



ACQUISITION, TECHNOLOGY AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE

3010 Defense Pentagon
Washington, D.C. 20301-3010

MEMORANDUM FOR MEMBERS OF THE ACQUISITION WORKFORCE

SUBJECT: Employment of Open Systems Architecture Contract
Guidebook for Program Managers, Version 1.1

Reference: (a) Open Systems Architecture Contract Guidebook for
Program Managers, Version 1.1, May 2013

The Department of Defense Open Systems Architecture (OSA) Contract Guidebook for Program Managers, Version 1.1 is to be used by the acquisition community for incorporating OSA principles and practices into the acquisition of systems or services. The Guidebook contains background information on OSA and provides contract language to capture the benefits of an open architecture and an open business model to increase opportunities for competition and improve access to innovation.

This contract language is designed to assist acquisition professionals in addressing the technical and business aspects of OSA in solicitations to industry. The language represents a long-term view and incorporates many of the principles of open systems pursuant to the Department of Defense (DoD) Better Buying Power initiative. This document supplements the Federal Acquisition Regulation, the Defense Federal Acquisition Regulation Supplement, and other applicable DoD policy and guidance.

Thoughtful use of this resource is an important element of the acquisition process. The goal is to reduce cost while balancing risk for DoD acquisitions by ensuring OSA and needed data rights are addressed early and given appropriate consideration in the acquisition strategy and process.

The Guidebook is accessible at the following websites:
<https://acc.dau.mil/oa> and <https://acc.dau.mil/osaguidebook>.

All acquisition professionals are directed to become familiar with the referenced Guidebook and implement its principles and practices. This includes enforcing OSA wherever applicable and effectively managing data rights over the entire life cycle of the product.

A handwritten signature in black ink, appearing to read "Frank Kendall", is written over a white background.

Frank Kendall

GREATER VALUE, INNOVATIVE SOLUTIONS FOR THE WARFIGHTER



DoD OPEN SYSTEMS ARCHITECTURE

JUNE, 2013

Contract Guidebook for Program Managers

v.1.1

Prepared by the Department of Defense Open Systems Architecture Data Rights Team
Distribution Statement A: Approved for Public Release; distribution is unlimited

GREATER VALUE, INNOVATIVE SOLUTIONS FOR THE WARFIGHTER

DoD OPEN SYSTEMS ARCHITECTURE

June 2013

Contract Guidebook for Program Managers v.1.1.

Table of Contents

<i>Section</i>	<i>Page</i>
EXECUTIVE SUMMARY	iii
INTRODUCTION	v
Chapter I: RECOMMENDATIONS FOR SECTION C DESCRIPTION/SPECIFICATIONS STATEMENT OF WORK OR STATEMENT OF OBJECTIVES	1
Chapter II: DEVELOPING CONTRACT LINE ITEM NUMBERS (CLINs) – RESERVED	19
Chapter III: EXAMPLES OF SECTION H SPECIAL CONTRACT REQUIREMENTS	21
Chapter IV: RECOMMENDATIONS FOR SECTION L INSTRUCTIONS CONDITIONS, AND NOTICES TO OFFERORS OR RESPONDENTS	42
Chapter V: RECOMMENDATIONS FOR SECTION M EVALUATION FACTORS FOR AWARD	69
Chapter VI: RECOMMENDATIONS FOR INCENTIVIZING CONTRACTORS	77
Appendix 1: RECOMMENDED CDRL AND DELIVERABLE ITEMS	83
Appendix 2: OSA CHECKLIST (short)	97
Appendix 3: OSA CHECKLIST (long)	101
Appendix 4: RECOMMENDED DATA LANGUAGE FOR CODE HEADERS	107
Appendix 5: OPEN SOURCE SOFTWARE	113
Appendix 6: GLOSSARY OF TERMS	129
Appendix 7: ASSESSING A PROGRAM’S INTELLECTUAL PROPERTY RIGHTS NEEDS AND DEVELOPING A TECHNICAL DATA RIGHTS STRATEGY (TDRS)	147
Appendix 8: CLICKWRAP OR EMBEDDED LICENSE ISSUES ..	157
Appendix 9: BETTER BUYING POWER: UNDERSTANDING AND LEVERAGING DATA RIGHTS IN DOD ACQUISITIONS	161
Appendix 10: BREAKING AND AVOIDING VENDOR LOCK	167
Appendix 11: SAMPLE CONTRACT DATA REQUIREMENTS LISTS (CDRLs)	177

