12.2 Section M - Evaluation

### 6.12.3 Section L - Instructions to Offerors

## 6.13 Safety-Critical Software - Safety Assessment Report

### 6.13.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Contractor shall perform a software Safety assessment and prepare a Safety Assessment Report (SAR) IAW DI-SAFT-80102B and deliver IAW CDRL xxx. The purpose of the SAR is to verify and document compliance with all system/software Safety requirements and policies, identify previously unidentified design hazards, identify all residual risks, and recommend actions to eliminate identified hazards/residual risks, or control identified hazard/risks, to an acceptable level. The SAR will include supporting analyses and activities such as system Functional Hazard Assessment (FHA), system fault tree analysis (FTA), system and software Hazard Causal Factor Analysis (HCFA), developmental testing, operational testing, live fire tests, field-testing, supportability, transportability, and maintenance. The SAR shall include the items specified in SAE ARP 4761, Appendix C* [Army 2006].

### 6.13.2 Section M - Evaluation

### 6.13.3 Section L - Instructions to Offerors

## 6.14 Safety-Critical Software - SW Safety Critical Function Analysis (SSCFA) Report

### 6.14.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall prepare/update the software Safety critical function analysis (SSCFA) reports IAW DI-MISC-80711A and deliver IAW CDRL xxx. This report shall identify which CSCI or Computer Software Unit (CSU) is Safety critical and shall illustrate the relationship each CSCI or CSU has with the Safety critical functions and show traceability to the software requirements. Subsection 4.3.5.1 of the Joint Software System Safety Handbook (JSSSH) may be used as guidance in the development of the SSCFA Report using the Software Hazard Criticality Matrix and the SSCFA template* [Army 2006].

### 6.14.2 Section M - Evaluation

### 6.14.3 Section L - Instructions to Offerors

## 6.15 Safety-Critical Software - Software/Firmware Safety Assessment Process

### 6.15.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall identify and evaluate functional hazards at the system and subsystem level to determine the criticality of hardware, firmware, and software components. The Safety assessment process shall include the evaluation of the effects of firmware and software failures, Safety hazards, and qualification deficiencies of the ABC system, IAW SAE ARP 4761. The Safety assessment process shall include system and subsystem level Functional Hazard Assessments (FHA), Hazard Causal Factor Analysis (HCFA), Fault Tree Analyses (FTAs), and Failure Modes and Effects Analyses (FMEA) to support the ABC System Safety assessments and the FRACAS requirements identified in section 6* [Army 2006].
>
> *The Safety analyses and assessments shall further define the specific hazards and identify new potential hazards and their impact on the system integrity throughout the development and qualification of hardware, firmware, and software. The Developer shall utilize the FHAs, HCFAs, FTAs, and FMEAs when preparing the preliminary system Safety Assessment Report (SAR) and updates to the SAR. The Developer shall assign risk assessment codes and criticality levels based on the impact to the total system, with the system being defined as the entire system unless otherwise specified. The Developer shall perform the system Safety assessment effort as an integrated effort encompassing all disciplines. This effort shall include integration of new system components and the interface with existing systems. The Developer shall present all identified functional and subsystem hazards to the ABC System Safety Working Group (SSWG). The Developer shall track all catastrophic and critical hazards as well as any other hazard meeting medium and high-risk thresholds IAW the approved ABC Project Office System Safety Management Plan. The Developer shall provide access to FHAs, FTAs, FMEAs and hazard tracking reports that identify the hazard severity level and probable frequency of occurrence, to the Government, through the Integrated Product Team (IPT) process and electronic access. The Developer shall ensure that the operation and maintenance instructions and training are generated with appropriate Safety procedures and precautionary information. The Developer may use the System Safety Analysis Handbook as a guide in addressing the software system Safety requirements* [Army 2006].

### 6.15.2 Section M - Evaluation

### 6.15.3 Section L - Instructions to Offerors

## 6.16 Safety-Critical Software - Software/Subsystem Hazard Analysis

### 6.16.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The Developer shall prepare a Software/Subsystem Hazard Analysis (SSHA) IAW MIL-STD 882D and deliver IAW CDRL xxx. The purpose of the SSHA is to determine and document all software that could contribute to a system hazard, including derived software requirements, or whose design does not satisfy contractual Safety requirements. [Software/Subsystem Hazard Analysis (SSHA)] areas to consider are* [Army 2006]:

1. *Performance,*
2. *Performance degradation,*
3. *Functional failures,*
4. *Timing errors,*
5. *Design errors or defects,*
6. *Inadvertent functioning, and*
7. *Exception/error handling.*

### 6.16.2 Section M - Evaluation

### 6.16.3 Section L - Instructions to Offerors

## 6.17 Safety-Critical Software - Software Hazard Analysis Tracking Reports

### 6.17.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The Developer shall prepare Software Hazard Analysis Tracking reports IAW DI-SAFT-80105B and deliver IAW CDRL xxx. The Reports shall include the Contractor's assessment of software criticality per the Software Hazard Criticality Index (SHCI) for each identified hazard using the Software Hazard Criticality Matrix. The contractor shall develop a method or procedure to document and track hazards and their controls thus providing an audit trail of hazard resolutions. A centralized file, computer data base, or document called a "Hazard Log" shall be maintained. The "Hazard Log" shall contain* [Army 2006]:

1. *Description of each hazard to include associated software and associated software hazard risk index.*
2. *Status of each hazard and control.*
3. *Traceability of resolution on each Hazard Log item from the time the hazard was identified to the time the risk associated with the hazard was reduced to a level acceptable to the managing activity.*
4. *Identification of residual risk.*
5. *Action person(s) and organizational element.*
6. *The recommended controls to reduce the hazard to a level of risk acceptable to the managing activity.*
7. *The signature from the managing activity accepting the risk and thus effecting closure of the Hazard Log item.*

### 6.17.2 Section M - Evaluation

### 6.17.3 Section L - Instructions to Offerors

## 6.18 Safety-Critical Software - Structural Coverage Analysis/Test

### 6.18.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*Structural Coverage Analysis/Testing shall be performed for any source code that functions in a flight/Safety critical capacity designated to have an SHCI value 1 through 3. The Developer shall document the selected method for demonstrating the structural coverage analysis/testing of the software in the Software Development Plan (SDP), STP, and Software Test Description (STD). The Contractor shall prepare and document the results of this coverage analysis/testing in the Software Test Report (STR). The structural coverage analysis/testing shall be performed as follows* [Army 2006]:

1. *Modified Condition Decision Coverage (NASA/TM-210876) is required for safety critical software components that meet Software Hazard Criticality Index (SHCI) value 1 during the development process.*
2. *Condition/Decision Coverage (NASA/TM-210876) is required for all software that meets an SHCI value of 2 during the development process.*
3. *Statement Coverage (NASA/TM-210876) is required for all software that meets an SHCI value of 3 during the development process.*

### 6.18.2 Section M - Evaluation

### 6.18.3 Section L - Instructions to Offerors

### 6.19 Safety-Critical Software - Structural Testing

#### 6.19.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *Structural testing shall be performed for any source code that functions in a flight critical capacity SHRI value 1 through 4 or is designated to have a DO-178B Level A, B, or C criticality (RTCA/DO-178B). Modified Condition Decision Coverage (NASA/TM-210876) is required for flight critical (RTCA/DO-178B Level A) software and all software components that must meet SHRI values 1 or 2 during the development process. Condition/Decision Coverage (NASA/TM-210876) is required for all software that must meet an Software Hazard Risk Index (SHRI) value of 3 during the development process. Statement Coverage (NASA/TM-210876) is required for all software that must meet an SHRI value of 4 during the development process. The Developer shall document the selected method for demonstrating the structural coverage of the software in the* Software Development Plan (SDP) [Army 2003].

#### 6.19.2 Section M - Evaluation

#### 6.19.3 Section L - Instructions to Offerors

## 6.20 Safety-Critical Software - System/Software Safety Program Plan

### 6.20.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall prepare a System Safety Program Plan (SSPP) IAW DI-SAFT-81626 and deliver IAW CDRL xxx. The SSPP shall describe in detail the tasks and activities of the system Safety engineering and management program established by the Developer. It shall also describe the Safety, systems, and software engineering processes to be employed to identify, document, evaluate, and eliminate and/or control system hazards to the levels of acceptable risk for the program. Software/firmware Safety should be addressed in this Plan. If software/ firmware Safety is not addressed in the SSPP, then the Developer shall prepare a separate Software/Firmware Safety Program Plan (SWSPP) IAW DI-MISC-80711A, using IEEE* Software Test Description (STD) *1228-1994 as a guide, and deliver IAW CDRL xxx* [Army 2006].

### 6.20.2 Section M - Evaluation

### 6.20.3 Section L - Instructions to Offerors

# 7 Software Architecture and Quality Attributes

The Software Architecture and Quality Attributes section of this document provides examples of RFP language that support visibility into contractor activities related to structural aspects of a particular system. These structural issues are design-related—software architecture is, after all, a form of software design that occurs earliest in a system's creation—but at a more abstract level than algorithms and data structures. According to what has come to be regarded as a seminal paper on software architecture, Mary Shaw and David Garlan suggest that these "structural issues include gross organization and global control structure; protocols for communication, synchronization, and data access; assignment of functionality to design elements; physical distribution; composition of design elements; scaling and performance; and selection among design alternatives [Clements 1996]."

## 7.1 Software Architecture Definitions

### 7.1.1 Section C - SOW/SOO; Requirements

### 7.1.2 Section M - Evaluation

### 7.1.3 Section L - Instructions to Offerors

GENERAL RECOMMENDATIONS

The RFP must request sufficient software schedule information to understand how the software development fits into the submitted IMS. This problem can be overcome by specifying supplemental information in the RFP to be submitted with the proposal such as [SMC 2004]

- IMS supplements to detail the lower level tasks to CSCI and incremental delivery
- mapping information showing where each CSCI is addressed in the IMS

The technical definitions of the computer software architecture and data metamodel, estimated sizing, throughput timing, and growth migration strategy also need to be defined as criteria in Section L of the RFP and in the offeror's proposal [SMC 2004].

## 7.2 Modeling and Simulation

### 7.2.1 Section C - SOW/SOO; Requirements

### 7.2.2 Section M - Evaluation

### 7.2.3 Section L - Instructions to Offerors

EXAMPLE 1

> *Enumerate, describe and show how the Offeror's modeling and simulation software items will be used to verify and validate requirements. Include software simulation items to be used in performing or supporting operations or sustainment* [SEI 2007c].
>
> *Provide the Offeror's architecture for models and simulators including the plans for verifying and validating them prior to release* [SEI 2007c].
>
> *Describe the Offeror's approach for using software test beds and software simulators during the operational software development and show how resource contention will be avoided, if any* [SEI 2007c].
>
> *Describe the Offeror's approach to synchronize ground and space simulators with operational software, synchronize simulators with multiple flight software versions, and support training functionality needs aligned with program milestones* [SEI 2007c].

## 7.3 Modular Design and Technology Insertion

### 7.3.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The Contractor's architectural approach shall support the rapid and affordable insertion and refreshment of technology through modular design, the use of open standards and open interfaces. The Contractor shall define the functional partitioning and the physical modularity of the system to facilitate future replacement of specific subsystems and components without impacting other parts of the system and to encourage third party vendor's participation.*

### 7.3.2 Section M - Evaluation

### 7.3.3 Section L - Instructions to Offerors

## 7.4 Modular Open Systems Approach (MOSA)

### 7.4.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The Offeror shall use modular open systems approach to* [OSJTF]:

1. *Facilitate development of a modular architecture and allow for affordable intraoperability*
2. *Ensure that the system design is sufficiently flexible and robust to accommodate changing technology and requirements*
3. *Facilitate integration with other systems and use of commercial products from multiple sources both in the initial design and in future enhancements*
4. *Enable technology insertion as currently available commercial products mature and new commercial products become available in the future*
5. *Allow for affordable support*
6. *Allow continued access to technologies and products supported by many suppliers (a broad industrial base which does not restrict available sources to the detriment of competition)* [OSJTF]

EXAMPLE 2

*The Offeror shall use a modular open systems approach (MOSA) to evaluate the appropriateness of implementing a modular design strategy for building systems. A primary consideration in selection of equipment to meet the design functionality shall be the impact to the overall modular open systems architecture. A modular open systems approach and analysis of long term supportability, interoperability, and growth for future modifications shall be major factors in the Offeror's final selection of equipment and integration approach. All the systems components shall facilitate future upgrades and permit incremental technology insertion to allow for incorporation of additional or higher performance elements with minimal impact on the existing systems* [OSJTF].

*The architectural approach shall provide a viable technology insertion methodology and refresh strategy that supports application of a modular open systems approach and is responsive to changes driven by mission requirements and new technologies* [OSJTF].

*The Offeror shall develop a detailed modular design and integration that includes but is not limited to the following aspects: interoperability, intra-operability, upgradeability, reconfigurability, transportability, software standards, interface standards, long term supportability, sources of supply and/or repair, business strategies, and other entities that affect application of a modular open systems approach* [OSJTF].

*For those portions of hardware, firmware, or software that are driven to proprietary and/or closed system architectures by mission specific requirements, a hardware/firmware/software partitioning or other design features to mitigate the system level impacts shall be provided*

*The Offeror shall provide an orderly, planned approach to address migration of proprietary or closed system equipment or interfaces to a modular design when technological advances are available* [OSJTF].

*The Offeror's modular design and integration shall preclude long term dependence on closed or proprietary interface standards, technologies, products, or architectures. Secure or classified data systems shall also conform to the modular design approach as much as practical. The design shall provide sufficient growth and open interface standards to allow future reconfiguration and addition of new capabilities without large-scale redesign of the system* [OSJTF].

EXAMPLE 3

*The Government intends to procure system(s) having an Open System Architecture and corresponding components. As part of this contract, the Contractor will be required to define, document, and follow an open systems approach for using modular design, standards-based interfaces, and widely-supported consensus-based standards. The Contractor shall develop, maintain, and use an open system management plan to support this approach and will be required to demonstrate compliance with that plan during all design reviews. As part of an open system management plan, the Contractor will be required to identify to the Government all Commercial-Off-the-Shelf/Nondevelopment Item (Commercial off-the-shelf software (COTS)/NDI) components, their functionality and proposed use in the system, and provide copies of license agreements related to the use of these components for Government approval prior to use. The proposed open system management plan will be incorporated into the contract with any changes, alterations, and/or modifications requiring Government approval. In addition, the Contractor shall provide the Government (and/or Government support contractors) electronic access to its integrated development environment throughout the term of the contract. In satisfying the Government's requirements, the following system architecture approach characteristics shall be utilized* [USN 2007a]:

a. *Open Architecture - The Contractor shall develop and maintain an architecture that incorporates appropriate considerations for reconfigurability, portability, maintainability, technology insertion, vendor independence, reusability, scalability, interoperability, upgradeability, and long-term supportability as required by the 23 DEC 2005 Office of the Chief of XXX Operations ) requirements letter* [USN 2007a].

b. *Modular Open Design – The Contractor shall develop an architecture that is layered and modular and uses Commercial off-the-shelf software (COTS)/NDI hardware, operating systems, and middleware that utilize non-proprietary or non-vendor-unique, key Application Programming Interfaces (APIs). The Contractor's design approach shall be applied to all subsystems and components. As part of its open system management plan, the Contractor will be required, at a minimum, to describe how the proposed system architecture meets these goals, including the steps taken to use non-proprietary or non-vendor unique Commercial off-the-shelf software (COTS) or reusable NDI components wherever practicable* [USN 2007a].

   - *Module Coupling - The Contractor's design approach shall result in modules that have minimal dependencies on other modules (low coupling), as evidenced by simple, well-defined interfaces and by the absence of implicit data sharing. The purpose is to ensure that any changes to one module will not necessitate extensive changes to other modules, and hence facilitate module replacement and system enhancement. The approach used to determine the level of coupling and the design trade-off approach shall be described* [USN 2007a].
   - *Module Cohesion – The Contractor's design approach shall result in modules that are characterized by the singular assignment of identifiable, discrete functionality*

*(high cohesion). The purpose is to ensure that any changes to system behavioral requirements can be accomplished by changing a minimum number of modules within the system. The approach used to determine the level of cohesion and the design trade-off approach shall be described* [USN 2007a].

### 7.4.2 Section M - Evaluation.

EXAMPLE 1

1.1. *Identification of specific acquisition objectives (e.g., affordability, ease of change, leveraging commercial investment in new technology, etc.) and operational capabilities (e.g., ease of integration, interoperability, etc.) directly or indirectly dictate the use of open systems in your program.*

1.2. *A system architecture characterized by modular design.*

1.3. *The degree to which the program risk management strategy and modular open systems approach (MOSA) complement each other.*

1.4. *Justification of modular open system design via business case analysis (e.g., cost/benefit analysis, market research findings, etc.).*

2.1. *Proactive management of system interfaces.*

2.2. *Identification of key system interfaces based on the module characteristics (e.g., criticality of function, ease of integration, change frequency, interoperability, commonality, etc.).*

2.3. *Appropriate designation of open standards for key system interfaces.*

3. *Open Standards Indicators* [OSJTF] *Feasibility studies to assess the use of open standards for key interfaces.*

3.2. *Application of a standards selection process that gives preference to open standards.*

3.3. *Standards selection for key interfaces is based on application of specific criteria (e.g., DoD mandate, industry consensus, market support, prime contractor recommendation, etc.).*

*Additionally, does the Offeror's proposal provide the User with the ability to:*

- *quickly interconnect, reconfigure, and assemble existing forces, systems, subsystems, and components?*
- *interchange and use information, services and/or physical items among components within a system?*
- *interchange and use information, services and/or physical items among systems within an integrated architecture, platform, domain, or a DoD Component?*
- *support reuse of software and the common use of components across various product lines?*
- *transfer a system, component, or data, from one hardware or software environment to another?*
- *adapt hardware or software to accommodate changing work loads?*

### 7.4.3 Section L - Instructions to Offerors

EXAMPLE 1

*The proposal shall describe how the Offeror's modular open systems approach will cause the Offeror to implement an integrated business and technical strategy that employs:*

*(1) a modular design and, where appropriate, (2) defines key interfaces using (3) widely-supported, consensus-based (i.e., open) standards that are published and maintained by a recognized industry standards organization* [OSJTF].