EXECUTIVE SUMMARY

This Open Systems Architecture Contract Guidebook provides contract language targeted at the needs of the Program Manager. This document contains the basic elements to capture the benefits of an open architecture and an open business model. The essence of Open Systems Architecture (OSA) is organized decomposition, using carefully defined execution boundaries, layered onto a framework of software and hardware shared services and a vibrant business model that facilitates competition. OSA is composed of five fundamental principles:

1. Modular designs based on standards, with loose coupling and high cohesion, that allow for independent acquisition of system components;
2. Enterprise investment strategies, based on collaboration and trust, that maximize reuse of proven hardware system designs and ensure we spend the least to get the best;
3. Transformation of the life cycle sustainment strategies for software intensive systems through proven technology insertion and software product upgrade techniques;
4. Dramatically lower development risk through transparency of system designs, continuous design disclosure, and Government, academia, and industry peer reviews;
5. Strategic use of data rights to ensure a level competitive playing field and access to alternative solutions and sources, across the life cycle.

A mandate of OSA is that technical requirements be based to the maximum extent practicable on open standards. Where there are no standards, the OSA methodology creates them. At a minimum, technical standards and related specifications, requirements, source code, metadata, interface control documents (ICDs), and any other implementation and design artifacts that are necessary for a qualified contractor to successfully perform development or maintenance work for the Government are made available throughout the life cycle.

INTRODUCTION

Purpose: *The Department of Defense (DoD) Open System Architecture Contract Guidebook for Program Managers (Guidebook)* is to be used by Program Managers (PMs) who are incorporating Open System Architecture (OSA) principles into the acquisition of any system or service, including those not considered to be “information intensive.” This guidance may be especially well suited for acquisition programs for national security systems (NSS), or for any system that seeks to integrate technologies originating from Government or noncommercial sources with those available under commercial or proprietary development and licensing models.

This Guidebook contains recommendations¹ and is offered with the understanding that individual Program Executive Offices (PEOs) and programs must have the flexibility to adapt its principles and guidance to meet their needs. This document is intended to implement and supplement, rather than replace, authoritative source materials such as the Federal Acquisition Regulations (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS), and other applicable DoD policy and guidance. Users must continue to consult and comply with the most recent versions of the FAR and DFARS, and other governing DoD policy and guidance, in addition to this *Guidebook*, when developing acquisition materials.

There are a variety of tools, devices and resources available to the PM when planning for and conducting the acquisition of a system using OSA guidelines such as those contained in this *Guidebook*. The proper use of these resources is an important element of the acquisition process and will reduce the overall risk to the Department of Defense by ensuring that all necessary OSA aspects of the procurement are covered. In addition to the contract, Request for Proposal (RFP), and Statement of Work (SOW) elements that are discussed in this *Guidebook*, the System Specification and other system architecture and design materials are important. Because the System Specification defines the attributes of the overall system to be developed, this

¹ This document may contain references to non-Government sources, information, products, or services that are provided solely for informational purposes or as representative examples. However, nothing in this guidebook is intended as, nor should be interpreted as, an endorsement of any such non-federal entity, or its products or services by the Department of the Defense or the U.S. Government.

document must describe how the technical system characteristics will contribute to overall system openness (such as its modularity and how open standards² will be incorporated). The System Specification should also address those areas where future growth is expected, where reuse is envisioned, etc. Proper balance and coordination among the contract, RFP, SOW, System Specification and related architecture and design documents is important to both the technical design and the overall life cycle support of the system. Additional information on these topics is included in the appendices of this *Guidebook*.

Organization: This document is divided into five chapters containing suggested language for RFP Sections C, H, L and M, and Award Fee Plans. This material can be tailored for use in the specific phase of an acquisition program. It can also be tailored for use in contract modifications. In addition, there is a short placeholder chapter on developing Contract Line Item Numbers (CLINs). Additional content will be provided in subsequent versions of this document. Appendix 1 contains suggested OSA-related Data Item Descriptions (DIDs) for use in preparing the Contract Data Requirements List (CDRL) and for identifying other contractual deliverables. Appendices 2 and 3 are checklists to assist the Program Manager to better understand the business and technical aspects of OSA. Appendices 2 and 3 also provide a detailed checklist describing the FAR and DFARS clauses required or recommended to be included in the contract. Appendices 4 and 5 address data markings and Open Source Software (OSS). Appendix 6 contains a Glossary of Terms. Appendix 7 includes guidelines for conducting an analysis of a program's intellectual property rights (IPR) requirements, Appendix 8 discusses contractor licensing of deliverables, Appendix 9 provides a guide to understanding and leveraging data rights in DoD acquisitions. Appendix 10 contains a summary of steps that PMs can take to avoid or break vendor lock.³ Finally, Appendix 11 contains sample Contract Data Delivery Lines

² "Open Standards" means widely accepted and supported standards set by recognized standards organizations or the marketplace. These standards support interoperability, portability, and scalability and are equally available to the general public at no cost or with a moderate license fee. [*Glossary of Defense Acquisition Acronyms & Terms, 13th Edition, Nov. 2009*]

³ Vendor lock, or vendor lock-in, is the situation in which customers are dependent on a single manufacturer or supplier. [See glossary.]

[http://www.linco.org/vendor_lockin.html referenced in http://cio-nii.defense.gov/sites/oss/Open_Source_Software_%28OSS%29_FAQ.htm]

that can be used in conjunction with Appendix 1 and the remainder of this *Guidebook*.

Providing Comments and Feedback: Development and maintenance of this *Guidebook* are interactive processes involving the “build-test-build” method on a roughly biennial release schedule. These releases will incorporate community inputs and address topics that emerge from the DoD Enterprise’s experience from implementing OSA. Therefore, the authors are very interested in comments, suggestions, and feedback. We are also very interested in any “real world” experiences you may have in using OSA principles in programs. Comments can be submitted via email, with “Comments on DoD OSA Contract Guidebook” in the subject line, to OSAGuidebook@dau.mil. A community collaboration site has also been established at <https://community.forge.mil/group/osa-guidebook> to exchange solutions to common problems, blog on ideas, create discussions and find other peer acquisition practitioners working on similar projects.

Background: An open architecture is a technical architecture that adopts open standards supporting a modular, loosely coupled and highly cohesive system structure that includes publishing of key interfaces within the system and full design disclosure. A key enabler for open architecture is the adoption of an open business model, which requires doing business transparently to leverage the collaborative innovation of numerous participants across the enterprise permitting shared risk, maximize asset reuse and reduce total ownership costs. The combination of open architecture and an open business model permits the acquisition of Open Systems Architectures that yield modular, interoperable systems allowing components to be added, modified, replaced, removed and/or supported by different vendors throughout the life cycle in order to drive opportunities for enhanced competition and innovation.⁴

The U.S. Government’s (“Government”) ability to obtain suitable technical data and computer software deliverables, along with rights sufficient for competitive use of that data and software is often critical to this effort. The laws applicable to DoD provide a spectrum of possible data rights licenses allowing more or less competitive use with concomitantly less or more administrative burden to the Government in

⁴ This definition is from the Department of Defense’s Better Buying Power (BPP) website – a restricted access website located at: <https://acc.dau.mil/bbp>. External parties currently have to apply for access to the Government-only BPP site through this link.

the handling and protection of the technical data or software. For example, the standard DFARS Government Purpose Rights (GPR) may often provide an optimal level of rights, allowing competitive use by the Government for Government purposes, while affording a level of exclusive rights for the vendor to non-Government commercial sales. In addition, the DFARS authorizes specially negotiated license rights whenever the parties mutually agree that such a specially tailored agreement is a better balance of the parties interests than the standard or pre-defined data rights licenses, or the otherwise applicable commercial licenses.

Data and design artifacts related to the interfaces between modules are particularly important. One way of measuring the “openness” of a system is how readily a system component can be replaced with one developed by a different vendor with no loss in overall system effectiveness.

OSA is composed of five fundamental principles:

1. Modular designs based on standards, with loose coupling and high cohesion, that allow for independent acquisition of system components;
2. Enterprise investment strategies, based on collaboration and trust, that maximize reuse of proven system designs and ensure we spend the least to get the best;
3. Aggressively transform our life-cycle sustainment strategies for software intensive systems through proven technology insertion and product upgrade techniques;
4. Dramatically lower development risk through transparency of system designs, continuous design disclosure, and Government, academia, and industry peer reviews;
5. Strategic use of data rights to ensure a level competitive playing field and access to alternative solutions and sources, across the life cycle.

Achievement of these five principles requires an affirmative answer to a fundamental question:

Can one or more qualified third parties add, modify, replace, remove, or provide support for a component of a system, based on open standards and published interfaces for the component of that system?

In order to successfully permit competitive opportunities for a third party to add, modify, replace, remove or provide support as noted in the

question above, the following business and technical elements must be integrated as foundational elements within a program:

Business Practices of OSA	Technical Practices of OSA
<ul style="list-style-type: none"> Seek data deliverables and rights in technical data and computer software sufficient for competition throughout the life cycle as an objective; 	<ul style="list-style-type: none"> Modular architectures with open standards and published interfaces;
<ul style="list-style-type: none"> Continuous competition throughout the life cycle; 	<ul style="list-style-type: none"> Separation of hardware and software through middleware⁵;
<ul style="list-style-type: none"> Increased capability to the warfighter on a faster development timeline; 	<ul style="list-style-type: none"> Maximized reuse of assets to limit unique development;
<ul style="list-style-type: none"> Reduced life cycle costs; 	<ul style="list-style-type: none"> Full Design disclosure⁶; and,
<ul style="list-style-type: none"> Shared risks with other programs; 	<ul style="list-style-type: none"> Limited use of well-defined proprietary solutions.
<ul style="list-style-type: none"> Minimized duplication for technology development investments, shared life cycle costs; and 	
<ul style="list-style-type: none"> Collaboration through peer reviews. 	