*In describing the modular open systems approach, the proposal shall include* [OSJTF]:

- *Plans for integrating the systems internally and with external system*
- *Identification of the means for ensuring conformance to widely used consensus standards (i.e., open standards) and profiles throughout the development process, and an explanation of how the modular open systems approach supports benefits such as reconfigurability, portability, interoperability, technology insertion, vendor independence, reusability, scalability, and commercial product based maintainability*
- *A description of how the technical approach ensures having access to mature as well as the latest technologies by establishing a robust, modular, and evolving architecture based on widely used consensus standards*
- *A description of how the design concept supports modular open systems approach principles*
- *A description of the strategy for maintaining the currency of technology (e.g., through Commercial off-the-shelf software (COTS) insertion, technology refresh strategies, and other appropriate means).*
- *Identification of processes for:*
  - *isolating functionality through the use of modular design.*
  - *identifying key interfaces.*
  - *selecting open standards for key interfaces.*
  - *specifying the lowest level (e.g., subsystem or component) at and below which they intend to control and define interfaces by proprietary standards and the impact of that upon their proposed logistics approach.*
  - *evaluating modular open systems baseline standards, defining and updating profiles, evaluating and justifying new and vendor unique profiles.*
  - *validating implementation conformance to selected profiles.*
  - *managing application conformance to selected profiles.*
  - *training in use of profiles.*

*The Offeror shall specify how they plan to use a modular open systems approach as an enabler to achieve the following objectives* [OSJTF]:

- *Adapt to evolving requirements and threats*
- *Accelerate transition from science and technology into acquisition and deployment*
- *Facilitate systems reconfiguration and integration*
- *Enhance modularity*

- *Leverage commercial investment in new technologies and products*
- *Reduce the development cycle time and total life-cycle cost*
- *Achieve commonality and reuse of components within a system (if commonality is a requirement)*
- *Maintain continued access to cutting edge technologies and products from multiple suppliers*
- *Mitigate the risks associated with technology obsolescence, being locked into proprietary technology, and reliance on a single source of supply over the life of a system*
- *Enhance life-cycle supportability*

EXAMPLE 2

*Subfactor 1.* ***Open Systems Approach and Goals****. The Offeror shall describe its open systems approach for using modular design, standards-based interfaces, and widely supported, consensus-based standards to achieve the following goals. At a minimum the Offeror shall provide the following as part of its proposal* [USN 2007a]:

*a. Address XXX Open Architecture Requirements – A detailed description of the Offeror's approach for addressing a system architecture that incorporates appropriate considerations for reconfigurability, portability, maintainability, technology insertion, vendor independence, reusability, scalability, interoperability, upgradeability, and long-term supportability . . . ..*

*b. Design Disclosure – Within the constraints of contractual data rights, a detailed description of the Offeror's approach to facilitate the sharing of system or component (e.g., software, hardware, middleware) design information in support of peer reviews and the spiral development process. The Offeror shall describe how its design will be documented and modeled using industry standard formats (e.g., Unified Modeling Language), and how it will use tools that are capable of exporting model information in a standard format (e.g., Extensible Markup Language Metadata Interchange (XMI) and AP233/ISO 10303). The Offeror shall identify the proposed standards and formats to be used.*

*c. Technology Insertion and Refresh – A detailed description of how the Offeror's proposed system will allow for rapid and affordable technology insertion and refresh. For example, the Offeror should describe how the proposed system will allow incremental systems improvement through upgrades of individual hardware or software modules with newer modular components. At a minimum, the description shall address how the Offeror's architectural approach will support this requirement including how components from third party providers and reuse sources shall be included.*

*d. Asset Reuse – A detailed description of the steps taken to reduce acquisition of duplicative system components where possible. At a minimum, the Offeror shall describe what artifacts from the [Explanation: The specific asset reuse repositories/libraries that the Contractors will review for components should be identified] or common components* [USN 2007a]

*e. Modular Open Systems Approach (MOSA) – A detailed description of the Offeror's modular open systems approach. At a minimum, the Offeror shall address:*

*i. Plans for integrating the systems both internally and with external systems;*

*ii. The means for ensuring conformance to open standards and profiles, as discussed in Section C, throughout the development process;*

*iii. A description of how the technical approach ensures having access to mature as well as the latest technologies by establishing a robust, modular, and evolving architecture based on open standards.*

*iv. A description of the strategy for maintaining the currency of technology (e.g., through Commercial off-the-shelf software (COTS) or reusable NDI insertion, technology refresh strategies, and other appropriate means); and*

*v. Identification of processes for:*

*(1) Isolating functionality through the use of modular design;*

*(2) Evaluating modular open system baseline standards, defining and updating profiles, and evaluating and justifying new or vendor-unique profiles;*

*(3) Validating implementation conformance to selected profiles;*

*(4) Managing application conformance to selected profiles; and*

*(5) Training in use of profiles.*

*f. Modular Open Systems Approach (MOSA) as an Enabler of Open Architecture Objectives – A detailed description of how the Offeror intends to use a modular open systems approach as an enabler to achieve the following objectives:*

*i. Adapt to evolving requirements and threats as identified by the Government;*

*ii. Enhance interoperability and the ability to integrate new capabilities without redesign of entire systems or large portions thereof;*

*iii. Accelerate transition from science and technology into acquisition and deployment;*

*iv. Facilitate systems reconfiguration and integration;*

*v. Reduce the development cycle time and total life-cycle cost;*

*vi. Maintain continued access to cutting edge technologies and products from multiple suppliers; and*

*vii. Mitigate the risks associated with reliance on a single source of supply over the life of the system, to include, but be not limited to, technology obsolescence and dependence on proprietary or vendor-unique technology.*

*g. Life-cycle Supportability – A detailed description of how the Offeror intends to enhance life-cycle supportability by implementing performance-based logistics arrangements to sustain the components through their lifecycle.*

*h. Employ a Layered Modular Architecture – A detailed description on how the proposed system architecture is layered, modular, and makes maximum use of Commercial-Off-the-Shelf/Non-developmental Item (Commercial off-the-shelf software (COTS)/NDI)hardware, operating systems, and middleware that utilize non-proprietary key APIs whenever practicable.*

*i. Traceability of System Requirements – A detailed description of the Offeror’s approach for ensuring that all system requirements (including those contained in the Initial Capabilities Document, Capabilities Development Document, and in Section C of this Solicitation) are accounted for through a demonstrated ability to trace each requirement to one or more modules. Modules consist of components (one of the parts that make up a* *system and may be hardware and/or software) which are self-contained elements with well-defined, standards-based and published interfaces*

j. *Minimize Inter-component Dependencies – A detailed description of the Offeror's approach for designing a system that, to the maximum extent practicable, minimizes inter-component dependencies and allows components to be decoupled and re-used, where appropriate, across various Naval programs or replaced by competitive alternatives.*

k. *Rationale for Modularization Choices – A detailed description of the Offeror's rationale for the modularization choices made to generate the design. At a minimum, the rationale shall explicitly address any tradeoffs performed, particularly those that compromise the modular and open nature of the system.*

l. *Future System Upgrades – A detailed description of how a modular design strategy will be demonstrated in all aspects of future system upgrades.*

    i. *In addressing the specified requirements, the proposal, at a minimum, must demonstrate how the modular design strategy applies, and the effect it will have on future systems upgrades.*

    ii. *The proposal shall describe an orderly planned process to address migration of proprietary, vendor-unique, or closed system equipment or interfaces to a modular open systems design when technological advances are available or when operational capability is upgraded. The proprietary, vendor-unique or closed systems implementation shall also be reflected in the Offeror's system level life cycle cost estimates.*

    iii. *The modular design approach shall either mitigate or partition – at the lowest subsystem or component level — proprietary, vendor unique or closed system implementation to avoid out-year supportability issues and diminished manufacturing and repair sources.*

## 7.5 Modular Open Systems Design

### 7.5.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Contractor's design approach shall result in a layered system design, maximizing software independence from the hardware, thereby facilitating technology refresh. The design shall be optimized at the lowest component level to minimize inter-component dependencies. The layered design shall also isolate the application software layers from the infrastructure software (such as the operating system) to enhance portability and to facilitate technology refresh. The design shall be able to survive a change to the computing infrastructure with minimal or no changes required to the application logic. The interfaces between the layers shall be built to open standards or available to the Government with at least GPR rights. The system architecture shall minimize inter-component dependencies to allow components to be decoupled and re-used, where appropriate, across various XXX programs and platforms* [USN 2007a].
>
> *The Contractor shall describe its rationale for the modularization choices made to generate the design. The Contractor's design approach shall produce a system that consists of hierarchical collections of software and hardware configuration items (components). These components shall be of a size that supports competitive acquisition as well as reuse. The Contractor's design approach shall emphasize the selection of components that are available commercially or within the DOD, to avoid the need to redevelop products that already exist and that can be re-used. The Contractor's rationale must explicitly address any tradeoffs performed, particularly those that compromise the modular and open nature of the system. MOSA Objectives – The Contractor shall specify how it plans to use MOSA to enable the system to adapt to evolving requirements and threats; accelerate transition from science and technology into technology and deployment; facilitate systems reconfiguration and integration; reduce the development cycle time and total life cycle cost; maintain continued access to cutting edge technologies and products from multiple suppliers; and mitigate the risks associated with technology obsolescence, being locked into proprietary or vendor-unique technology, and reliance on a single source of supply over the life of the system* [USN 2007a].

### 7.5.2 Section M - Evaluation

### 7.5.3 Section L - Instructions to Offerors

## 7.6 Open Architecture

### 7.6.1 Section C - SOW/SOO; Requirements

GENERAL RECOMMENDATIONS

Section C, Description, Guidance, and Objectives will include the following Open Architecture attributes and objectives [Goff 2006]:

- open architecture
  - portability
  - interoperability
  - upgradeability
- open modular design—self-contained elements with well-defined interfaces
- interface design and management
  - All configuration item (CI) level interfaces are defined.
  - Technology insertion capability will be maximized.
- treatment of proprietary elements
  - Proprietary elements will be isolated.
  - They will not force additional closed or proprietary equipment or functions [Goff 2006].

### 7.6.2 Section M - Evaluation

EXAMPLE 1

*Factor ( ): Technical Approach and Processes* - *In evaluating the Open Architecture Technical Approach and Processes, the Government will use information provided in the proposal to assess the Offeror’s ability to execute* [USN 2007a]:

- *Subfactor 1. Open Systems Approach and Goals*
- *Subfactor 2. Interface Design and Management*
- *Subfactor 3. Treatment of Proprietary or Vendor-Unique Elements*
- *Subfactor 4. Life Cycle Management and Open Systems*

*Factor ( ): System Compliance with Open Architecture Guidance* - *In evaluating the System Compliance with XXX Open Architecture Guidance, the Government will use information in the proposal to assess the degree to which the Offeror’s approach complies with PEO-specified (or Enterprise) Technical Guidance Points as identified in Table X of Section L.*

*Factor ( ): Management Approach* - *In evaluating the Management Approach, the Government will use information in the proposal to assess the degree to which the Offeror’s approach facilitates competition at various levels (tiers) of the offered modular system, awards significant portions of the overall system to third party sources, and uses an Integrated Product Team (IPT) to improve processes, manage risk, and increase efficiency.*

### 7.6.3 Section L - Instructions to Offerors

## 7.7 Open Systems and Life-Cycle Management

### 7.7.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The Contractor's architecture shall provide for insertion of Commercial off-the-shelf software (COTS) into the system and demonstrate that Commercial off-the-shelf software (COTS), reusable NDI, and other components are logistically supported throughout the life cycle. The Contractor shall describe and demonstrate the strategy for reducing product or system and associated supportability costs through insertion of Commercial off-the-shelf software (COTS) and other reusable Commercial off-the-shelf software (COTS) or NDI products. The Contractor shall establish a process to logistically support Commercial off-the-shelf software (COTS) or NDI products. The Contractor shall describe the availability of commercial repair parts and repair services, facilities, and manpower required for life cycle support; and demonstrate they are adequate to ensure long term support for Commercial off-the-shelf software (COTS) or NDI products. The Contractor shall provide the proposed methodology for pass through of Commercial off-the-shelf software (COTS) warranties to the Government* [USN 2007a].

### 7.7.2 Section M - Evaluation

### 7.7.3 Section L - Instructions to Offerors

EXAMPLE 1

*The Offeror shall describe and demonstrate the strategy for reducing product or system and associated supportability costs through insertion of Commercial off-the-shelf software (COTS) or reusable NDI products* [USN 2007a].

*a. The Offeror shall identify and demonstrate a strategy to insert Commercial off-the-shelf software (COTS) technologies and other reusable NDI into the system and demonstrate that Commercial off-the-shelf software (COTS), other reusable NDI, and other components are logistically supported throughout the system's life cycle.*

   i. *The proposal shall identify specific hardware and software elements of the subsystem designs that are planned for Commercial off-the-shelf software (COTS), Open Source Software, Proprietary and other reusable NDI replacement and the supportability plans for those elements.*

   ii. *The Offeror shall demonstrate how the subsystem is designed to allow for timely and cost-effective replacement of subsystem elements or modules. The Commercial off-the-shelf software (COTS) selection processes shall be specifically addressed, including validation of those processes, and shall be supported by documentation of the decision leading to the selection of specific Commercial off-the-shelf software (COTS) products (e.g. with test results, architectural suitability, "best value" assessments, etc.).*

*b. The Offeror shall provide a description of processes that will be established and demonstrate that Commercial off-the-shelf software (COTS) and other reusable NDI products are logistically supported.*

*c. The Offeror shall describe the availability of commercial repair parts and repair services, facilities and manpower required for life cycle support and demonstrate that they are adequate to ensure long term support for Commercial off-the-shelf software*

*(COTS) and other reusable NDI products. The Offeror shall provide the proposed methodology for pass through of Commercial off-the-shelf software (COTS) warranties to the Government* [USN 2007a].

## 7.8 Quality Attribute Requirements

### 7.8.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *Software Quality requirements will be specified for the program. The development of these requirements shall be the responsibility of the program office. The program office will work together with the end-user of the system to generate requirements based on an analysis of the system requirements, life expectancy, development costs and user concerns. Example user concerns to consider are performance (e.g. reliability, usability and efficiency), design architecture (e.g. maintainability and correctness) and re-engineering (e.g. reusability, interoperability and portability)* [USAF 1996].
>
> *Software Quality requirements will be specified and documented within the baselined Software Requirements Specification (SRS). A hierarchical quality model of quality factors, criteria and metrics will be used to predict software quality. Factors representing the user's concerns will be decomposed (using relevant standards and guidebooks) into software oriented characteristics. Metrics/measures of these characteristics will also be defined. The specified model will apply to all software development phases and products. Quality progress will be reported and reviewed at each major program milestone* [USAF 1996].
>
> *All open and closed software quality problems will be tracked and reported. The achievement of software quality requirements will be demonstrated, using industry accepted Metrics/measures of operational quality (e.g. reliability = mean-time-to-failure), during integration testing. Failures will be categorized according to a Government approved severity standard* [USAF 1996].

### 7.8.2 Section M - Evaluation

### 7.8.3 Section L - Instructions to Offerors

### 7.9 Reliability, Availability, and Maintainability (RAM)

#### 7.9.1 Section C - SOW/SOO; Requirements

GENERAL RECOMMENDATIONS

A Reliability, Availability, and Maintainability (RAM) rationale is the information that becomes the basis for developing RAM-related portions of the request for proposal and contract(s) to design, develop, test, produce, deploy, and operate the capability. The RAM rationale also supports: tradeoff studies to balance cost and performance; development test planning and evaluation; and operational test and evaluation [DOD 2005].

The RAM rationale expresses quantitative metrics/measures of the levels of reliability, availability, and maintainability needed by the user in operational terms; as well as corresponding quantitative metrics/measures in contractual terms for use in the RFP and contract [DOD 2005].

The core elements of the RAM rationale are [DOD 2005]

- quantitative metrics/measures of the levels of reliability, availability and maintainability needed by the user, in operational terms, as well as corresponding quantitative measures in contractual terms for use in the RFP and contract [DOD 2005]
- an operational mode summary and mission profile, which quantifies how and in what environments the capability, will be used throughout the life cycle [DOD 2005]
- the hardware and software failure definitions and scoring criteria for assessing mission failures and logistics failures during modeling, simulation, test and other activities used for estimating, verifying, or predicting levels of RAM [DOD 2005]

The RAM rationale also [DOD 2005]

- explains why the RAM levels are needed and how they interact and relate to other aspects of the capability (such as performance, force structure, affordability, concept/plan, logistics footprint); and, logistics footprint); and
- documents RAM performance of current capability to provide the basis for assessing measurable improvements to mission capability and operational support [DOD 2005]

R&M requirements included in solicitations should include quantified R&M requirements and allowable uncertainties (such as statistical risks) the FD/SC (provides reliability failure definitions and thresholds of functioning for assessing failures); and the OMS/MP (provides life-cycle usage operation and conditions). Solicitations should require access to information adequate for evaluating the source data, models and reasonableness of modeling assumptions, methods, results, and risks and uncertainties. Requirements to use particular models or statistical test plans are not to be specified. Solicitations should not cite any language, specification, standard, or handbook that specifies “how to “design, manufacture, or test for reliability.

MIL–HDBK–217 or any of its derivatives are not to appear in a solicitation; it has been shown to be unreliable, and its use can lead to erroneous and misleading reliability predictions [Army 2003a].

Develop an RFP that addresses all aspects of system performance. The RFP should clearly identify all constraints, assumptions, and definitions needed for the contractors to put the RAM situation in context, derive the inherent levels of RAM (those that are determined by design and manufacturing), determine the best approach for achieving satisfactory RAM, and state the operational RAM requirements (e.g., operational availability) [DOD 2005].