Several years ago, the Navy and Marine Corps adopted Naval Open Architecture (NOA) as a way to reduce the rising cost of Naval warfare systems and platforms while continuing to increase capability delivery on shortened demand timelines. NOA was defined as the confluence of business and technical practices yielding modular, interoperable systems that adhere to open standards with published interfaces.⁷ As such, NOA is the Naval implementation of the Office of the Secretary of Defense’s Open Systems Joint Task Force’s (OSJTF) Modular Open System Approach (MOSA) that was first introduced in 2004. NOA provided the foundation for and is aligned with OSA.

The Undersecretary of Defense (Acquisition, Technology and Logistics) (USD(AT&L))’s *Better Buying Power* initiatives provide specific guidance related to delivering better value to the taxpayer and warfighter by improving the way the Department does business. One of

⁵ Middleware” is software that connects two otherwise separate applications. See Appendix 6 for a more detailed explanation and examples of middleware.

⁶ Full design disclosure describes a continuum of data and software deliverables ranging from Form, Fit and Function data to detailed manufacturing and process data or source code.

⁷ OA and OSA refer to the same approach, i.e., OA & OSA are interchangeable terms.

the main themes is promotion of effective competition across the entire DoD Enterprise. A critical element for enabling competition is the use of acquisition and contracting language that:

- Addresses the business and technical principles,
- Comprises and leads to an OSA,
- Minimizes vendor locked situations, and
- Maximizes acquisition choices and flexibility.

OSA facilitates greater collaboration within and across different Military Departments (Army, Navy, Air Force), and Defense Agencies, Acquisition Domains and warfare communities through the use of an open business model.

Individual Departments, Acquisition Domains and PEOs may opt to pursue common architectures or capabilities across platforms; the OSA principles highlighted in these materials would apply to these common architectures. The Office of the Secretary of Defense's Unmanned Aircraft Systems Control Segment Working group case below exemplifies how these OSA principles were leveraged to improve acquisition outcomes.⁸

OSA also allows for incorporating more commercial or

Case Study: Office of the Secretary for Defense, Unmanned Aircraft Systems Control Segment Working Group

The UCS-WG changed DoD's traditional approach to acquisition and used open business and technical principles to develop a Service Oriented Architecture (SOA) Based Architecture for a common ground control station (GCS) across the Services. The UCS WG funded a limited number of development pilots to demonstrate the UCS architecture and illustrate the potential for Joint development and integration of GCS capabilities by various companies proving to be a major breakthrough in improving acquisition flexibility and breaking out of vendor lock. The set of Initial Work Packages (IWP) demonstrated how the U.S. Air Force Weather service capability could be integrated into other Service's GCS, thus permitting acquisition flexibility and breaking vendor lock. This innovation resulted in:

- *75% reduction in development and integration costs*
 - *Integration time of one - three weeks*
- The typical cost for creating a GCS-specific weather service is in excess of \$2M, thus making the case for only one service development effort for use across multiple GCSes.*

⁸ Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD AT&L) *Unmanned Aircraft Systems (UAS) Ground Control Station (GCS) Acquisition Decision Memorandum (ADM)*, dated February 11, 2009.

commercial-off-the-shelf (COTS) technology in warfare systems and enabling reuse of software and related assets. More importantly, OSA increases competition among system developers through the use of open standards and standard, published interfaces. OSA principles are also supportive of and consistent with using Open Source Software (OSS) in systems. It is important to understand that use of OSS does not, by itself, constitute compliance with OSA.

On October 16, 2009, the Assistant Secretary of Defense (Networks & Information Integration) / DoD Chief Information Officer (CIO) issued a memorandum clarifying guidance on Open Source Software (OSS). The memo stated that in “almost all cases, OSS meets the definition of ‘commercial computer software’ ” and, therefore, should be given similar consideration to a more traditional commercial computer software when a program is looking to acquire such software.⁹ This will allow the Department of Defense (DoD) to utilize OSS throughout the enterprise when acquiring capabilities to meet DoD business and warfighter requirements. As with any COTS solution, the use of OSS must adhere to all Federal, DoD, and Service laws and policies and should be based on open standards to support the DoD’s goals of net-centricity and interoperability. In addition, all DoD organizations must work with their intellectual property Legal Counsel to ensure compliance with OSS license agreements.

This contract language guidance is designed to assist PEOs, Program Managers, legal, and contracting officials in addressing the technical and business aspects of OSA in the solicitation and award of DoD and Service contracts. The language represents a long-term view and incorporates many of the principles of open systems pursuant to the DoD’s Better Buying Power initiative.

Discussion: This *Guidebook* contains recommended language for Section C and associated Contract Data Requirements Lists (CDRLs) of contracts and Sections L and M of solicitations issued by DoD and Service organizations. These approaches have been used successfully for acquisitions of NSS or larger “systems of systems” that integrate NSS with platforms such as aircraft, submarines, land vehicles, satellites or ships. There are also recommendations for language that can be incorporated in Section H of solicitations, including solicitations for existing programs.

⁹ ASD(NII)/DoD CIO memorandum, *Clarifying Guidance Regarding Open Source Software (OSS)*, October 16, 2009.

Sections L and M are pre-award documents not incorporated into the awarded contract, but are the keys to ensuring contractor understanding of and compliance with OSA principles. Execution of an effective OSA strategy including strategic asset reuse must be considered from both a Pre-Award and Post-Award perspective. The language contained in this document should be tailored to reflect the program's phase and the goals of the intended procurement action.

Program Managers are advised to use this recommended language and other appropriate technical documents after determining the specific acquisition relevance to the requirement. Prior to tailoring this language to the specific needs of the acquisition program, Program Managers should have a clear understanding of OSA principles. Acquisition Programs should have a strategy and supporting plan that addresses an appropriate business and technical OSA end state and acts as a framework for structuring contract language that is consistent with DoD guidance for interoperability, such as that included in PEO C4I's Net-Centric Enterprise Solutions for Interoperability (NESI) V3.1.0 (available at <http://nesipublic.spawar.navy.mil/>). The Open Architecture Assessment Tool (OAAT)¹⁰, developed by the Naval Open Architecture Enterprise Team, can also be used to formulate an OSA strategy. Additionally, the Naval Air Systems Command (NAVAIR) Key Open Sub Systems (KOSS) tool can be used to identify the components of a modular architecture that are the most dynamic and, therefore, should receive extra OSA emphasis.¹¹ The Army developed the Army Guide for the Preparation of a Technical Data Rights Strategy (TDRS) (<https://www.dodtechipedia.mil/dodc/x/H4Bt>) that will help programs address the challenges associated with assessing and addressing intellectual property rights issues. Appendices 2 and 3 consist of two checklists that will assist in preparing quality acquisition materials. The goal of maximizing program flexibility to enable competition and programmatic course changes must be balanced against providing the contractor enough incentive to agree to the contract. Short duration tasks and small deliverable quantities provide the Program Manager with the flexibility to shift to other providers to obtain better performance, introduce different products and technologies, or when

¹⁰ The OAAT can be found in the "Tools" section of the Naval OA website at <https://acc.dau.mil/oa>.

¹¹ The KOSS tool can be found in the "Tools" section of the Naval OA website at <https://acc.dau.mil/oa>.

otherwise deemed in the best interest of the Government. Such mechanisms are not a substitute for effective project and contract management practices by the program, but can provide additional leverage to support these practices.

Intellectual Property Rights (IPR) and Data Rights: Section 2320(e) of title 10, United States Code (U.S.C.), as implemented in DODI 5000.02 and DFARS 207.106 (S-70), requires ACAT I and II Program Managers to assess the IPR and data rights requirements of their program, create a Technical Data Management Strategy¹² and take steps to secure the Government's appropriate rights consistent with the FAR and DFARS. Other programs, e.g., ACAT III and IV, are encouraged to follow these steps. Program Managers responsible for ACAT I and II programs are further advised to immediately take steps to incorporate the requirements of DoD Instruction 5000.02 dated December 2, 2008¹³. General guidance for performing an assessment of IPR and Data Rights is contained in Appendix 7 of this document. This analysis will help Program Managers develop Acquisition Strategies that anticipate potential reuse in other programs and thus guide decisions related to IPR and data rights. These decisions include the extent to which:

(1) These deliverables and associated license rights will be procured, and

(2) The offered deliverables and rights will be considered as part of the source selection evaluation.

The approach selected by the Program Manager will drive different solutions in the construct of Sections C, H, L, and M. The attached suggested language for Sections C, H, L, and M provides general guidance on data rights, while specifics must be tailored to individual programs. Appendix 9 provides a summary of recommendations for leveraging data rights in DoD acquisitions.