Translate the operational RAM terms into suitable RFP and contractual terms for the material development contractor to pursue. Develop the mission and logistics reliability specification requirements and the maintainability and integrated diagnostics specification requirements. These and associated RAM program and acceptance test requirements become part of the RFP and contract. Specification development requires conversion of the operational RAM parameters to an equivalent contractual measurement. This process has been recognized as a weak link [DOD 2005].

### 7.9.2 Section M - Evaluation

GENERAL RECOMMENDATIONS

RFP responses should be evaluated, in part, on the basis of a reliability, availability, and maintainability (RAM) program plan (RAMPP) as follows [DOD 2005]:

Understanding [DOD 2005]

The plan should show a clear understanding of

- importance of designing in reliability, availability, and maintainability
- RAM techniques, methodology, and concepts
- importance of integrating RAM activities into the overall systems engineering process

Approach [DOD 2005]

- Management. The plan should identify
  - who is responsible for RAM and their experience and qualifications
  - the number of RAM personnel assigned to the program, the experience level of the RAM personnel, and the number of labor hours allocated to RAM activities
  - how RAM personnel fit in the organizational framework of the program
  - an effective means of communication and sharing of information among RAM engineers and analysts, design engineers, manufacturing engineers, and higher management
  - the contractor's system for controlling the RAM of items from subcontractors and vendors

- how the contractor implements concurrent engineering practices and integrates RAM into the overall engineering and manufacturing effort

- Design. The plan should explain
  - if and how design standards; guidelines; and criteria such as part derating, thermal design, modular construction, Environmental Stress Screening (ESS), and testability will be used
  - the contractor's system for tracking failures and the actions taken to correct (i.e., eliminate or reduce the effect of) the failures. If and how a parts control program will be implemented and the approval procedures for non-standard parts
  - if and how tradeoff studies will be used for critical design areas
  - the time-phasing of RAM activities in relation to key program milestones.
  - any areas of RAM risk
  - if and how software reliability will be addressed

- Analysis/Test. The plan should identify and describe
  - methods of analysis and math models to be used
  - RAM modeling, prediction, and allocation procedures
  - the time phasing and dependencies of the RAM and other testing in relation to the overall program schedule
  - the time available for the test type required (such as maximum time for sequential test) and how that time was determined
  - how the ESS program (if one is planned) is consistent with the requirements in terms of methodology and scheduling
  - if the contractor will predict the RAM (in whatever parameters are specified) prior to the start of testing
  - how the contractor will monitor the level of RAM through the development
  - the resources (test chambers, special equipment, etc.) needed to perform all required testing, how they are determined, and their availability
  - how the results of all testing will be used to evaluate RAM and identify RAM problems

<u>Compliance [DOD 2005]</u>

- Design. The plan should include
  - justification (models, preliminary estimates, data sources, etc.) to back up the claims of meeting RAM requirements
  - evidence of compliance with required military specifications and standards, when required, and good engineering practices for RAM
  - each equipment environmental limitation specified
  - if derating will be used and, if so, the methods of verifying derating requirements

- Analysis/Test. The plan shall indicate
  - an explicit commitment to perform all RAM analyses cited in the RAMPP or required by contract
  - an explicit commitment to perform all RAM testing and screening cited in the RAMPP or required by contract
  - that the contractor complies with all product-level RAM test requirements and that the contractor will demonstrate that the contractor uses the failure definitions in the specification (if none are provided in the specification, then definitions commonly accepted within the engineering community should be used).
  - if and how the contractor will perform verification testing, the type of verification testing planned, and the specific purpose of the testing
- Data. The plan should show an explicit commitment to deliver all required RAM data items in the format specified.

### 7.9.3 Section L - Instructions to Offerors

GENERAL RECOMMENDATIONS

The RFP should normally require a preliminary reliability, availability, and maintainability (RAM) program plan (RAMPP) be developed as part of the systems engineering plan (SEP). The SEP should identify the RAM engineering techniques that will be applied to develop system or elemental RAM performance. The requirements for RAM demonstration, as appropriate, should be identified in the specification and relevant verification matrix, and normally outlined in the contractor's preliminary test and evaluation plan (TEP) [DOD 2005].

## 7.10 Scalability Support

### 7.10.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *An automated, computer-based software life cycle development and support environment will be used by the contractor. Development of the environment's requirements shall be the responsibility of the program office. The ability of the environment's hardware/software complex (including each of its associated CASE tools) to adequately and efficiently support the breadth of software under development (i.e., scalability to the size of the problem) will be a primary consideration* [USAF 2000].

### 7.10.2 Section M - Evaluation

### 7.10.3 Section L - Instructions to Offerors

### 7.11 Software Architecture Approach

#### 7.11.1 Section C - SOW/SOO; Requirements

#### 7.11.2 Section M - Evaluation

EXAMPLE 1

Proposal Requirement #1: Software Architecture [USAF 2005]

> *The proposal requirement will be met when the Offeror proposes an effective software architecture that:*
>
> > *Is developed with Modular Open System Approach principles. Supports the development of software items that are highly modular and independent of non-developmental hardware and software items.*
> >
> > *Implements the proposed architecture for TNOM and supports the TSAT system information assurance architecture.*
> >
> > *Supports system evolution and integration through open and well-defined component interface standards.*
> >
> > *Provides a flexible design that accommodates requirement changes with minimal impact to the TNOM software architecture.*
> >
> > *Is compatible with legacy systems and subsumes the AEHF planning function.*

#### 7.11.3 Section L - Instructions to Offerors

EXAMPLE 1

Proposal Requirement #X: Software Architecture [USAF 2005]

> *Describe your proposed software architecture in Attachment MC9 in your chosen architectural representation technique consistent with the Software Architecture Format described in Attachment 8. Include diagrams indicating the components/subcomponents and their interfaces, with descriptions of the data used by each component and the functionality of the components. The architecture representation in the proposal shall model component/sub-component relationships and support component/subcomponent replacement. Explain how your software architecture supports the DoD Modular Open Systems Approach.*
>
> *Explain how the proposed software architecture implements the TMOS requirements (including IA and AEHF planning) and how the architecture interfaces are compatible with existing legacy systems.*
>
> *Show how the proposed TMOS software architecture is evolvable from early TSAT capability through full functionality. Describe architecture considerations needed to enable additional requirements.*
>
> *Provide results of high-level performance analysis that explains key aspects of the proposed software architecture. The analysis must show how the proposed architecture, sizing estimates, and design demonstrate understanding of functional and interface requirements, components, COTS/NDI, necessary data flow, and risks. This should include a mapping of ELOC/COTS to each requirement (or set of requirements).*

*Describe the proposed process for developing, documenting, and maintaining your TMOS software architecture (reference DI-MISC-80508/T). The process description shall explain: (1) how the architecture will be maintained during system development, implementation, and sustainment; (2) how the system compliance to the architecture will be established and maintained (for example by using mappings from architecture representation model to implemented code and hardware/software COTS/reuse product); and (3) any proposed architectural evaluation and analysis activities.*

## 7.12 Software Architecture Development

### 7.12.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The contractor will develop a software architecture in conjunction with the development of the system and system architecture. The software architecture will satisfy the requirements specified in the system specification. The software architecture will be developed, evaluated, and baselined prior to the initial incremental system build* [Fisher 2008].

### 7.12.2 Section M - Evaluation

### 7.12.3 Section L - Instructions to Offerors

## 7.13 Software Architecture - Documentation of Engineering Efforts

### 7.13.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *Results of the engineering efforts during the development of the software architecture, including all evaluations, will be documented, including rationale for both design decisions and changes to the baselined architecture. Documentation will support the architecture evaluation method and the tracking of changes to the baselined software architecture. Specific information must include, but not limited to, module structure, component interfaces, process structure, and data-flow structure. In each structure, the view-specific relationships among the entities must be documented. For the module structure, relationship information includes but is not limited to the unique information that is encapsulated in each module. For the process structure, the relationship information includes but is not limited to synchronization and concurrency relationships. For the data-flow structure, relationship information includes but is not limited to a high-level description of the data that is produced, stored, or consumed* [Fisher 2008].

### 7.13.2 Section M - Evaluation

### 7.13.3 Section L - Instructions to Offerors

## 7.14 Software Architecture Evaluation

### 7.14.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*An evaluation team shall conduct a series of software architecture evaluations in accordance with the special requirements of Section H* [Bergey 2005].

EXAMPLE 2

*The contractor will development and document scenarios required to conduct architecture evaluation using the method described in Appendix YY for* [Fisher 2008]:

- *Evaluation of the software architecture prior to the first incremental system build*
- *Evaluation of the system prior to acceptance*

*Scenarios are developed to exercise specified system change scenarios that are specified in the system specification. These will reflect the non-functional quality attributes of interest. These scenarios will also present interactions from different roles, such as end-user, system administrator, maintainer, and developer. (this task should be undertaken by a domain expert. These scenarios should reflect all roles relevant to the system.)* [Fisher 2008]

*Following the design of these scenarios, the contractor and the Government will conduct a technical interchange meeting, assessing the scenarios to determine that these are sufficient to demonstrate that the software satisfies the contractual requirements* [Fisher 2008].

EXAMPLE 3

*After resolution of issues identified during the evaluation readiness review (see Software Architecture Evaluation Readiness Review), and prior to full implementation of the system, the contractor will plan and jointly conduct with the Government evaluations against the contractual requirements using the architecture evaluation method and contractor-generated scenarios. The contractor will develop an evaluation agenda (plan) to the Government's satisfaction* [Fisher 2008].

*Weaknesses or deficiencies in the software architecture found during these evaluations will be entered into the contractor's corrective action system and resolved by the contractor prior to implementation of incremental systems builds* [Fisher 2008].

GENERAL RECOMMENDATIONS

If a software architecture evaluation is to be required, both the SOW and the product requirements must specify the particular method (such as the Architectural Trade-Off Analysis Method) as well as how the software architecture evaluation method will be used and implemented in the acquisition. This information must be integrated and compatible with other acquisition requirements that are part of the RFP [Bergey 2002].

The statement of work (SOW) describes what the supplier must accomplish. In terms of any evaluation method, the SOW describes which evaluation steps are the supplier's responsibilities. The software architecture evaluation steps in the SOW must be consistent with the overall acquisition. In addition, the SOW should indicate if certain evaluation steps are to be performed jointly by the acquirer and the potential system supplier [Bergey 2002].

### 7.14.2 Section M - Evaluation

EXAMPLE 1

*To incorporate architecture evaluation, Section M must specify how the architecture evaluation will relate to the factors and subfactors. And, it must specify the criteria to be used in judging the bidder's approach to satisfying the RFP/contract architecture requirements* [SEI SASS].

*It is important to emphasize that all RFP sections must be consistent with each other. For example, Section M must include the specific criteria to evaluate only those RFP responses that correspond to the requested areas identified in Section L* [SEI SASS].

EXAMPLE 2

1. *Basis For Award*

   *The award of the <SYSTEM NAME> contract will be based upon the offer that provides the best overall value to the Government in terms of technical, prices, [and] performance risk. All proposals will be evaluated in terms of the factors and subfactors in accordance with the criteria set forth below. Award may not necessarily be made to the offeror with the lowest evaluated price* [Bergey 2002].

2. *Factors And Subfactors To Be Evaluated* [Bergey 2002]

   *The following factors and subfactors will be evaluated* [Bergey 2002].

| | |
|---|---|
| *FACTOR:* | *Technical*<br>*Subfactors:*<br>*Hardware*<br>*Software architecture*<br>*Software* |
| *FACTOR:* | *Price* |
| *FACTOR:* | *Performance Risk* |
| *FACTOR:* | *Management* |

*The following criteria will be applied to measure the quality of the proposed approach under the Technical, and Performance Risk factors and their respective subfactors, as indicated in Paragraph 5 below* [Bergey 2002].

*4.1 Adequacy of Response*

*Adequacy of response is defined as the extent to which the proposed approach is complete and demonstrates an understanding of the requirements* [Bergey 2002].

*Completeness is defined as the extent to which: the proposal describes approaches, including proposed solutions, that address all requirements of the acquisition as requested in the RFP, Section L, and associated risks; means for resolution of the risks have been provided; and the approaches are discussed with sufficient, substantive information to convey to the evaluator a clear and accurate description of how the requirements are to be satisfied* [Bergey 2002].

*Understanding of requirements is the extent to which the approach, including proposed solutions, demonstrates an accurate comprehension of the specified requirements, the intended mission environment, and program goals* [Bergey 2002].

*4. 2 Feasibility*

*Feasibility is defined as the extent to which the approach, including proposed solutions, is capable of satisfying requirements and is realistically achievable, including the extent to which all risks associated with the approach have been mitigated for successful achievement of the requirements* [Bergey 2002].

*4.3 Flexibility*

*Flexibility is the extent to which the approach is adaptable to changing needs or requirements, including future growth. For evaluation of software architecture, flexibility is further defined in terms of modifiability, security, and reusability, which are defined as* [Bergey 2002]:

> *Modifiability. The extent to which the system can be changed quickly and cost effectively*
>
> *Reliability. A measure of the proportion of time the system is up and running.*
>
> *Security. A measure of the system's ability to resist unauthorized attempts at usage and denial of service, while still providing its services to legitimate users.*

*4.4 Performance Risk Assurance*

*Performance Risk Assurance (PRA) is defined as the Government's level of confidence that the offeror (including each subcontractor/team member) will meet technical, delivery, quality, and small disadvantaged business subcontracting objectives of the <SYSTEM NAME> contract, based upon the degree that the offeror (including each subcontractor/ team member) has met these same objectives for similar and related efforts, and based upon the feasibility of his proposed management and technical approaches for the <SYSTEM NAME > contract* [Bergey 2002].

*4.5 Source Selection Demonstration*

*Results of the Source Selection Demonstration will be used to verify the feasibility and flexibility of the proposed approaches and claimed capabilities to satisfy the <SYSTEM NAME> requirements, including the offeror's capability to design and evaluate software architectures, and the offeror's understanding of the requirements* [Bergey 2002].

EXAMPLE 4

*Modifiability – the extent to which the system can be changed quickly and cost effectively* [Fisher 2008].

*Portability – the extent of the system's ability to run under different computing environments* [Fisher 2008].

*Reusability – the extent to which the structure of the system or some of its components can be reused in future applications* [Fisher 2008].

EXAMPLE 5

*Results of the pre-award demonstration will be used to verify the feasibility and flexibility of the proposed approaches and claimed capabilities to satisfy the requirements; and, the offeror's understanding of the requirements, including the methods of evolution of the software architecture* [Fisher 2008].

### 7.14.3 Section L - Instructions to Offerors

EXAMPLE 1

*VOLUME 3 - TECHNICAL*

*This Volume shall contain a full discussion of how the offer and proposed approach intends to satisfy requirements identified in the respective paragraphs of the RFP* [Bergey 2002].

*Software Architecture*

*For each paragraph associated with the software architecture in the Statement of Work (SOW), the offeror shall describe the proposed software architecture, the approach to the development and evaluation of the final software architecture and how this approach will result in a software architecture to meet the RFP requirements* [Bergey 2002].

*VOLUME 4 - PERFORMANCE RISK*

*Volume 4 shall contain a full discussion of how the offeror intends to satisfy the RFP requirements indicated below.*

*Volume 4 will be partitioned as follows* [Bergey 2002]*:*

*Past Performance* [Bergey 2002]

*Management Control Environment*

*Organization*

*Project Management*

*Data Management*

*Schedule*

*Facilities*

*The contents of these Sections are defined as follows* [Bergey 2002]:

*4.1 Past Performance* [Bergey 2002]

*Describe work performed on software projects similar in scope to the requirements for <SYSTEM NAME>, to include design methodology, software architecture design, software architecture evaluation, software integration, integration of NDI software, utilization of industry standards for developing and integrating software (e.g., open system architecture), software security, computer aided software engineering (CASE) tools, and original estimated lines of code versus actual lines of code at completion* [Bergey 2002].

*Discuss concurrent engineering approaches, including software architecture development and evaluation that were used, including lessons learned, and resulting engineering, manufacturing, and equipment improvements that enhanced equipment and contract performance* [Bergey 2002].

*In the event that the offeror/subcontractor(s) (if applicable) has not had applicable contracts, a summary of other experience with similar and/or related work over a like period of time shall be submitted with POCs for each customer* [Bergey 2002].

*The Government may elect to verify all or some past performance data provided in the proposal by obtaining additional information outside of the written content of the proposal. In addition, the Government may consider relevant data extrinsic to the proposal which is otherwise available to the Government. In the event of an unresolved discrepancy, the Government-obtained data will take precedence* [Bergey 2002].

*For the software architecture and software architecture evaluation portion of the demonstration, the offeror shall conduct an Architectural Trade-Off Analysis Method (ATAM) prior to submission of proposal following the evaluation steps described in the Attachment A: Architectural Trade-Off Analysis Method (ATAM) Evaluation Steps to this PPI. The offeror must use scenarios provided by the Government in the RFP as part of this ATAM* [Bergey 2002].

*The offeror must designate a Demonstration Director who will be the sole responsible person to interface with the Government-appointed Demonstration Director/Leader during the conduct of the demonstration. The offeror's designee must be identified prior to the demonstration and must be available during the entire demonstration* [Bergey 2002].

*For the purposes of the demonstration, the requirements to be demonstrated are those stated in the system specification, including those requirements related to the software architecture and the software architecture evaluation* [Bergey 2002].

*For conduct of the demonstration the offeror shall prepare the Source Selection Demonstration plans/procedures to be used in conducting the demonstration. The system capabilities will be demonstrated in the following order* [Bergey 2002]:

*Weeks one and two* [Bergey 2002]:

1. *Software architecture*
2. *<Other capability to be demonstrated>*
3. *<Other capability to be demonstrated>*

*Weeks three and four:*

1. *<Other capability to be demonstrated>*
2. *<Other capability to be demonstrated>*

*To the extent that the software and associated software architecture to be demonstrated differs from that which is offered for delivery, the offeror must completely describe the differences in this volume. The offeror shall fully describe in this volume his approach to providing the proposed software and associated software architecture meeting the requirements of the demonstration* [Bergey 2002].

*No demonstrations will be performed without procedures submitted as part of the proposal* [Bergey 2002].