Program Managers (in coordination with their PEOs and Resource Sponsor) should develop a post-award strategy to ensure they are exercising their IPR as defined by the FAR and DFARS. Historically, the DoD and Military Departments have not effectively and consistently acquired, exercised, or enforced the IPR procured by the

¹² The term "Data Management Strategy" is being replaced by Data Rights Strategy (DRS) with the understanding that the DRS includes the DRS includes both technical data and computer software.

¹³ Which implemented USD(AT&L) memorandum on *Data Management and Technical Data Rights*, July 19, 2007.

Government or identified by contractors in their proposals, in part by not including effective Contract Data Requirements Lists (CDRLs) and Data Item Descriptions (DIDs) in contracts. The Statement of Work (SOW) establishes the product/system development expectations; the CDRL orders the delivery of the data according to the SOW, and the DID describes the format and content of the data ordered by the CDRL as articulated in the FAR and DFARS. It is incumbent upon the Government, in general, and the Program Manager and Contracting Officer's Representative (COR) specifically, to review each deliverable and report unjustified, nonconforming, or other inappropriate markings on delivered data to the Contracting Officer in order to ensure the PEO is able to take full advantage of available procedures to validate the Government's rights.¹⁴ The Contracting Officer, with the assistance of Legal Counsel, is responsible for enforcement of the DFARS provisions.

An overarching concern is reconciling certain statutory¹⁵ restrictions with the proposed evaluation factors for data rights. More specifically, the Government cannot condition award to, or responsiveness of, the Offeror on its relinquishing greater data rights in privately developed technologies than specified in the statute. However, the DFARS clarifies¹⁶ the Government can evaluate data rights as part of its best value determination (see below), and can always request and negotiate pricing for additional rights that the Offeror is willing to provide, or, if necessary, for the development of alternative sources of supply and manufacture. It is recommended that any priced technical data/software (TD/SW) CLIN specifically address exactly what types of technical data/software are associated with what types of rights the Government desires, instead of using a generic CLIN applicable to all TD/SW with less than Government Purpose Rights (GPR)¹⁷. For example, the Program Manager may consider the following related CLINs:

Depot Data Licensing Fee – The Contractor shall provide licensing for all technical data, including computer software documentation, and computer software necessary to perform depot level maintenance for

¹⁴ For example, correction of unjustified or nonconforming markings is addressed at DFARS 252.227-7013(h) and 252.227-7014(h).

¹⁵ 10 U.S.C. Section 2320 (a)(2)(F).

¹⁶ See DFARS 227.7103-10(a)(5) and 227.7203-10(a)(5).

¹⁷ GPR, as a standard rights category that allows the competitive use of the data/software for any Government purpose (including competitive procurement), may serve as a convenient point to distinguish offers of license rights that may further restrict such competitive uses.

the program. The Contractor grants or obtains for the Government license rights for the technical data, including computer software documentation, and computer software in accordance with a specific H clause.¹⁸

Technical Data Engineering Services – Composite labor rates to include the costs of compiling, reproducing and providing the data and software in the format specified by the Government per a specific H clause and CDRLs.

The Government should also identify and define what constitutes complete delivery of the necessary TD/SW.

If appropriate, the Government can also challenge asserted restrictions as unjustified. A review of the mandatory documentation¹⁹ listing the contractor's data rights assertions provides an opportunity to establish a baseline that determines what developments were funded by the Government. Also, under DFARS 227.7103-2(b)(2) "Acquisition of Technical Data" and DFARS 227.7203-2(b)(2) "Acquisition of Noncommercial Computer Software and Computer Software Documentation," the Government can and must balance the original assessment of the Government's data needs with data prices contained in the offer. Furthermore, 10 U.S.C. Section 2305(d)(4)(B) "Contracts: Planning, Solicitation, Evaluation, and Award Procedures" states: "[i]n considering offers in response to a solicitation requiring proposals described in paragraph (1)(B) or (2)(B), the head of an agency shall base any evaluation of items developed exclusively at private expense on an analysis of the total value, in terms of innovative design, life cycle costs, and other pertinent factors, of incorporating such items in the system." Such factors may include the IPR specified in an offer. See Chapter IV for additional information on this.

As part of a best value analysis, the Government may consider an Offeror's willingness to provide the Government with the necessary data deliverables, along with the equivalent of GPR or other license rights that would allow competition. The evaluation criteria must make clear how the Government will be evaluating these elements, such as the effect on costs associated with an Offeror's restrictions on data and

¹⁸ An offer can satisfy the license rights component of this approach either by offering a standard license category (e.g., Unlimited Rights or GPR), or a special license agreements, as long as the license authorizes the depot level maintenance activity for the program (including using competitive procedures).