EXAMPLE 2

*The steps of the evaluation method are* [Fisher 2008]:

- *Express the candidate architecture(s) in a common syntactic architectural notation and with a common granularity. (Typical views solicited include the process view, the module (logical) view, and a data flow view.)*
- *For each scenario, determine whether the candidate architecture supports this task without modification (i.e., can the system carry out this scenario without human intervention or whether the candidate architecture needs to be modified in order to support the task*
- *For each scenario executed and this execution indicating need for modification, the contractor will identify computational components affected by that scenario execution. (This requires in-depth knowledge of the architecture which would typically be provided by a complete set of specifications. Catalog the identified modification(s) from the following list:*
  - *Change to data connection between components*
  - *Change to control connection between components*
  - *Change to internals of a component*
  - *Introduction of new (or deletion of old) component*
  - *Introduction of new (or deletion of old) data or control connections*
- *For those scenarios executed that require modification(s) to the software architecture, the contractor will determine how many components within each architecture are affected by multiple, different in kind, scenarios. (This may identify a component that (a) has been designed to be responsible for too many differing concerns; or (b) needs to be further decomposed in the documentation for the evaluation exercise.)*
- *For each scenario executed, modifications to the software and associated architecture are recorded on change requests which contain proposed modifications in all software documentation, e.g., requirements, design, and software architecture design rationale. These change requests form the basis for an estimate of the effort required to make the change(s).*

- *For the change(s) for each scenario, the effort required in man-days to make the modifications is estimated. The effort must include all aspects of making the actual change, including requirements analysis, functional analysis, hardware/software requirements, modification to the documentation, further evaluations, planning the modifications, etc. Estimates of effort must be made with a validated estimation method agreed upon before initiation of the contract.*
- *The contractor will conduct jointly with the Government a walkthrough of the software architecture and the proposed changes for each scenario executed. These walkthroughs will allow a mutual understanding of the proposed changes and further validate the effort estimates. Validated estimates are then compared to the contractual requirements, and weaknesses and deficiencies are identified.*

## 7.15 Software Architecture

### 7.15.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *Following the completion of the software architecture design, the resolution of weakness and deficiencies, and prior to evaluation, the contractor will plan and jointly conduct with the Government an evaluation readiness review to determine that the software architecture design is sufficiently complete to enable evaluation and to identify any issues in the design* [Fisher 2008].
>
> *Weaknesses or deficiencies in the software architecture found during this review will be entered into the contractor's corrective action system and resolved by the contractor to the software architecture evaluation* [Fisher 2008].

### 7.15.2 Section M - Evaluation

### 7.15.3 Section L - Instructions to Offerors

### 7.16 Software Architecture Pre-Award Demonstration

#### 7.16.1 Section C - SOW/SOO; Requirements

#### 7.16.2 Section M - Evaluation

#### 7.16.3 Section L - Instructions to Offerors

EXAMPLE 1

*The Government intends, through Pre-Award Demonstration , to verify the capabilities of the proposed hardware and software items and associated software architectures. Results of the* Pre-Award Demonstration *will be used to verify the feasibility and flexibility of the proposed approaches and claimed capabilities to satisfy the <SYSTEM NAME > requirements. The demonstrations must be sufficient to verify the proposed approaches and claimed capabilities. The offerors shall conduct demonstrations using existing hardware/software. It is not the Government's intent to burden the offerors with development of <SYSTEM NAME > unique hardware/software for the purposes of this demonstration* [Bergey 2002].

*Demonstrations will take place at the Government facilities at <LOCATION>. The demonstration is solely an offeror demonstration with Government representatives observing. The Government may query the offeror during the demonstration regarding the proposed capability being demonstrated or regarding the plans and procedures being performed* [Bergey 2002].

*Volume XX of the proposal will contain the Pre-Award Demonstration plan and procedures, which will be used by the offeror during the conduct of the demonstration. The plan and procedures will be developed using as a guide for format and content <ACQUIRER'S STANDARD TEMPLATES>* [Bergey 2002].

*The plan and procedures will address all demonstrations and their sequence, and specific schedules of events for each demonstration, as defined in this section of the RFP. The demonstration schedule shall be in a matrix format as shown by the EXAMPLE below. Offeror will not be allowed to conduct simultaneous demonstrations. The demonstration plan and procedures are considered part of the proposal and as such, the Government will assess the plan and procedures. The Government may forward comments to the offeror based upon such assessments. The plan and procedures submitted in this volume, as modified as a result of Government comments, will be the only ones used by the Government and the offeror during the demonstrations. Any deviations or changes to these plans and procedures will require the offeror during his scheduled demonstration period to review, in detail with Government observers, the reason for the deviation/change and explain how that deviation/change is necessary to verify the capability being demonstrated. This review shall be conducted prior to the demonstration involving the deviation/change* [Bergey 2002].

*The offeror will be allotted four (3) weeks, for a total of 130 hours, in which to conduct and complete his demonstration of the system. The offeror may demonstrate other unique capabilities in addition to the "SOW Requirements to be Demonstrated" within the allotted total time. The offeror shall allocate time for unique demonstrations and re-demonstrations within this time frame. However, re-demonstrations will be performed within the time frame for the specific equipment/software category given in this Section (see EXAMPLE schedule below). The hours of demonstration will be 0800-1130 and 1230-1600 Monday-Friday* [Bergey 2002].

*Offeror must bring sufficient equipment and other material, e.g., documentation, to accomplish demonstrations, as well as spares in the event of equipment failures. Offerors are completely responsible for the physical control and maintenance of their equipment* [Bergey 2002].

*The Government also intends to conduct an audit of all offeror equipment and software to be demonstrated or used in the demonstration. The offeror shall be allowed twelve (12) hours to set up all his equipment/software and to conduct the audit. It is planned that the set up and audit will commence at 0800 hours one day prior to the scheduled start date of the demonstrations, to allow maximum time for demonstrations. The set up and audit will be completed by 2000 hours on the day started. If additional time is needed by the offeror, it will be completed before the demonstrations are started and this additional time, if required, shall be subtracted from the offerors' allowed 130 hours for conducting all of the demonstrations* [Bergey 2002].

*The Government will require the offeror to perform the audit under Government control and direction, including opening the hardware for Government inspection and identifying software. No changes or modification to the equipment or software will be allowed after the audit without Government approval. The Government reserves the right to revalidate the audit or conduct additional audits, as necessary, during the demonstration period* [Bergey 2002].

### 7.17 Software Architecture Quality Requirements

#### 7.17.1 Section C - SOW/SOO; Requirements

GENERAL RECOMMENDATIONS

Section 1 of the RFP specifies system quality requirements from which software architecture requirements (runtime and non-runtime) are derived. They must be stated in terms of [SEI SASS]

- definition of system quality attributes
- specification of acceptable values
- definition of scenarios and test cases
- specification of other requirements (e.g., C4ISR)

Section 2 of the system specification describes the software architecture evaluation methods, such as the Architectural Trade-Off Analysis Method (ATAM) or QAW, to determine if the software architecture can support the satisfaction of the requirements in Section 1 [SEI SASS].

Section 1 of the System Specification should contain system quality requirements and their respective characterizations. Modifiability, reliability, and security are examples of the types of system quality attributes. If reliability is a required quality attribute, a characterization might be that “the system will not fail under maximum load.” [Bergey 2002].

A system specification typically has two main sections of interest. Section 1 specifies functional and quality requirements for the system. Here, quality requirements refer to the quality attributes of the system and their respective characterizations. Modifiability, reliability, and security are examples of the types of system quality attributes that may be considered. For example, if reliability is a required quality attribute, a characterization might be that the system must meet a specific mean time between failure (MTBF) requirement. Eliciting the quality attributes of primary interest as well as their characterizations is part of the ATAM [Bergey 2002].

Section 2 of the system specification describes the software architecture evaluation methods (such as the ATAM) that the supplier must use to evaluate the software architecture during the post-award phase of the acquisition. The evaluation results will be the basis for determining if the software architecture can support the satisfaction of the requirements in Section 1 of the system specification [Bergey 2002].

Sometimes an acquisition organization will elect (or is required) to include a statement of objectives (SOO) in the RFP instead of a SOW. In these cases, the contract language that would traditionally be included in the SOW (to describe the requirements for software architecture evaluation) should be included under Section H (Special Contract Requirements) of the RFP [Bergey 2002].

### 7.17.2 Section M - Evaluation

### 7.17.3 Section L - Instructions to Offerors

GENERAL RECOMMENDATIONS

In the Technical volume, you ask the offerors to describe their approach for implementing and analyzing architecture requirements [DOD 2005].

In the Past Performance volume, you ask offerors to describe previous work on software architecture development and architecture evaluation [DOD 2005].

In the Pre-Award Demonstration, you give offerors requirements for demonstrating the capability of their software architecture [DOD 2005].

## 7.18 Software Architecture Reviews and Technical Interchange Meetings

### 7.18.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The contractor will address the progress of the software architecture development effort at normally scheduled acquisition reviews and as required to resolve software architecture related issues. In addition, the contractor will conduct technical interchange meetings with the Government at specific times during the software architecture development and evaluation as specified herein* [Fisher 2008].

### 7.18.2 Section M - Evaluation

### 7.18.3 Section L - Instructions to Offerors

## 7.19 Software Architecture System Evaluations

### 7.19.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *After completion of the system implementation, the contractor will plan and jointly conduct with the Government evaluations against the contractual requirements using the architecture evaluation method and contractor-generated scenarios. The contractor will generate test procedures. The test procedures will be based on an evaluation of software code either by code walkthrough or by actual code modification and testing. The contractor will develop an evaluation agenda (plan) to the Government's satisfaction* [Fisher 2008].

### 7.19.2 Section M - Evaluation

### 7.19.3 Section L - Instructions to Offerors

## 7.20 Software Architecture System Specifications

### 7.20.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*Run-time Requirements. The software architecture will not impede the achievement of the system functions and performance, and the requirements of security, availability, and usability as specified in this specification* [Fisher 2008].

*Non Run-Time Requirements. The software will be compliant with DII COE. The software architecture will not impede the achievement of the following system quality attributes as determined by the evaluation method described in XXXX, using the change scenarios described* [Fisher 2008].

### 7.20.2 Section M - Evaluation

### 7.20.3 Section L - Instructions to Offerors

## 7.21 Throughput Timing

### 7.21.1 Section C - SOW/SOO; Requirements

### 7.21.2 Section M - Evaluation

### 7.21.3 Section L - Instructions to Offerors

GENERAL RECOMMENDATIONS

The technical definition of the computer software architecture and data metamodel, estimated sizing, throughput timing, and growth migration strategy also need to be defined as criteria in Section L of the RFP and in the offeror's proposal [SMC 2004].

# 8 Technical Solutions and Products

The Technical Solutions and Products section of this document provides examples of RFP language which allows the acquiring organization to gain visibility into the activities of evaluating and selecting designs, developing detailed designs, and implementing the designs as a product or product component. The RFP examples apply not only to the product and product components but also to product-related life-cycle processes. Such development may include selecting and adapting existing processes (including standard processes) for use as well as developing new processes [SEI 2006].

## 8.1 Commercial Off-The-Shelf Software (COTS)

### 8.1.1 Section C - SOW/SOO; Requirements

GENERAL RECOMMENDATIONS

Contract requirements should address commercial off-the-shelf software (COTS) market place issues in light of the total system lifetime: These issues include [SEI SASS]

- technology refresh
- version upgrade plans
- market and technology watch groups
- evolvable architecture
- test beds and prototypes
- supplier support
- planned reassessments
- appropriate license agreements (e.g., pass-through)
- substantial justification for COTS product modification
- accommodation of process mismatch

### 8.1.2 Section M – Evaluation

GENERAL RECOMMENDATIONS

Consider criteria in the following areas for judging the bidders' proposals when choosing a COTS integration contractor [SEI SASS]:

- candidate supplier and product, including references and bidder demonstrations
- technology refresh plan
- knowledge of COTS market and domain
- past experience and success at integration of COTS products in this domain
- strawman system (hardware, software, and people) architecture
- plans for COTS upgrade and configuration management
- licensing proposals
- understanding simultaneity of system context, architecture, and marketplace tradeoffs
- proposed CBS development process
- criteria for acceptance of COTS components from vendors and other integrators
- initial identification of COTS risks and mitigation plans
- plans for early involvement of stakeholders
- recognition and treatment of parts that are as-is cots, modifications, custom-developed, and so forth

### 8.1.3 Section L - Instructions to Offerors

### 8.2 Commercial Off-The-Shelf Software Use

#### 8.2.1 Section C - SOW/SOO; Requirements

#### 8.2.2 Section M - Evaluation

EXAMPLE 1

Proposal Requirement #X: Commercial off the Shelf (COTS) Use [USAF 2005]

*The proposal requirement will be met when the Offeror proposes the appropriate use of COTS software consistent with the software architecture, including:*

*Addressing COTS product selection criteria, including TMOS requirements allocation and trade studies.*

*An evolutionary path consistent with the TNOM software architecture covering total life of the system to include proposed solutions to obsolescence issues.*

*Proposed plans for addressing the risks associated with COTS usage*

#### 8.2.3 Section L - Instructions to Offerors

EXAMPLE 1

Proposal Requirement #X: Commercial off the Shelf (COTS) Use [USAF 2005]

*Provide a detailed explanation of the plan to ensure interoperability between all system components (to include COTS/reuse/NDI) and products during and after the selection process. Provide examples from your previous programs of successful implementation of COTS software elements as parts of operational systems.*

*Outline the process for implementing and maintaining each COTS SW product. Address how conflicts among components associated with COTS software are minimized; concentrate on the integration process of those components into TMOS. Address how COTS changes from outside suppliers will be handled and your plans for managing supplier relationships. Discuss the security considerations toward the selection of COTS for TMOS implementation.*

*Identify current IPv6 capabilities in proposed COTS SW products. Describe risks associated with providing full IPv6 compliance for COTS SW. Describe the risk mitigation strategy if COTS SW IPv6 availability is delayed.*

## 8.3 Human Systems Integration/Human Factors Engineering

### 8.3.1 Section C - SOW/SOO; Requirements

### 8.3.2 Section M - Evaluation

EXAMPLE 1

> *The Government will evaluate the extent to which the Offeror provides an effective Human Systems Integration/Human Factors Engineering (HSI/HFE) approach that will reduce rework, delay in operational acceptance, staffing and training costs* [SEI 2007].

### 8.3.3 Section L - Instructions to Offerors

GENERAL RECOMMENDATIONS

Describe the Offeror's strategy to incorporate human systems integration (HSI) considerations into the software development, integration and test phases. Show how operations products (e.g., user's manuals, operator's manuals, Tech Orders, rules and guidebooks) include HSI considerations. Include any external data and operator participation required to develop the operations products such as reports used by operators [SEI 2007].

## 8.4 Independent Witnessing of Software Test Activities

### 8.4.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The contractor shall provide for the independent witnessing of the conduct of software testing as specified in the approved Software Quality Assurance (SQA) Plan. Included in the witnessing of the test is assurance that the approved test procedures are being followed, that accurate records of the tests are being kept, that all discrepancies discovered during the tests are being properly reported, documented, and the certification of the associated test reports are duly performed* [Army 2003].

### 8.4.2 Section M - Evaluation

### 8.4.3 Section L - Instructions to Offerors

## 8.5 Interface Design and Management

### 8.5.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The Contractor shall*: [USN 2007a]

i. *Clearly define and describe all component and system interfaces;*

ii. *Define and document all subsystem and configuration item (CI) level interfaces to provide full functional, logical, and physical specifications;*

iii. *Identify processes for specifying the lowest level (i.e. subsystem or component) at and below which it intends to control and define interfaces by proprietary or vendor-unique standards and the impact of that upon its proposed logistics approach. Interfaces described shall include, but not be limited to, mechanical, electrical (power and signal wiring), software, firmware, and hardware.*

iv. *Identify the interface and data exchange standards between the component, module or system and the interconnectivity or underlying information exchange medium;*

v. *Consider using these interfaces to support an overall information assurance strategy that implements Information Assurance (IA) Processes in accordance with DoD Instruction 8500.2 (dated February 6, 2003) and*

vi. *If applicable, select external interfaces from existing open or Government standards with an emphasis on enterprise-level interoperability. The Contractor shall describe how its selection of interfaces will maximize the ability of the system to easily accommodate technology insertion (both hardware and software) and facilitate the insertion of alternative or reusable modular system elements.*

vii. *Describe the extent that the change or configuration management process proposed will use "community of interest" (See Appendix 10) teams in an integrated team approach to effectively identify how individual change(s) impact the system's internal or external interfaces and information exchange standards.*

### 8.5.2 Section M - Evaluation

### 8.5.3 Section L - Instructions to Offerors

EXAMPLE 1

*Interface Design and Management* - *The Offeror shall describe how it will clearly define component and system interfaces. At a minimum, the Offeror shall address the following:*

a. *The Offeror shall describe how it will define and document all subsystem and configuration item (CI) level interfaces to provide fully functional, physical and electrical specifications.*

   i. *The Offeror shall identify processes for specifying the lowest level (i.e. subsystem or component) at and below which it intends to control and define interfaces by proprietary, vendor-unique standards, as well as the impact of those standards upon the proposed modularity and logistics approach.*

   ii. *Interfaces described shall include, but not be limited to, mechanical, electrical (power and signal wiring), software, firmware, and hardware.*

*iii. The Offeror shall address the interface and data exchange standards between the component, module or system and the interconnecting or underlying information exchange medium.*

*iv. The Offeror shall state how these interfaces support an overall Information Assurance strategy that provides a defense in depth in accordance with CJCSI 3170.01E and*

*b. The Offeror shall describe how interfaces will be selected from existing open or Government standards with emphasis on system-level or enterprise-level (where applicable) interoperability. The Offeror shall describe how its selection of interfaces will maximize the ability of the system to readily accommodate technology insertion (both hardware and software) and facilitate the insertion of alternative or reusable modular system elements.*

*c. The Offeror shall describe how its system will allow for:*

*i. Quickly interconnecting, reconfiguring, and assembling existing systems, subsystems, and components;*

*ii. Interchanging and using information, services and/or physical items among components within a system; items among systems within an integrated architecture, platform, PEO, Community of Interest, or a DoD component;*

*iii. Supporting reuse of software and the common use of components across various product lines;*

*iv. Transferring a system, component, or data, from one hardware or software environment to another.*

*d. The Offeror shall describe the degree to which the defined interfaces will support an Information Assurance (IA) strategy that implements IA Processes in accordance with DoD Instruction 8500.2 (dated February 6, 2003)*

*e. The Offeror shall describe the degree to which proposed interfaces use defined commercial or Government standards as called for in Section C.*

## 8.6 Inter-Component Dependencies

### 8.6.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Contractor's design approach shall result in a layered system design, maximizing software independence from the hardware, thereby facilitating technology refresh. The design shall be optimized at the lowest component level to minimize inter-component dependencies. The layered design shall also isolate the application software layers from the infrastructure software (such as the operating system) to enhance portability and to facilitate technology refresh. The design shall be able to survive a change to the computing infrastructure with minimal or no changes required to the application logic. The interfaces between the layers shall be built to open standards or available to the Government with at least GPR rights. The system architecture shall minimize inter-component dependencies to allow components to be decoupled and re-used, where appropriate, across various XXX programs and platforms.*

### 8.6.2 Section M - Evaluation

### 8.6.3 Section L - Instructions to Offerors

## 8.7 Net-Centric Strategy

### 8.7.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The contractor shall ensure that any IT systems covered in this procurement or identified in this RFP/RFQ support the goals of the DoD Net-Centric Data Strategy dated May 9, 2003* [DOD 2004b].

*Also, the contractor must ensure that any IT systems covered in this procurement or identified in this RFP/RFQ meet the requirements detailed below. Additionally, it is acceptable for vendors and/or integrators to provide functionality (via wrappers, interfaces, extensions) that tailor the Commercial off-the-shelf software (COTS) system to enable these requirements below (i.e. the Commercial off-the-shelf software (COTS) system need not be modified internally if the vendor/integrator enables the requirements through external or additional mechanisms. In this case, these mechanisms must be acquired along with the Commercial off-the-shelf software (COTS) system procurement)* [DOD 2004b].

*Access to Data. The contractor shall ensure that all data managed by the IT system can be made accessible to the widest possible audience of Global Information Grid (GIG) users via open, web-based standards. Additionally, the system's data should be accessible to GIG users without 1) the need for proprietary client-side software/hardware, or 2) the need for licensed user-access (e.g. non-licensed users should be able to access the system's data independent to the licensing model of the Commercial off-the-shelf software (COTS) system). This includes all data that is used to perform mission-related analysis and processing including structured and unstructured sources of data such as databases, reports, and documents. It is not required that internal, maintenance data structures be accessible* [DOD 2004b].

*Metadata. The contractor shall ensure that all significant business data made accessible by the IT system is tagged with descriptive metadata to support the net-centric goal of data visibility. Accordingly, the system data shall be tagged to comply, at a minimum, with the DoD Discovery Metadata Specification (DDMS) . This specification is available at the DoD Metadata Registry found at http://diides.ncr.disa.mil/mdreg HomePage/mdregHome.portal. The system should provide DoD Discovery Metadata Specification (DDMS) compliant metadata at an appropriate level based on the type of data being tagged. It is not required that individual records within databases be tagged; rather it is expected that the database itself or some segment of it is tagged appropriately. Additionally, the contractor shall ensure that all structural and vocabulary metadata (metamodels, data dictionaries) associated with the exposed system data be made available in data formats and definitions. This includes proprietary metadata if it is required to effectively use the system data* [DOD 2004b].

*Enterprise Services/Capabilities. The contractor shall ensure that key business logic processing and other functional capabilities contained within the IT system are exposed using web-based open standards (e.g. APIs provide for Web Services-based access to system processes and data). The level of business logic exposure shall be sufficient to enable reuse/extension within other applications and/or to build new capabilities. The contractor shall provide an assessment of how any licensing restrictions affect or do not affect meeting the goals of re-use and exposure as Global Information Grid (GIG)-wide enterprise services* [DOD 2004b].

*Optional Components/Modules. The contractor shall ensure that all standard and/or optional components of the IT system are identified and procured in a manner that ensures the requirements outlined in this document are met* [DOD 2004b].

### 8.7.2 Section M - Evaluation

### 8.7.3 Section L - Instructions to Offerors

## 8.8 Net-Centric Technical Requirements Document (TRD)

### 8.8.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*Include a reference to* Net-Centric Enterprise Solutions for Interoperability(NESI) Part 3: Migration Guidance *in the SOW Section 2, Applicable Documents (BP1792)* [USN 2007].

*Include a reference to* Net-Centric Enterprise Solutions for Interoperability (NESI) Part 4: Node Guidance *in the SOW Section 2, Applicable Documents (BP1793)* [USN 2007].

*Include a reference to* Net-Centric Enterprise Solutions for Interoperability (NESI) Part 5: Developer Guidance *in the SOW Section 2, Applicable Documents (BP1794)* [USN 2007].

*Include a reference in the SOW Section 2, Applicable Documents to the Technical Evaluation Checklist for measuring net-centric compliance (BP1795)* [USN 2007].

*Include in the TRD specific requirements extracted from the* Net-Centric Enterprise Solutions for Interoperability (NESI) *guidance based on the net-centric capabilities and functions the Government needs as part of the acquisition (BP1789)* [USN 2007].

### 8.8.2 Section M - Evaluation

### 8.8.3 Section L - Instructions to Offerors

## 8.9 Network Architecture and Functionality

### 8.9.1 Section C - SOW/SOO; Requirements

### 8.9.2 Section M - Evaluation

EXAMPLE 1

> *The TMOS Contract requires the development of the TSAT network architecture and design. This section provides criteria that will be used to evaluate the Offeror's proposed network architecture* [USAF 2005].

Proposal Requirement #X: Initial TSAT Network Architecture

> *The proposal requirement will be met when the Offeror provides an initial TSAT network architecture, analysis of shortfalls, and plan to evolve the initial architecture, resulting in a TSAT network architecture that:*
>
> *Forms a basis for meeting all threshold functional and performance requirements for the TSAT network as defined in the TSAT System TRD and is consistent with applicable sections of the DoD Information Technology Standards Registry (DISR), DoD CIO memoranda, the Network-Centric Operations and Warfare Reference model, Net-Ready KPP, and GIG Systems Engineering working group outputs.*
>
> *Provides technically sound, manageable and cost-effective solutions to: quality of service; routing; support for mobile, receive-only, and disadvantaged terminals, networks, and users; and network support for information assurance.*
>
> *Provides an effective tradeoff between functionality, performance, and security to derive required information flows across the red/black interface at the edge of the GIG black core network consistent with the selected network architecture, including taking into account realistic considerations for government restrictions on information passing across such interfaces. The Offeror provides an approach to TSAT network architecture/design with fallback options if needed due to red/black information transfer restrictions.*
>
> *Demonstrates an understanding of the TSAT network boundary and the implications for performance, security, and interoperability, by defining the boundaries, roles, and functions of network elements within the TSAT network and between the TSAT network and external network elements.*
>
> *Identifies sources and specific anticipated types of uncertainty and change in external networks, network standards, interfaces, and policies. The Offeror highlights specific network architecture features which accommodate such changes while minimizing the impact on network performance, manageability, security, cost, and schedule.*
>
> *Provides an approach and rationale for how the TSAT network will interface with other black core networks to maximize network capabilities while meeting security requirements.*
>
> *Documents specific features enabling the proposed network to perform well in nominal conditions, degrade gracefully under stressed conditions, and support required variations in the amount of traffic, geographic density of traffic, application mix, circuit to packet ratio, and differing priorities of traffic.*
>
> *Is shown to support the expected number and types of terminals and networks as defined in the DISA 1-4-2-1 scenario, TSAT and TMOS TRDs, and other Government furnished scenarios, and is scalable to higher levels of performance if required.*

*Is compatible with the GIG architecture and the architecture of DoD Tier 2 and Tier 3 networks as defined in the Net-Centric Implementation Directive.*

*Makes effective use of COTS hardware and software where appropriate, and describes a pragmatic approach for compliance with commercial (e.g. IETF) standards for the use of IPv6 and other protocols.*

Proposal Requirement #X: Analysis and Approach

*The proposal requirement will be met when the Offeror:*

*Provides a credible approach to maturing the network architecture to fully meet network requirements in the TSAT and TMOS TRDs. The Government reserves the right to evaluate and give evaluation credit for proposed features that meet stated objective requirements of the TSAT TRD.*

*Provides sound engineering analysis identifying and describing the shortfalls of the initial TSAT network architecture and identifies where additional engineering development is needed to meet all requirements.*

*Identifies appropriate trade studies for selecting between candidate network architectures and protocols. These trade studies should include routing protocol selection, network interface configuration, quality of service architecture, and trades between security and performance. Trade criteria may include performance, interoperability, scalability, robustness, security, government policy, and overhead. Proposes a high-level schedule for resolution of each key trade coordinated to major TMOS/TSAT contract milestones/events.*

*Identifies an appropriate and robust set of system engineering methods and tools (including test bed and simulation) that will be used to complete trade studies. The Offeror provides a plan which maps the methods and tools to the trade studies and includes proper technical and schedule justification.*

Proposal Requirement #X: Integration and Test

*The proposal requirement will be met when the Offeror provides an approach to testing and integration of the network architecture that:*

*Demonstrates that the network architecture accommodates the constraints of the TSAT space and terminal segments, including optimization of the network design for TSAT terminals, TSAT satellites, and the CONUS Ground Gateway Element (CGGE).*

*Demonstrates an understanding of TSAT network testing that incorporates interdependencies with external elements, including NSA/GIG IA architecture, GIG QoS, routing, mobile network approaches, and Network Centric Enterprise Services (NCES).*

*Describes and provides engineering rationale for a set of simulation and test bed facilities (including use of non-TMOS testbeds as appropriate) to test and validate the TSAT network, including mapping to the identified shortfalls and risks and mapping of network tests to TMOS and TSAT need dates.*

*Provides specific simulations and tests that are critical to the network design, with engineering justification as well as an approach to coordinating design and test activities with space hardware testing.*

*Defines space and terminal network hardware and software needed to support network design, network requirements verification, and network test. Need dates provided by the Offeror meet the proposed TMOS and TSAT schedules.*

Proposal Requirement #X: Risk Identification/Mitigation

*The proposal requirement will be met when the Offeror identifies and analyzes the list of prioritized risks according to probability of occurrence and severity of consequence. The risk analysis adequately justifies these risks and includes isolation of causes and determination of effects. For associated risk-related activities, the Offeror identifies organizational responsibilities, provides risk burndown plans, and includes a realistic work schedule in the IMS and costs shown in the CWBS which are consistent with objectives for TSAT/TMOS milestones.*

### 8.9.3 Section L - Instructions to Offerors

EXAMPLE 1

Subfactor X: TSAT Network Architecture and Functionality [USAF 2005]

Proposal Requirement #X: Initial TSAT Network Architecture

*Provide in Attachment MC5 an initial TSAT network architecture and description. Attachment MC5 should conform to Attachment 9 of Section L, "TSAT Network Architecture Instructions". Attachment MC5 should only include your response to Proposal Requirement #X. This initial TSAT network architecture will be evaluated in accordance with the criteria specified in Section M, 4.3.2.1.*

Proposal Requirement #X: Analysis and Approach

*Provide a plan for maturation of the TSAT network architecture, including the following:*

*Compare the initial network architecture with key TRD requirements.*

*List and describe the shortfalls of the initial architecture and explain where additional engineering development is needed to meet all requirements. Identify alternative network architecture approaches, protocols, and trade studies for selecting between them. Describe the tools and methods used to perform this work.*

*Explain the activities planned in order to mature the architecture into a system level network design meeting all requirements. Identify trade studies for selecting between candidate network architectures and protocols. These trade studies should include routing protocol selection, network interface configuration, quality of service architecture, and trades between security and performance. Trade criteria may include performance, interoperability, scalability, robustness, security, government policy, and overhead. Propose a high-level schedule for resolution of each key trade coordinated to major TMOS/TSAT contract milestones/events.*

*Identify all relevant constraints to maturation of the network architecture.*

Proposal Requirement #X: Integration and Test

*Provide a plan to integrate and test the final network implementation that:*

*Describes how to ensure the network design accommodates the TSAT space payload and terminal constraints.*

*Discusses how to optimize the network design across the TSAT satellite, CONUS Ground Gateway Element (CGGE), and TSAT terminal designs. Identify and discuss* *interdependencies with external elements, including NSA/GIG IA architecture, GIG QoS, routing, mobile network approaches, and Network Centric Enterprise Services (NCES).*

*Describes the simulation and test bed facilities expected to be employed to test and validate the network design. Tie this description explicitly to the shortfalls and risks identified in paragraph 4.2.2.2.2. Show how the simulation and test bed work will evolve over the course of development. List and describe specific simulations and tests critical to the network design. Explain how the test activities relate to space hardware testing. Describe any space and terminal network hardware required to complete the network design, network requirements verification, and network test. Provide need dates for required hardware.*

*Describes systems engineering methods and analysis tools (aside from simulation and test beds) that will be used to verify and test the TSAT network.*

Proposal Requirement #X: Risk Identification/Mitigation

*Provide information about network architecture risks that:*

*Includes a prioritized list of technical architecture risks with justification.*

*Describes specific engineering activities that will resolve these risks. Discusses areas where technologies are immature, and presents an approach and schedule for maturing all such technologies.*

*Describes an approach to managing design with regard to uncertainties and key risks, with specifics on network design features that minimize the impact of such uncertainties.*

*Describes the impact to the network architecture and fallback approaches if Government IA restrictions prevent control or management plane data from being communicated across red/black boundaries or between peer GIG black core networks.*

### 8.10 Network Management and Operations

#### 8.10.1 Section C - SOW/SOO; Requirements

#### 8.10.2 Section M - Evaluation

EXAMPLE 1

Subfactor 3: TSAT Network Management and Operations [USAF 2005]

Proposal Requirement #X: TSAT Network Management and Operations Architecture

> *The proposal requirement will be met when the Offeror proposes an initial TMOS architecture, analysis of shortfalls, and plan to evolve the initial architecture, resulting in a TMOS architecture that:*
>
> *Forms a basis for meeting all threshold technical requirements for TNOM, TSAT Network Services element and TSAT GIG Border Element as defined in the TMOS TRD. The proposed architecture is consistent with applicable sections of the Joint Technical Architecture, DoD CIO memoranda, Network-Centric Operations and Warfare Reference Model, Net-Ready KPP, and GIG System Engineering products. The Government reserves the right to evaluate and give evaluation credit for proposed features that meet stated objective requirements of the TMOS TRD.*
>
> *Provides TSAT functionality to operate effectively with the AEHF system. The proposed architecture provides this functionality concurrent with all other TSAT functions.*
>
> *Provides for a seamless transition between TNOM planning and real-time, automated system operations, particularly in the delivery of quality of service. The Offeror effectively allocates functions to centralized and distributed components of the proposed architecture. The Offeror describes and justifies the use of all managed network and security components, including message guards, and explains the impact of such components on the responsiveness of TNOM activities. The Offeror describes an effective, responsive process by which contention for the use of TSAT resources is resolved in accordance with national and operational policies, in a timely fashion, and in a way that is responsive to mission needs. The Offeror also describes the integration of a flexible, extensible decision support system with network management and operations, including planning, and provides concrete information on how the decision support system is used to improve planning, network management, and operations.*
>
> *Provides a robust approach to continuity of operations for TNOM and TSAT Network Services, including a description of the proposed feature sets and architectures of primary, alternate, transportable and distributed TNOM capabilities to provide maximum utility to operators and users, including tactical planning, network management and operations, during normal, autonomy, and endurance operations. The Offeror describes how transitions among facilities are managed in accordance with the TSAT system concept of operations.*
>
> *Includes a robust, scalable, and evolvable TGBE architecture that meets all threshold technical requirements for the TSAT GIG Border Element as defined in the TSAT System TRD and can function with minimal management when required.*

Proposal Requirement #X: TMOS OM/NM Initial Design

*The proposal requirement will be met when the Offeror provides an effective top-level design for TNOM and TSAT Network Services, including all functional areas and a specification tree that shows the flow down to Element and subsystem specifications. The Offeror provides a design that:*

*Meets technical requirements in a manner that is consistent with the proposed TNOM architecture, robust to varying demand and patterns of usage, and accommodating of changes over time. The design description provides credible and appropriate supporting data, technical rationale, and a maturity assessment of system components, including the identification and characterization of those components identified by the Offeror as design drivers as well as justification for the selection of the design drivers.*

*Implements highly capable dynamic mission planning, resource control, monitoring, and device configuration for the TSAT network. The TNOM design supports all TSAT network services across the full range of pre-planned and ad-hoc mission scenarios for fixed and mobile terminals on terrestrial, airborne, maritime, and space-based platforms. The Offeror identifies capabilities and constraints of the TSAT network, including both the initial network design and the TSAT concept of operations that impact the design of TNOM and TSAT Network Services. The Offeror also addresses the use of precedence and priority levels throughout the resource allocation lifecycle, including the number of such levels and interactions among these attributes. The Offeror's TNOM architecture supports an approach to MLPP that is consistent with national requirements. The proposed design supports the migration of Satellite Database (SDB) 'requirements' from circuit-switched to a mix of circuit-switched and packet-switched services. The Offeror provides realistic expectations and sound engineering justification for robust performance under a variety of packet and circuit mixes and loading levels.*

*Applies policy-based management and control mechanisms across the TNOM architecture, including planning, resource allocation, and network operations for services specified in the TMOS TRD. The Offeror explains how these mechanisms increase the effectiveness of the proposed design. The Offeror also assesses the impact of these mechanisms on the complexity of the system, especially in relation to the human-machine interface and the role of the human operators.*

*Includes a top-level design for TGBE. The design should scale to meet performance objectives under maximum load as defined in the 1-4-2-1 and other Government furnished scenarios. It should accommodate uncertainties and changes in external elements, standards, interfaces, and policies. The TGBE design is shown to accommodate a robust range of mixes of circuit and packet data at up to full uplink/downlink data rates.*