¹⁹ See DFARS 252.227-7017 for pre-award assertions; which may be updated under certain circumstance post-award, pursuant to DFARS 252.227-7013(e) or -7014(e).

software-related assets that would be delivered under the contract. The Government may assess the impact on evaluated costs for deliveries with license rights that do not support competitive procedures, such as:

- 1) limited rights (LR) technical data,
- 2) restricted rights (RR) software,
- 3) standard proprietary licenses in commercial computer software (CS), or
- 4) technical data for commercial items covered under DFARS 252.227-7015(b)(2).

For example, the Government may examine the impact of LR in data on system life cycle costs. When making cost assessment keep in mind alternatives like use of form, fit, function, etc., as assessment must be “reasonable”. To avoid unstated evaluation criteria or other such problems, the criteria must meet applicable FAR, DFARS, and DoD requirements²⁰ for evaluation factors, such as specifying the relative importance of costs associated with needs set forth in the “Data Rights and Patent Rights” portion of the solicitation, e.g., life cycle costs for system. Finally, the data rights and associated markings of intellectual property – including Distribution Statements and Export Controls – will impact the Government’s ability to deposit intellectual property (IP) in asset repositories/libraries and be able to use these assets in other systems.

For programs that are leveraging the Small Business Innovative Research (SBIR) program, the DoD SBIR data rights clause is at DFARS 252.227-7018, which implements the Small Business Innovation Research Policy Directive.²¹

²⁰ See, e.g., the *Department of Defense Source Selection Procedures*, dated March 02, 2011 (available at <http://www.acq.osd.mil/dpap/policy/policyvault/USA007183-10-DPAP.pdf>), and other materials available from the DAU Source Selection topic page at <https://acc.dau.mil/CommunityBrowser.aspx?id=18888>.

²¹ See <http://www.sbir.gov/about/about-sbir> for more information. The SBA Policy Directive was published in the Federal Register Vol. 67, No. 185, Tuesday, September 24, 2002. More specifically, Section 8 of the Directive provides direction for all federal agencies regarding IP/data rights. As of this publication, the Small Business Administration has published a proposed update of its SBIR Policy Directive. Those concerned with SBIR contracts should monitor developments on the Directive.

Contract Incentives: This guidebook provides information not covered in other guidance documents associated with contract incentives. The incentive structures described in this guide have the added benefit of reinforcing the importance of the Government's emphasis on collaborative business relationships, technical leadership, planning, and execution. Earnings, including capture of contract incentives, are typically briefed to the highest levels within corporate management. These incentives for adoption and adherence of OSA business and technical principles will motivate exceptional contractor performance that might not otherwise be emphasized. Chapter VI of this guidebook provides the structure for incentivizing OSA technical tenets, business practices, and cooperative behavior with other vendors as well as the more usual quality, timeliness, technical progress, technical ingenuity, and cost-effective management requirements.

When performing new product development, as is often the case for creating open systems architecture products, cost contracts with incentive mechanisms are appropriate for new product development:

- Cost Plus Incentive Fee (CPIF) for constant work that is spread out over the duration of the contract (e.g. 3 years), such as sustainment and upgrading of delivered capability;
- Cost Plus Award Fee (CPAF) for engineering development of large scale open systems where the volume of effort varies over the contract period (e.g. 5 years). Award Fee determinations can be effective when applied to measureable development milestones, like achieving entrance criteria for technical reviews or achieving scheduled deliveries against published development time frames; and
- Cost Plus Award Term (CPAT) for integration contracts for bringing together multiple products from an array of third parties over a longer period of time (up to 10 years) and motivation of industry investment is mutually beneficial. CPAT for depot repair contracts is also worthy of consideration. This is another area where long-term relationships can be beneficial, provided that the service continues to be satisfactory and metrics can be used as the basis for awarding additional terms.

The use of Fixed-Price Incentive Firm (FPIF) and Firm Fixed Price contracts in development and production is only appropriate for

activities like early or low rate production as long as the following conditions can be met:²²

- Firm requirements
- Low technical risk
- Qualified suppliers
- Financial capacity to absorb overruns
- Motivation to continue.

Software and Systems Process Improvement (SSPI)

Section 804 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003²³ required DoD component organizations, including the military departments, to undertake certain software and systems process improvement (SSPI) actions. Accordingly, this Guidebook contains additional guidance for acquisition managers which is intended to provide improved visibility into the software development processes used by Offerors and contractors. This guidance is aimed at helping to ensure there are well-documented, effective software processes and continuous process improvement practices in place during contract performance.