*Includes engineering analysis regarding the shortfalls of the initial TNOM design and identifies and justifies key trade studies where additional engineering development is needed to meet all requirements.*

Proposal Requirement #X: Inter-domain Planning and Management

*The proposal requirement will be met when the Offeror:*

*Comprehensively identifies the information and communications standards that the proposed design will implement to monitor, control, and configure the TSAT network and to perform inter-domain planning and management with peer and customer networks.*

*The Offeror provides information exchange requirements (IERs) for each TMOS interface that will maximize the quality, responsiveness, and reliability of TSAT network services, support mission planning and replanning in conformance with policy, enable best practices for network management, and ensure the TSAT network meets SLA commitments. IERs should include both TSAT-internal and external interfaces. The Offeror specifies the information content of Service Level Agreements (SLAs) to be established with peer and customer networks. The Offeror defines these agreements in quantitative terms, characterizes the precision and accuracy of SLA contents, and demonstrates how the SLA content supports the TSAT CONOPS and helps to ensure the reliable, predictable delivery of service to the TSAT user.*

*Describes functions and procedures of the proposed TNOM design that are invoked in the inter-domain planning and management of the TSAT network and demonstrates the value of these functions and procedures to the TSAT and TMOS system goals/requirements. The Offeror identifies interactions along mission timelines between TNOM and the planning and management systems of peer and user networks. The Offeror describes how IERs and SLAs are used by TNOM operators, TSAT users, operators of peer networks, mission planners, and GIG NETOPS centers.*

Proposal Requirement #X: Operations

*The proposal requirement will be met when the Offeror:*

*Describes how TMOS will be operationally employed to maximize the probabilities of TSAT and TMOS mission success, including the operational role of the Offeror throughout the period of performance. The operational description is consistent with the TMOS design proposed by the Offeror.*

*Fully identifies and clearly describes the TSAT network services that are proposed to be delivered and managed by TMOS, including a realistic hardware and software implementation approach and plan for optimization. Examples of network services include DNS, IP address allocation/assignment/management, antenna/beam control, and key management. The Offeror provides justification for the selection of these services and explains how each service contributes to TSAT and TMOS mission success. The Offeror defines key remaining trades on network services which may have significant impact on network performance, reliability, or cost.*

Proposal Requirement #X: Risk Identification/Mitigation

*The proposal requirement will be met when the Offeror identifies and analyzes the prioritized list of risks according to probability of occurrence and severity of consequence. The risk analysis adequately justifies these risks and includes isolation of causes and determination of effects. For associated risk-related activities, the Offeror identifies organizational responsibilities, provides risk burndown plans, and includes a realistic work schedule in the IMS and costs shown in the CWBS which are consistent with objectives for TSAT/TMOS milestones.*

### 8.10.3 Section L - Instructions to Offerors

EXAMPLE 1

Subfactor X: TSAT Network Management and Operations [USAF 2005]

Proposal Requirement #X: Architecture

> *Present the TMOS architecture and show that it will form a basis for meeting all threshold requirements for TNOM, TSAT Network Services Element, and TSAT GIG Border Element as defined in the TMOS TRD. Be consistent with applicable sections of the DISR, DoD CIO memoranda, Network-Centric Operations and Warfare Reference Model, Net-Ready KPP, and GIG System Engineering working group outputs.*
>
> *Identify the elements of the architecture that support operation with the Advanced EHF (AEHF) system.*
>
> *In the context of the architecture, describe the relationship between TNOM planning and real-time, automated system operations. As part of this description, identify relevant events along a planning and operations timeline and describe the process for resolution of resource contention. Describe how planning and management functions are allocated among centralized and distributed components of the architecture. Describe the integration of a decision support system with network management and operations, including planning, and provide information on how the decision support system is used to improve planning, network management, and operations.*
>
> *Provide analysis identifying and describing the shortfalls of the initial TNOM architecture and identify where additional engineering development is needed to meet all requirements.*
>
> *Provide a continuity of operations plan for TNOM and TSAT Network Services. The plan should describe each instantiation of TNOM capabilities (primary, secondary, transportable, distributed), identifying its architectural features, as well as how transitions among these instances are accomplished. Illustrate how this approach helps maximize utility to operators and users, including tactical planning, network management and operations, during normal, autonomy, and endurance operations.*
>
> *Provide an initial TSAT GIG Border Element (TGBE) architecture and show how the architecture will address requirements for circuits, IPv6 data, routing, multicast, QoS, and traffic engineering between CGGE and GIG-BE. The TGBE architecture must meet all relevant TRD requirements and be consistent with applicable DISA interface specifications and GIG standards. Discuss features of the TGBE architecture providing robustness, scalability and the ability to function with minimal management as required.*

Proposal Requirement #X: Initial TMOS OM/NM Design

> *Present your top-level design for TNOM and TSAT Network Services. Identify the functions performed by each design element and provide a flow-down of TMOS TRD requirements to the elements of the proposed design. Provide data to support and explain your design decisions. Assess the maturity of each component and identify all components perceived to be drivers of the design. Identify and justify key trade studies where additional engineering development is needed to meet requirements. Identify the capabilities and constraints of the TSAT system that your top-level design will address.*
>
> *Describe specific features of the architecture that provide the ability to modify the design in response to changes in cost/funding, schedule, and requirements. In particular, describe the*

*evolution of TNOM as the DoD migrates from predominantly circuit-switched services to operations incorporating an increasing percentage of packet-switched services. Describe the relationship between TNOM, JCS apportionment, and the Satellite Database (SDB) throughout the lifetime of the system. Identify capabilities and constraints of the TSAT system, including both the initial network design and the TSAT concept of operations that impact the proposed TNOM implementation.*

*The design description should address dynamic mission planning, resource control, monitoring, and device configuration. These topics should be discussed in support of all TSAT network services across the full range of pre-planned and ad-hoc mission scenarios for fixed and mobile terminals on terrestrial, airborne, maritime, and space-based platforms. Identify which aspects of your design are implemented by the central, distributed, and transportable TNOM elements.*

*Describe how precedence and priority levels are implemented in the design to provide an MLPP system in conformance with national policy.*

*Describe the policy-based management and control mechanisms in the design. Assess the impact of your proposed design on the effectiveness and complexity of the system.*

*Present the top-level design for TGBE. Identify the functions performed by each design component and provide a flow-down of TMOS TRD requirements to the components of the proposed design. Provide data to support and explain the design decisions made. The design must define functions and responsibility boundaries between TGBE and the CGGE, and TGBE and GIG-BE. Describe design features enabling TGBE to meet performance under maximum loads and varying mixes of circuit and packet data. Describe how the design can accommodate uncertainties in external elements, standards, interfaces, and policies.*

Proposal Requirement #X: Inter-Domain Planning and Management

*Identify the information and communications standards to be used by the proposed design. Describe all TMOS interfaces including those both internal and external to TSAT. Clearly define how Service Level Agreements (SLAs) will be implemented for the TSAT system. Specify and characterize the information content of these agreements, how SLAs are created, used and monitored, and how conformance with the SLAs is maintained. Define information exchange requirements (IERs) for each TMOS internal and external interface that will maximize the quality, responsiveness, and reliability of TSAT network services, support mission planning and replanning in conformance with policy, enable best practices for network management, and ensure the TSAT network meets SLA commitments.*

*Describe the functions and procedures of the proposed TNOM design that are invoked in the inter-domain planning and management of the TSAT network. Identify interactions along a mission timeline between TNOM and the planning and management systems of peer and customer networks. Describe how IERs and SLAs are used by TNOM operators, TSAT customers, operators of peer networks, and GIG NETOPS centers.*

Proposal Requirement #X: Operations

*Provide a description of how TMOS will be operationally employed. Identify the operational role of the Offeror throughout the period of performance.*

*Identify and describe the TSAT network services that are delivered and managed by TMOS. Examples of potential network services include DNS, IP address allocation/assignment/management, antenna/beam control, and key management. Define and justify key remaining trades on network services which may have significant impact on* *network performance, reliability, or cost. Propose a physical implementation for TSAT network service servers (locations, numbers, redundancy approach) and describe planned trades to optimize the implementation.*

Proposal Requirement #X: Risk Identification/Mitigation

*Identify TMOS risk areas for TNOM, TSAT Network Services, and TGBE. For each major risk, assess the probability and consequence of the risk and identify the approach to risk reduction. Provide an analysis, including justifying rationale, of the required work in each risk area. Where risk reduction is primarily the TMOS contractor's responsibility, show proposed burn-down plans that are consistent with TSAT/TMOS milestones.*

### 8.11 Programming Language Selection

#### 8.11.1 Section C - SOW/SOO; Requirements

| GENERAL RECOMMENDATION |
| --- |
| Effective selection criteria for programming and scripting language(s) that demonstrates how software written with the language(s) will be easily maintainable [SE DEV 2007].<br><br>• Look for:<br>industry standard programming languages, bidder's experience with proposed language (both by project team and enterprise), bidder's experience of proposed language on "similar" projects, number/variety of target compilers (allows for migration of existing source to other/future processors, thus enhancing maintainability), or other criteria that identify candidate languages and support the selection, consistency with legacy programs, software maintenance plan [SE DEV 2007].<br>• Expected threshold:<br>detailed rationale supporting proposed programming languages; software maintenance plan along with the Software Development Plan (SDP) [SE DEV 2007].<br>• Possible strengths:<br>trade studies that identify candidate languages and use comprehensive criteria and objective measurements to select a recommended language; explicit mention of software maintenance in the Software Development Plan (SDP) or in a standalone document [SE DEV 2007]. |

#### 8.11.2 Section M - Evaluation

#### 8.11.3 Section L - Instructions to Offerors

## 8.12 Requirements Traceability

### 8.12.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Contractor will be required to ensure that all system requirements (including those contained in the Initial Capabilities Document, Capabilities Development Document, Capabilities Production Document, and in this Section C) are accounted for through a demonstrated ability to trace each requirement to one or more modules that consist of components that are self-contained elements with well-defined, open and published interfaces implemented using open standards* [USN 2007a].

### 8.12.2 Section M - Evaluation

### 8.12.3 Section L - Instructions to Offerors

## 8.13 Requirements Verification

### 8.13.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The contractor's assessment of the software performance requirements, as documented, shall ensure compliance in the following areas* [MIL-STD-QQQ]*:*

- *Completeness—Collectively, the software requirements shall specify the total product software and provide full implementation of all required functions* [MIL-STD-QQQ]
- *Traceability—The software requirements shall be derived directly from higher level requirements contained in or traceable to system specifications. A cross reference shall be developed indicating where each of the high level requirements are implemented in the detailed requirements. All higher level requirements shall be completely satisfied but shall not exceed those requirements unless approved by the procuring agency* [MIL-STD-QQQ].
- *Consistency—All requirements shall be consistent with one another, with interfacing systems/subsystems, and with those at the next higher level* [MIL-STD-QQQ].
- *Realism—Each detailed requirement shall be reviewed to ensure that it can be achieved* [MIL-STD-QQQ].
- *Testability—The contractor shall ensure that the software performance requirements are expressed in quantitative terms that can be directly translated into acceptance criteria* [MIL-STD-QQQ].

*The Government shall have the option to conduct, or utilize a third party to conduct, an independent verification of the detailed software requirements to assess the satisfaction of the higher level requirements* [MIL-STD-QQQ].

*The contractor shall conduct independent assessments of the software requirements development process to ensure that the detailed software requirements are being determined and documented in accordance with the procedures and standards established by the contractor and by the contract* [MIL-STD-QQQ].

### 8.13.2 Section M - Evaluation

### 8.13.3 Section L - Instructions to Offerors

### 8.14 Reuse

#### 8.14.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *As part of the* Software Development Plan (SDP)*, reuse software engineering and planning shall be addressed. The* Software Development Plan (SDP) *shall contain a WBS that includes the establishment and implementation of a reuse program. Reuse shall be an integral part of the* Software Development Plan (SDP) *, review, audit and reporting. As part of the contractor's SEE, a Software Reuse Library shall be established and maintained after appropriate review and approval by the Government* [USAF 1996].

EXAMPLE 2

> *The Contractor shall reuse preexisting or common items unless a determination is made to not re-use. Exceptions to reuse of pre-existing items must be accompanied by justification such as cost (both of adoption and life cycle support), schedule, functional and non-functional performance, etc. The general objective of these efforts shall be the development of common system and/or common elements or components which meet the performance requirements of the various [organizational] platform missions, where commonality offers the greatest technical and cost benefits* [USN 2007a].

#### 8.14.2 Section M - Evaluation

GENERAL RECOMMENDATIONS

Stipulate that evaluation criteria will include the extent to which an Offeror's proposed technical solution builds on reuse of common functionality (Guidance 1775) [USAF 1996].

Stipulate that evaluation criteria will include the extent to which an Offeror's proposed technical solution builds on well defined services (Guidance 1776) [USAF 1996].

#### 8.14.3 Section L - Instructions to Offerors

EXAMPLE 1

> *All Contractors shall use* Net-Centric Enterprise Solutions for Interoperability (NESI) *to assess the proposed technical solution* [USN 2007].
>
> *Stipulate that the Offeror is to describe how the proposed technical solution reuses services from other systems or demonstrates composeability and extensibility by building from existing reusable components and/or services (Best Practice1790)* [USN 2007].
>
> *Stipulate that the Offeror is to describe how the proposed technical solution demonstrates software practices that support reuse (Best Practice 1791)* [USN 2007].

GENERAL RECOMMENDATIONS

Give specific directions when requesting metric data on software reuse, so proposals can be compared [SEI SASS].

Ask how the offeror determined percentage of code that could be reused [SEI SASS].

Will the system, network, and software architectures be implemented to minimize the amount of modification and additions to reuse code? If so, discuss how this architecture will minimize modification and addition to the code you will reuse [SEI SASS].

Below are examples of approaches to reusability with respect to software; similar examples are appropriate for the reusability of other artifacts [USN 2007]:

- Component-based software: mission applications are architected as components integrated within a component framework.
- Layered software architecture: application software is separated into tiers that separate concerns; minimally, client, presentation, middle, and data tiers.
- Service-oriented architecture (SOA): services enable access to data and application functionality through public interfaces exposed to the enterprise.
- Separation of implementation and interface: services expose mission capabilities through well-defined interfaces and provide reliable and scalable components.

### 8.15 Software Design Assessments

#### 8.15.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

*The contractor shall conduct assessments of the software design during its development to ensure that all software requirements, as approved by the procuring agency, are being satisfied and that the design being documented in accordance with standards established by the contractor and the contract* [MIL-STD-QQQ].

- *Architecture Examination. The contractor shall ensure that the architecture of the computer program is examined for its implementability and capability to support the computational work load. This examination shall be completed satisfactorily prior to the commencement of any program implementation.*
- *Design Walk-Through. The contractor shall employ the software engineering assessment practice of conducting internal design walk-through. A design walk-through of each portion of the software design must be completed prior to that portion of the design being implemented.*
- *Computer System Resources. The contractor shall monitor periodically the availability of computer system resources such as memory, processor time, and input/output capacity. Their availability as contracted against allocated budgets shall be reported as part of the contractor's status reporting system.*
- *Program Functional Flow. The contractor shall provide for the independent assessment of the various types of graphical representations used to depict the flow of program data and control in all required modes of program operation for compliance with established standards.*
- *Interface Definition. The contractor is required to identify and define all internal and external interfaces between the system being developed and all other interfacing systems/subsystems. These interfaces shall be verified as a part of the Design Requirements Verification prescribed below.*
- *Database Definition. The contractor is required to identify and define all computer program data that is used by two or more subprograms. These data definitions shall be verified as part of the Design Requirements Verification Prescribed below.*
- *Design Requirements Verification. The contractor's assessment of the software design, as documented, shall ensure compliance in the following areas:*

#### 8.15.2 Section M - Evaluation

#### 8.15.3 Section L - Instructions to Offerors

## 8.16 System Requirements

### 8.16.1 Section C - SOW/SOO; Requirements

GENERAL RECOMMENDATIONS

RFPs need to contain a description of the requirements of the system to be acquired, such as in a system specification. In some cases, these requirements (based on capability description documents and other information sources) may be general, with the expectation that the offerors will refine these based on their experience and engineering judgment. In other cases, these requirements will be specific, based on clearly defined capabilities and expectations. The ultimate goal is to ensure that the system requirements specifications meet the nine qualities described in IEEE Standard 830-1998, *IEEE Recommended Practice for Software Requirements Specifications*.

- Complete – All external behaviors are defined.
- Unambiguous – Every requirement has one and only one interpretation.
- Correct – Every requirement stated is one that software shall meet.
- Consistent – No subset of requirements conflict with each other.
- Verifiable – A cost-effective finite process exists to show that each requirement has been successfully implemented.
- Modifiable – Software requirements specifications structure and style are such that any changes to requirements can be made easily, completely, and consistently while retaining structure and style.
- Traceable – Origin of each requirement is clear, and structure facilitates referencing each requirement within lower-level documentation.
- Ranked for importance – Each requirement rated for criticality to system, based on negative impact should requirement not be implemented.
- Ranked for stability – Each requirement rated for likelihood to change, based on changing expectations or level of uncertainty in its description.

### 8.16.2 Section M - Evaluation

### 8.16.3 Section L - Instructions to Offerors

## 8.17 Technical Performance Requirements Criteria

### 8.17.1 Section C - SOW/SOO; Requirements

### 8.17.2 Section M - Evaluation

EXAMPLE 1

*The Offeror's system performance specification will be evaluated in conjunction with the proposed technical solution based on the following criteria* [DOD 2006]:

1. *Specification includes the key requirements and functionality identified in the RFP's preliminary system performance specification.*
2. *Performance (including logistics/sustainment/support) requirements are quantifiable and testable and/or verifiable.*
3. *Objective values (goals) are clearly identified and distinguished from firm requirements.*
4. *The operational and support environment is described and defined.*
5. *Environmental design requirements are specified.*
6. *Functional, electronic, physical, hardware, and software interfaces for the system are included.*
7. *System FoS and SoS interoperability and interface requirements are established (both physical and functional). Considers Open Systems and Modularity standards.*
8. *Appropriate use of Government and industry specifications, standards, and guides.*
9. *Verification approaches for all system performance and sustainability requirements included in the specification are complete and appropriate.*
10. *The specification does not include unnecessary requirements and language (e.g., SOW tasks, data requirements, and product or technical solution descriptions)* [DOD 2006].

### 8.17.3 Section L - Instructions to Offerors

EXAMPLE 1

*The Offeror shall propose a System Performance Specification that meets the Government minimum requirements. The specification should be performance based and address the allocation of Government performance requirements plus any derived requirements necessary to describe the performance of the integrated system solution. Elements to be addressed in the System Performance Specification include* [DOD 2006]*:*

1. *Accurate and complete understanding of the performance and support requirements in the Government's preliminary system performance specification included in the RFP.*
2. *Derived requirements necessary to document the system performance and sustainability that will govern the design, development, and test program.*
3. *Identified and documented system-level operational, physical, and functional interfaces that define the program external interfaces and constraints. SoS and FoS interoperability and interface requirements are included for both physical and functional interfaces. Include considerations for Open Systems design.*
4. *A verification section to the specification that delineates the approach to verifying all performance and support characteristics.*

5. *A cross-reference matrix showing the tracking of Government performance requirements to the Offeror's proposed system performance specification (i.e., traceability). The specification should be structured for the proposed system solution and not restricted by the structure of the Government's preliminary system performance specification. Include cross-reference to verification methods* [DOD 2006].

### 8.18 Technology Readiness Assessment

#### 8.18.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *The Developer shall perform a system and software technology readiness assessment, utilizing the Technology Readiness Levels (TRLs) definitions/criteria specified in xxx of this SOW, and then prepare a Technology Readiness Assessment Report IAW DI-MISC-80508A and deliver IAW CDRL xxx. The purpose of the technology readiness assessment is to determine the software maturity state while determining the software development and operational risks. The TRL metrics can be associated with risk using the Technology Readiness Assessment versus Risk Assessment Table provided in Attachment 4 of this SOW* [Army 2006].
>
> *If the assessed TRL is TRL 7 or lower, then the Developer shall prepare a Technology Transition Plan (TTP) IAW DI-MISC 80508A. The purpose of the TTP is to address the programmatic and technical issues required to ensure that the software will be assessed at TRL 8 or above at the completion of its development. The* DOD Technology Readiness Assessment Deskbook *may be used as a guide in the preparation of these reports* [Army 2006].

#### 8.18.2 Section M - Evaluation

#### 8.18.3 Section L - Instructions to Offerors

### 8.19 Technical Solution and Technical Supporting Data

#### 8.19.1 Section C - SOW/SOO; Requirements

#### 8.19.2 Section M - Evaluation

EXAMPLE 1

*The technical solution and technical supporting data factor (subfactor) is satisfied when Offeror's proposal demonstrates* [DOD 2006]:

1. *The Offeror has conducted a series of trade studies, analyses, and modeling and simulations that systematically evaluated the range of alternatives leading to a preferred technical solution. The results support the technical and program requirements and validate the proposed configuration and the corresponding performance in the system specification.*
2. *The trade study process was uniformly and consistently applied and followed the Offeror's documented corporate enterprise processes.*
3. *Trade study and decision criteria addressed the critical cost, schedule, technology, risk, and performance requirements (including operational and sustainment) and other considerations for the program with a high degree of confidence.*

#### 8.19.3 Section L - Instructions to Offerors

EXAMPLE 1

*The Offeror shall provide a summary of the trade studies and analyses accomplished to arrive at the proposed technical solution. The Offeror shall* [DOD 2006]:

1. *Describe the trade study, analysis, and modeling and simulation processes implemented to arrive at the proposed technical solution; explain the level of fidelity of the models and simulations to support accurate and reliable results.*
2. *Provide a summary of the trade studies, demonstrations, and analyses results that support the proposed technical solution and program technical approach.*
3. *Provide a description of the trade study evaluation criteria, how they relate to the key performance requirements and constraints for the program, and the planned technical approach addressed in the contractor's integrated SEP. The data shall address the range of alternatives considered and the important results that support the technical decisions and the program technical approach. If the contractor plans to mature a technology, back up plans should be assessed as well as risk mitigation planning.*

## 8.20 Test and Evaluation

### 8.20.1 Section C - SOW/SOO; Requirements

EXAMPLE 1

> *Environmental Testing: Contractual qualification testing conducted to illustrate the equipment's ability to operate during and after exposure to environmental extremes. The Government should provide within the RFP a comprehensive characterization of intended operational environments. Contractors will then develop tests to verify that system performs reliably in these environments* [DOD 2005].

EXAMPLE 2

> *In addition to functional testing of the software to assure compliance with requirements, the software will be tested such that 100 percent of the software branches (i.e., decision to decision statements) are exercised prior to release in the field. Reasons for not achieving 100 percent execution coverage must be formally documented in the Software Test Report* [USN 2006].
>
> *Software tools (i.e., test coverage analyzers) to automate the branch testing process are available. Intrusive analyzers insert software code into the software under development to capture and record the execution coverage and are appropriate for non-real-time software developments. If a software product under development must operate in real-time, if it is highly memory constrained, or if the software units are very large, non-intrusive analyzers should be used. Non-intrusive analyzers use a separate hardware processor to capture and record this same execution coverage information* [USN 2006].

### 8.20.2 Section M - Evaluation

EXAMPLE 1

> *The Government will evaluate the extent to which the Offeror provides a reasonable and complete strategy for planning and conducting qualification testing and regression testing for each build, for the incremental portion of each software item developed in the build, and for end-to-end build testing including reuse software, commercial item, GOTS, software tools, and test bed software. The strategy credibly shows comprehensive testing is performed, efficient test progression, efficient use of software tools and test beds. The regression test strategy ensures continued adequacy of previously verified software following any changes to the software, including changes driven by problem reports, changed requirements, or integration of subsequent blocks, if applicable. The strategy includes a credible, comprehensive approach for managing and resolving risks and weaknesses identified during test reviews, adequate insight through Government-witnessed tests, and an achievable strategy to obtain test facility certification* [SEI 2007a].

### 8.20.3 Section L - Instructions to Offerors

# References


**[Army 2003]**
U.S. Army. *Program Manager (PM) Handbook for Flight Software Airworthiness (PMHFSA).* 2003.

**[Army 2003a]**
U.S. Army. *Army Regulation 70–1; Research, Development, and Acquisition – Army Acquisition Policy*. December 2003.

**[Army 2006]**
U.S. Army. *Program Manager’s Handbook for Software Safety*. 2006.

**[Army 2008]**
U.S. Army. *AFARS—Appendix AA: Army Source Selection Manual*. Washington, DC: Department of the Army, May 2008.

**[Bergey 2002]**
Bergey, John K.; Fisher, Matthew J.; & Jones, Lawrence G. *Use of the Architecture Tradeoff Analysis Method℠ (ATAM℠) in Source Selection of Software-Intensive Systems* (CMU/SEI 2002-TN-010, ADA403813). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2002.
http://www.sei.cmu.edu/publications/documents/02.reports/02tn010.html

**[Bergey 2005]**
Bergey, John & Morrow, Timothy. *Integrating Software Architecture Evaluation in a DoD System Acquisition*. Presentation at The Software Architecture Technology User Network (SATURN). Software Engineering Institute, Carnegie Mellon University, March 30, 2005.
http://www.sei.cmu.edu/architecture/saturn/2005/clip/clip_1.htm

**[Clements 1996]**
Clements, Paul C., & Northrop, Linda M. *Software Architecture: An Executive Overview* (CMU/SEI-96-TR-003, ADA305470). Pittsburgh, PA: Software Engineering Institute. Carnegie Mellon University, 1996.
http://www.sei.cmu.edu/publications/documents/96.reports/96.tr.003.html

**[DHS 2008]**
Department of Homeland Security. *Software Assurance in Acquisition: Mitigating Risks to the Enterprise: A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing*. October 2008.
https://buildsecurityin.us-cert.gov/swa/acqact.html

**[DHS 2009]**
Department of Homeland Security. *Contract Language for Secure Software - Software Assurance Pocket Guide Series: Acquisition & Outsourcing, Volume 3 Version 1*. February 2009.
https://buildsecurityin.us-cert.gov/swa/downloads/Contract_Language_PocketGuide.pdf

**[DOD 1998]**
Department of Defense. *DoD Integrated Product and Process Development Handbook*. Washington, DC: Office Of the Under Secretary Of Defense for Acquisition and Technology, 1998.
https://acc.dau.mil/CommunityBrowser.aspx?id=106001

**[DOD 2004b]**
Department of Defense. *Defense Acquisition Guidebook*. Washington, DC; U.S. Department of Defense, 2004
https://akss.dau.mil/dag/

**[DOD 2005]**
Department of Defense. *DOD Guide for Achieving Reliability, Availability, and Maintainability*. Washington, DC; Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics), 2005.
http://www.acq.osd.mil/sse/docs/RAM_Guide_080305.pdf

**[DOD 2006]**
Department of Defense. *Guide for Integrating Systems Engineering into DoD Acquisition Contracts, Version 1.0*. Washington, DC; Office of the Under Secretary Of Defense (Acquisition, Technology, and Logistics), 2006.
https://acc.dau.mil/CommunityBrowser.aspx?id=127987

**[DOD 2007]**
Department of Defense. *Defense Federal Acquisition Regulation Supplement.* September 2007.
http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

**[DOD 2008]**
Department of Defense. *Defense Cost and Resource Center* - *Enhancing DoD Cost Analysis – Example RFP Language* - *SRDR*. 2008
http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

**[DOD 2008a]**
Department of Defense. *Defense Cost and Resource Center* - *Enhancing DoD Cost Analysis – Example RFP Language* - *CSDR*. 2008
http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

**[FAR]**
Federal Acquisition Regulation. *Subpart 15.2—Solicitation and Receipt of Proposals and Information.*
http://acquisition.gov/far/current/html/Subpart%2015_2.html#wp1125227

**[Fisher 2008]**
Fisher, Matthew. *Software Architecture in System Acquisitions Module, Draft Evaluation Factors For Award (Section M)*. (Unpublished)

**[Goff 2006]**
Goff, Richard N. *Changes in Open Architecture Contract Language*. Presentation, Open Architecture Industry Day. Defense Acquisition University, 2006.
https://acc.dau.mil/GetAttachment.aspx?id=44964&pname=file&lang=en-US&aid=13053

**[MIL-STD-QQQ]**
Military Standard. *Software Quality Assurance Program Requirements*. (Unpublished)

**[OSJTF]**
Open Systems Joint Task Force. *Implementation and Assessments, RFP Language*.
http://www.acq.osd.mil/osjtf/rfpspeak.html

**[SE DEV 2007]**
Software Engineering Institute. *Software Engineering Development*. Presentation, Software Engineering Institute, Carnegie Mellon University. March 23, 2007.

**[SEI 2006]**
CMMI Product Team. *CMMI® for Development, Version 1.2*. (CMU/SEI-2006-TR-008, ADA455858). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.
http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html

**[SEI 2007]**
Software Engineering Institute. *Human Software Interface*. Presentation, Software Engineering Institute, Carnegie Mellon University. March 23, 2007.

**[SEI 2007a]**
Software Engineering Institute. *Software Test*. Presentation, Software Engineering Institute, Carnegie Mellon University. March 23, 2007.

**[SEI 2007b]**
Software Engineering Institute. *Understanding and Leveraging a Supplier's CMMI® Efforts: A Guidebook for Acquirers* (CMU/SEI-2007-TR-004, ADA465951). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2007.
http://www.sei.cmu.edu/publications/documents/07.reports/07tr004.html

**[SEI 2007c]**
Software Engineering Institute. *Software Simulation*. Presentation, Software Engineering Institute, Carnegie Mellon University. March 23, 2007.

**[SEI SASS]**
Software Engineering Institute. *Software Acquisition Survival Skills*. Course Materials, Software Engineering Institute, Carnegie Mellon University.
http://www.sei.cmu.edu/products/courses/sass.html

**[SMC 2004]**
U.S. Air Force Space and Missile Systems Center. *Space and Missile Systems Center (SMC) Software Acquisition Handbook*. 2004.
http://www.sei.cmu.edu/programs/acquisition-support/publications/handbook1.pdf

**[USAF 1996]**
U.S. Air Force Software Technology Support Center. *Guidelines for Successful Acquisition and Management of Software Intensive Systems (GSAM), Version 2, Appendix M*. 1996.
http://www.stsc.hill.af.mil/resources/tech_docs/gsam2.html

**[USAF 2000]**
U.S. Air Force Software Technology Support Center. *Guidelines for Successful Acquisition and Management of Software Intensive Systems (GSAM), Version 3.0, Chapter 6-8, 10, 12-13*. 2000.
http://www.stsc.hill.af.mil/resources/tech_docs/gsam3.html

**[USAF 2005]**
U.S. Air Force. *Transformational Satellite Communications System (TSAT): Mission Operations System (TMOS) - Section L*. May 2005.
http://www1.eps.gov/EPSData/USAF/Synopses/901/MC%3AFA8808%2D05%2DR%2D0001/TMOSSectionLFinalRelease%2Edoc

**[USAF 2005a]**
U.S. Air Force. *Transformational Satellite Communications System (TSAT): Mission Operations System (TMOS) - Section M*. May 2005.
http://www1.eps.gov/EPSData/USAF/Synopses/901/MC%3AFA8808%2D05%2DR%2D0001/TMOSSectionMFinalRelease%2Edoc

**[USN 2006]**
U.S. Navy. *Software Process Improvement*. Memorandum, Office of the Assistant Secretary, Research, Development, and Acquisition. May 15, 2006.http://acquisition.navy.mil/content/view/full/4628

**[USN 2007]**
U.S. Navy. *Net-Centric Implementation Framework, v 2.0*. Program Executive Office, C4I, USAF Electronic Systems Center (ESC); and Defense Information Systems Agency (DISA). April 30, 2007.
http://nesipublic.spawar.navy.mil/docs/part6/Part6_v2pt1-12Oct07.pdf

**[USN 2007a]**
U.S. Navy. *Naval Open Architecture Contract Guidebook.* Program Executive Office, IWS. April 30, 2007.
https://acc.dau.mil/GetAttachment.aspx?id=183088&pname=file&aid=31912&lang=en-US

**[USN 2008]**
U.S. Navy. Office of the Assistant Secretary of the Navy (Research, Development and Acquisition). September 2008.
http://acquisition.navy.mil/organizations/dasns/rda_cheng

**[USN 2008a]**
U.S. Navy. Department of the Navy *Software Measurement Policy for Software Intensive Systems.* Office of the Assistant Secretary of the Navy. July 2008.
http://sepo.nosc.mil/DoN_Software_Measurement_Policy.pdf

# Index


**A**

Access to Data, 203
Adequacy of response, 180
Agenda items for Developer Kick-Off Meeting, 131
Agreements with international or multi-national defense organizations, 17, 28
Airworthiness, 128, 132, 143, 228
Airworthiness Qualification Plan, 143
Airworthiness Release (AWR), 128
Application logic, 164, 202
Application software layers, 164, 202
Architectural Trade-Off Analysis Method (ATAM), 179, 188
Architecture, 4, 126, 132, 133, 155, 156, 157, 158, 159, 160, 161, 162, 164, 165, 166, 168, 176, 177, 178, 179, 180, 182, 183, 189, 191, 196, 201, 202, 220, 221
Assignment of copyright to Government, 40
Automated software engineering environment, 106

**B**

Board of Contract Appeals, 46, 47, 48, 53

**C**

Capabilities Development Document, 162, 217
Capabilities Production Document, 217
Capability Description Documents, 222
Capability Level 3, 78
Certification and accreditation processes, 57
Characterization of intended operational environments, 227
Classified data systems, 158
CMMI, 78, 101, 106, 110, 230
CMMI Maturity Level 3, 105
Code walkthrough, 191
Commercial off-the-shelf software (COTS), 97, 99, 105, 111, 125, 126, 158, 160, 162, 166, 167, 195, 196, 203
Common Vulnerabilities and Exposures (CVE®)—The Standard for Information Security Vulnerability Names, 74
Common Weakness Enumeration, A Community-Developed Dictionary of Software Weakness Types, 74
Component-based software, 220
Computer database - definition, 16
Computer hardware resource utilization, 60
Computer program - definition, 16
Computer software - definition, 16, 27, 40
Computer Software Configuration Item (CSCI), 131, 139, 141, 146, 154
Computer software documentation, 16, 17, 19, 21, 27, 28, 40
Computer Software Unit (CSU), 139, 146
Computer System Resources, 221
Computer-aided Software Engineering (CASE), 56, 182
Concurrent engineering approaches, 182
Condition Decision Coverage, 150, 151
Confidentiality, integrity, and availability, 72
Configuration control board, 111
Configuration management, 55, 58, 64, 111, 112, 196, 200
Consensus-based standards, 158, 161
Contracting Officer, 9, 14, 20, 21, 22, 25, 26, 32, 33, 34, 37, 38, 40, 41, 45, 46, 47, 48, 50, 51, 52, 53, 54
Contractor Flight Release (CFR), 128
Contractor procedures and records to prove software markings, 24, 37
Contractors or subcontractors performing service contracts, 18, 29
Contractor's written permission to use software, 14

Contracts for commercial items, 50
Contractual non-conformance, 64
Copyright owner of software and special works, 21, 32, 41
Corrective action, 64, 77, 85, 137, 178, 185
Criteria for evaluation of system performance specification, 223
Critical Design Review (CDR), 133, 134
Critical Design Review (CDR) agenda items, 133
Criticality - DO-178B Level A, B, or C criticality, 151
Criticality of hardware, firmware, and software components, 147

**D**

Data evaluation by foreign Governments, 17, 28, 29
Data metamodel, 3, 193
Data-flow structure, 177
Decompile, disassemble, or reverse engineer software, 18, 19, 30
Defect, 59, 117
Defense Federal Acquisition Regulation Supplement. See DFARS
Deferred Delivery Of Technical Data Or Computer Software, 6
Deferred Ordering Of Technical Data Or Computer Software, 7
Definitions, 14, 16, 27, 40, 45, 50
Derived requirements, 223
Description of offeror's previous experience, 101, 106, 110
Description of teaming and subcontractor arrangements, 117
Design information, 161
Design information documentation, 87
Design requirements, 138
Design Walk-Through, 221
Determination of private expense development of software, 17, 28
Developed - definition, 16, 27
Developed exclusively at private expense - definition, 17, 28
Developed exclusively with Government funds - definition, 17, 28
Developed with mixed funding - definition, 17, 28
Development and test resources, 111
Development schedule, 86, 111
DFARS, 4, 5, 6, 7, 8, 10, 11, 12, 14, 15, 16, 18, 20, 26, 27, 30, 32, 39, 40, 41, 42, 43, 45, 48, 49, 50, 54
Direct contact with subcontractors or suppliers, 45
Direct technical visibility, 106
Documentation, 8, 14, 23, 86, 106, 111, 113, 177
DoD Discovery Metadata Specification (DDMS), 203
DoD Instruction 8500.2, 200, 201
DoD Metadata Registry, 203

**E**

End-to-end build testing, 227
Enterprise Services Capabilities, 203
Environmental Testing, 227
Error reporting, 111
Evaluations, 55, 140, 177, 178, 184, 191
Extensible Markup Language Metadata Interchange (XMI), 87, 161

**F**

Failure Modes and Effects Analyses (FMEA), 147
Failure Reporting, Analysis, and Corrective Action System (FRACAS), 137, 147
Fault tree analysis (FTA), 145
Feasibility - defined, 180
Five key software RFP elements, 106
Flight critical capacity, 151
Flight critical software Modified Condition Decision Coverage (NASA/TM-210876), 151
Flight Qualification Test (FQT), 129, 134

Flight Readiness Review (FRR) agenda items, 128
Flight Readiness Review(FRR), 128
Flight Safety critical capacity, 150
Flowdown, 15, 48, 54
Form, fit, and function data - definition, 28
Functional Configuration Audit, 136
Functional Hazard Assessment (FHA), 145, 147
Functional partitioning, 156
Functional testing, 227

**G**

Global Information Grid (GIG), 203
Government Purpose - definition, 17, 28
Government Purpose Rights - definition, 11, 17
Government Purpose Rights five-year or other negotiated period, 19
Government-furnished information (GFI), 11, 15, 41
Growth migration strategy, 154, 193

**H**

Hardware firmware software partitioning, 157
Hazard, 142, 148, 149
Hazard Causal Factor Analysis (HCFA), 138, 145, 147
Hazard Criticality Matrix, 130
Hazard Log, 149
Hierarchical quality model, 168
Human Systems Integration and Human Factors Engineering (HSI/HFE), 198

**I**

IEEE Recommended Practice for Software Requirements Specifications, 222
IEEE/EIA Std 12207, 109
Indemnification, 12, 41
Independent software Quality Assurance reviews, 67
Independent Verification and Validation (IV&V), 88, 114
Independent witnessing of the conduct of software testing, 199
Industry standard programming languages, 216
Information Assurance (IA) strategy, 201
Initial Capabilities Document, 162, 217
In-Process Reviews (IPR), 133
Instructions to offerors (ITO), 117
Integrated development environment, 158
Integrated information development environment (IDE), 88, 89
Integrated Master Plan (IMP), 89, 105, 111, 122, 123
Integrated Master Schedule (IMS), 89, 105, 111, 122, 123, 134, 136, 154
Integrated Product Team (IPT), 122, 126, 147, 165
Integration, Operations, Test, and Evaluation (IOT&E), 135
Intellectual Property (IP) assets, 125, 126
Inter-component dependencies, 163, 164, 202
Interface Definition, 221
Interface Requirements Specification (IRS), 131, 141
Internal change control, 112
Interoperability, 157, 158, 160, 161, 162, 165, 200, 201, 223
Intraoperability, 157

**K**

Key product characteristics, 59

**L**

Layered software architecture, 220
Layered system design, 164, 202
Legacy programs, 216
License to use computer software, 5, 8, 9, 11, 12, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 40, 41, 43, 46, 48, 51, 116, 117, 126, 158, 161, 195, 203
License to use computer software - definition, 29

**M**

Market survey to identify Commercial off-the-shelf software (COTS) candidates, 125
Metadata, 203
Methodology used to perform software sizing and cost estimating, 117
Metrics Usage Plan, 61
Metrics/measures, 60, 61, 88, 105, 117, 133, 168, 169, 220, 225
Metrics/measures performance thresholds, 61
Migration, 157, 163, 193
Migration Guidance, 205
MIL-STD 882D, 148
Minor modification - definition, 17, 29
Model-based process maturity appraisals, 101, 105, 106, 110
Modeling and simulation, 4, 155, 226
Modeling assumptions, 169
Modular design, 156, 157, 158, 159, 160, 161, 162, 163, 165
Modular Open Design, 158
Modular Open Systems Approach (MOSA), 97, 99, 157, 159, 161, 162, 164
Modular Open Systems Design, 159
Modular Open Systems Support Plan, 97
Module Cohesion, 158
Module Coupling, 158
Module size, 116
Module structure, 177

**N**

Net-Centric Enterprise Solutions for Interoperability (NESI), 205, 219
Net-Centric Data Strategy, 203
Noncommercial computer software - definition, 17, 29
Noncommercial Technical Data and Computer Software--Small Business Innovative Research Program, 8, 11, 14, 15, 35, 36
Non-Developmental items (NDI), 97, 105, 111, 125, 126, 158, 162, 166, 182
Non-disclosure agreement, 12, 18, 20, 30, 32, 48
Non-intrusive analyzers, 227

**O**

Offeror demonstration, 186
Offeror's previous experience, 105, 110
Open Architecture, 86, 99, 158, 161, 162, 165
Open Source Software, 126, 166
Open Standards, 99, 156, 158, 159, 160, 162, 164, 202, 203, 217
Open System Architecture, 158
Open system management plan, 158
Operational mode summary, 169
Operations and maintenance requirement, 98
Optional Components/Modules, 204

**P**

Pass through of Commercial off-the-shelf software (COTS) warranties to the Government, 166, 167
Past performance, 4, 99, 105, 181, 182, 189, 216
Peer review, 88, 126
Physical Configuration Audit, 136
Physical modularity, 156
PMO Safety Officer, 135
PMO Specified Safety Requirements, 143, 144
PMO System Safety Management Plan, 143, 144
PMO System Safety Policies, 143, 144
Pre-Award Demonstration, 181, 186, 189
Pre-existing Government rights for use of software, 20, 32
Preliminary Design Review (PDR), 132
Preliminary Design Review (PDR) agenda items, 132
Preliminary Hazard Analysis (PHA), 142
Preliminary Hazards List, 143, 144
Preliminary Readiness Review (PRR) agenda items, 136

Privity of contract between the Government and the Contractor's subcontractors or suppliers, 45
Problem/change reports, 60, 65, 227
Process compatibility topics, 89
Process improvement plan, 61
Process structure, 177
Product lines, 159, 201
Production Readiness Review (PRR), 136
Program Functional Flow, 221
Program management, 114, 123
Program Manager Handbook for Software Safety (PMHSS), 127
Program tracking system, 86
Programming language, 116
Project Management and Oversight,, 78
Project Office System Safety Management Plan, 147
Proprietary solutions, 26, 41, 44, 88, 125, 126, 157, 158, 160, 161, 162, 163, 164, 165, 200, 203
Protection of subcontractors or suppliers computer software rights, 25, 38
Publication of Unlimited rights software by Government, 26, 38
Publicly available computer software, 19, 46, 53

**Q**

Qualification testing, 227
Quality attribute, 67, 168, 188
Quality attributes, 188, 192

**R**

Rationale used for computer resource timing and sizing estimates, 117
Real-time access, 88
Refresh strategy, 157
Reliability, Availability, and Maintainability (RAM), 170
Reliability, Availability, and Maintainability (RAM) Program Plan (RAMPP), 170, 172
Reliability, Availability, and Maintainability (RAM) Rationale, 169
Requirements, 60, 78, 86, 105, 125, 131, 132, 139, 141, 161, 162, 168, 169, 186, 188, 192, 218, 221, 222
Requirements Traceability, 217
Requirements Volatility, 60
Reusable Non-Developmental items (NDI), 125, 158, 162, 166, 167
Reuse, 126, 158, 159, 160, 161, 164, 168, 180, 181, 201, 203, 219, 220, 227
Rights In Noncommercial Computer Software And Noncommercial Computer Software Documentation, 16
Rights In Noncommercial Technical Data And Computer Software--Small Business Innovation Research (SBIR) Program, 27
Rights In Technical Data And Computer Software (Foreign), 42
Rights to use computer software, 8, 12, 14, 17, 18, 20, 21, 22, 23, 24, 25, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 40, 45, 46, 47, 48, 50, 51, 52, 53, 54, 117, 196, 203, See License to use computer software
Risk, 3, 4, 59, 61, 69, 78, 89, 105, 106, 117, 122, 123, 128, 135, 138, 142, 145, 147, 149, 152, 161, 162, 164, 165, 169, 170, 179, 180, 181, 196, 225, 226, 227
Risk Management Plan (RMP), 89
Risk mitigation, 69, 122, 133, 226

**S**

SAE ARP 4761, 145, 147
Safety assessment process, 147
Safety Assessment Report, 145, 147
Safety Assessment Review (SAR), 135, 145, 147
Safety Assessment Review (SAR) agenda items, 131, 135
Safety critical elements, 139, 146
Safety Critical Software, 127, 140, 150
Safety Criticality Functional Analysis (SSCFA), 143, 144

Safety engineering and management program, 152
Safety substantiation and assure compliance, 131
SCAMPI, 105
Scenarios, 178, 182, 183, 191, 192
Schedule baseline, 86
Security, 4, 26, 38, 88, 112, 180, 182, 188, 192
Security acceptance and measurement criteria, 74
Security controls and standards, 72
SEI Capability Maturity Model— Integrated. See CMMI
Separation of open elements from proprietary elements, 125
Sequencing requirements, 134
Service-oriented architecture (SOA), 220
Sharing software development information with the Government, 106
Small Business Innovation Research (SBIR), 8, 9, 11, 14, 15, 22, 27, 30, 31, 33, 34, 35, 36, 38
Small Business Innovation Research (SBIR) data rights, 30, 31, 33, 34, 38
Software Acquisition Planning, 78
Software architecture, 3, 153, 154, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 188, 189, 190, 192, 193
Software architecture evaluation methods, 188
Software architecture evaluation readiness review, 178, 185
Software Architecture Factors And Subfactors To Be Evaluated, 179
Software architecture requirements, 188
Software Assurance Case, 73
Software code, 227
Software Design Description (SDD), 132, 133
Software development approach, 109, 114
Software development capability assessment, 105
Software development experience, 110
Software Development Plan (SDP), 58, 60, 64, 69, 86, 101, 105, 109, 110, 111, 114, 117, 150, 151, 216, 219
Software Development Plan (SDP) rationale, 101, 110
Software development process, 56, 106, 109, 110
Software development process experience, 105, 110
Software documentation, 113
Software Engineering, 105, 109, 228, 230, 231
Software engineering environment (SEE), 116, 117, 219
Software Failure Modes, Effects, and Criticality Analysis (SFMECA), 129
Software Firmware Safety Program Plan (SWSPP), 152
Software Hazard Analysis Tracking reports, 149
Software Hazard Criticality Index (SHCI), 131, 132, 149, 150
Software Hazard Criticality Matrix, 146
Software Hazard Risk Index (SHRI), 139, 151
Software Integrated Process Team, 114
Software maturity, 225
Software metrics, 117
Software organization, 61
Software performance requirements, 218
Software process capability, 105
Software Process Improvement Plan, 105
Software Quality, 61, 64, 65, 67, 111, 114, 168
Software Quality Assurance (SQA), 58, 64, 66, 111, 133, 199
Software Quality Assurance Plan, 199
Software Quality indicators, 65
Software Requirements Specification (SRS), 131, 132, 139, 168
Software Reuse Library, 219
Software Safety Critical Functional Analysis (SSCFA), 132, 146
Software Safety criticality, 143, 144
Software Safety Program Plan, 152
Software size, 60, 61

Software Specification (Requirements) Review (SSR), 131, 133
Software Subsystem Hazard Analysis (SSHA), 132, 148
Software supportability requirements, 116
Software test beds and software simulators, 155
Software Test Description (STD), 129, 150, 152
Software Test Plan (STP), 129, 150
Software Test Report (STR), 129, 150, 227
Software Transition Plan (STRP), 124
Software trouble report database, 132
Software Trouble Reports, 58
Software validation criteria, 16, 17, 28
Software/Subsystem Hazard Analysis (SSHA) areas to consider, 148
Source code, 16, 26, 27, 40, 113, 117, 150, 151
Source selection, 3, 21, 33, 105, 117
Source Selection Demonstration, 181, 182
Spare computer system, 116
SSR, 60
Standard CMMI Appraisal Methodology for Process Improvement. See SCAMPI
Standard Safety Oriented Artifacts/Data, 144
Standard Secure Configuration, 71
Standards, practices, and guidelines, 111
Standards-based interfaces, 158, 161
Statement Coverage, 150
Status monitoring, 111
Structural Coverage Analysis/Testing, 150
Structural testing, 151
Subcontractor, 4, 6, 7, 8, 11, 15, 18, 19, 20, 22, 24, 25, 29, 30, 31, 34, 37, 38, 45, 48, 50, 51, 52, 53, 54, 64, 67, 88, 89, 114, 115, 117, 122, 125, 170, 181, 182
Subcontractor Quality Assurance Audits, 67
Sufficient information to prove computer software assertions, 9, 22, 34, 45
Support environment, 117, 124, 173
Support planning, 116
Supportability, 116, 117, 157, 158, 161, 162, 163, 166
Supportability issues, 117, 163
Supportable architecture, 117
Synchronization, 177
System change scenarios, 178
System development plan, 60
System interfaces, 200
System performance specification, 3, 223, 224
System Performance Specification, 223
System RAM requirements, 60
System Safety Analysis Handbook, 138, 147
System Safety Program Plan (SSPP), 152
System specification, 176, 178, 182, 188, 226
System/Software Safety Plan, 143, 144
System/Subsystem Design Description (SSDD), 131
Systems Engineering Plan (SEP), 4, 123, 172, 226

**T**

Technical approach, 3, 109, 122, 123, 162, 226
Technical baseline, 122, 123
Technical data, 6, 7, 8, 9, 11, 12, 14, 15, 19, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 42, 43, 50, 51, 53, 54
Technical Data Or Computer Software Previously Delivered To The Government, 43
Technical definitions of computer software architecture and data metamodel, 154
Technical interchange meetings, 190
Technical solution, 4, 219, 223, 226
Technology insertion, 99, 157, 158, 160, 161, 200, 201
Technology Readiness Assessment, 135, 136, 225
Technology Readiness Level (TRL), 225
Technology refresh, 97, 160, 162, 164, 196, 202
Technology Transition Plan (TTP), 225
Test and Evaluation Plan (TEP), 99, 172
Test procedures, 191, 199
Test Readiness Review (TRR), 134

Test Readiness Review (TRR) agenda items, 134
Third party copyrighted software or documentation, 21, 32, 41
Third-party development, 44, 126
Throughput timing, 154, 193
Traceability, 67, 146, 149, 162, 218, 224
Trade study, 226
Trade study evaluation criteria, 226
Trained workforce, 122
Treatment of proprietary elements, 165
Trustworthy software, 75

**U**

Unified Modeling Language (UML), 87
Uniform Contract Format [FAR], 2
Upgradeability, 157, 165

**V**

Verification, 221
Vulnerability test report, 74

**W**

Work Breakdown Structure (WBS), 60, 61

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| | | |
|---|---|---|
| 1. AGENCY USE ONLY<br>(Leave Blank) | 2. REPORT DATE<br>May 2009 | 3. REPORT TYPE AND DATES COVERED<br>Final |
| 4. TITLE AND SUBTITLE<br>Incorporating Software Requirements into the System RFP: Survey of RFP Language for Software by Topic, v. 2.0 | | 5. FUNDING NUMBERS<br>FA8721-05-C-0003 |
| 6. AUTHOR(S)<br>Charlene Gross | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>Software Engineering Institute<br>Carnegie Mellon University<br>Pittsburgh, PA 15213 | | 8. PERFORMING ORGANIZATION REPORT NUMBER<br>CMU/SEI-2009-SR-008 |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)<br>HQ ESC/XPK<br>5 Eglin Street<br>Hanscom AFB, MA 01731-2116 | | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER |
| 11. SUPPLEMENTARY NOTES | | |
| 12A DISTRIBUTION/AVAILABILITY STATEMENT<br>Unclassified/Unlimited, DTIC, NTIS | | 12B DISTRIBUTION CODE |

13. ABSTRACT (MAXIMUM 200 WORDS)

Organizations developing a Request for Proposal (RFP) often look to existing sources for ideas on how to phrase language for a specific topic -- a time-consuming exercise that usually involves searching across multiple publications.

With this report, the Software Engineering Institute has compiled publicly available recommendations for RFP content, and examples of language for federal RFP Sections C, M, and L. The paper, one element of the implementation plan for the Army Strategic Software Improvement Program, defines and communicates software engineering and management events and deliverables necessary to support the successful acquisition of software intensive systems.

| | | | |
|---|---|---|---|
| 14. SUBJECT TERMS<br>acquisition, RFP, FAR, DFARS | | | 15. NUMBER OF PAGES<br>246 |
| 16. PRICE CODE | | | |
| 17. SECURITY CLASSIFICATION OF REPORT<br>Unclassified | 18. SECURITY CLASSIFICATION OF THIS PAGE<br>Unclassified | 19. SECURITY CLASSIFICATION OF ABSTRACT<br>Unclassified | 20. LIMITATION OF ABSTRACT<br>UL |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102