Army: The Army Strategic Software Improvement Program was established in August 2002; guidance is provided by the Army Strategic Software Improvement Program (ASSIP) Senior Steering Group, which includes the Assistant Secretary of the Army for Acquisition, Logistics, and Technology Military Deputy and Program Executive Offices (PEOs). Information on the Army's Software Engineering Center can be found at http://www.sec.army.mil/secweb/external_links.php.

Air Force: The Air Force Software-Intensive Systems Strategic Improvement Program was established in January 2004, the program is overseen by a working group that consists of Air Force software experts and engineers. Information on the Air Force's Software Technology Support Center (STSC) can be found at <http://www.stsc.hill.af.mil/about/index.html>.

²²*Use of Fixed-Price Incentive Firm (FPIF) Contracts in Development and Production*, Kendall, Defense AT&L magazine, March-April 2013

²³ Public Law 107-314, December 02, 2002. Note that section 804 is published at 10 U.S.C. § 2302 note.

Navy: The Navy established its Software Process Improvement Initiative (SPII) Program in May 2006. The program is led by a steering group, which is headed by the Assistant Secretary of the Navy for Research, Development and Acquisition Chief Engineer and composed of senior engineers. Navy SPII Policy and accompanying documents are available on Naval Open Architecture website at <https://acc.dau.mil/CommunityBrowser.aspx?id=180966&lang=en-US>.

[General Notes to Preparers:

The main thrust for DoD and Service systems engineering and Program Manager communities should be on the development of appropriate SOW requirements, Data Item Descriptions (DIDs), and CDRLs across the enterprise.

Although the Guidebook was developed for mixed systems consisting of hardware, middleware and software elements, the recommended language can be easily tailored to reflect hardware- or software-only acquisitions.

Program Managers should include testing materials (software, tools, instructions, testing results, design artifacts, etc.) in the contract DIDs and CDRLs as required to support the system life cycle but especially for those items developed with Government funding. The Government should ensure that it has appropriate rights and that these items are marked correctly by the contractor.

Establish separate Contract Line Item Numbers (CLINs) for technical data and computer software to be delivered under a contract as required by DFARS 227.7103-1(b)(3) and 227.7203-1(b)(3). Solicitations and contracts should also include priced contract option CLINs for future delivery of technical data and computer software that were not acquired upon initial contract award. Although the Deferred Ordering clause at DFARS 252.227-7027 should be included in contracts, the Government should not overestimate the scope of that clause, e.g., it does not cover technical data or computer software that were not generated under the contract²⁴. Priced contract option CLINs should also be included for technical data rights licenses or computer software licenses when the Government desires additional rights in technical data/computer software. Consult with the contracting officer and cognizant attorney for preparation of CLINs and option CLINs.

Program Managers should be careful to prevent unintended contractual restrictions on the ability to use software and other components on updated hardware. There have been occasions when software licenses preclude or restrict the removal of software packages

²⁴ Note that Section 815 of the NDAA for Fiscal Year 2012 (Pub. L. 112-81) added new paragraph (b)(9) to 10 U.S.C. § 2320, which creates a new deferred ordering scheme that will be implemented in the DFARS (see pending DFARS case 2012-D022).

from a specific hardware installation with subsequent reinstallation on another platform.

The Government team needs to conduct a markings review of OSA-compliant deliverables prior to Government acceptance. This enforcement must be done during execution of the contract by rejection of inappropriately marked deliverables (as defined in CDRs/DIDs). Program Manager review of markings on deliverables is critical to ensure the Government obtains and can readily exercise data rights for which it has contracted. It also should be noted that even if the Government initially accepts an erroneously marked deliverable, the Government still has the right to challenge these markings in accordance with DFARS 252.227-7019, DFARS 252.227-7013(h), DFARS 252.227-7014(h), DFARS 252.227-7018(h).

Offerors should be contractually required to propose and maintain an Open System Management Plan, which is required to describe—but is not limited to—the Offeror's approach to modular, open design; inter-component dependencies; design information documentation; technology insertion; life cycle-sustainability; interface design and management; treatment of proprietary or vendor-unique components; reuse of pre-existing or common items; and treatment of proprietary elements. Any changes, modifications, or alterations to this plan should be incorporated into the contract as appropriate.

Implementing OSA principles includes specifying a finite duration for the contracting vehicle and/or a finite number of deliverable units. Short duration taskings and small deliverable quantities provide the Program Manager with the flexibility to shift to other providers when deemed in the best interest of the Government or to obtain better performance or a better product from a different vendor competitively selected or programmatically assigned. However, these considerations must be balanced against economies of scale and possible volume discounts. Such mechanisms are not a substitute for effective project and contract management practices by the program, but can provide additional leverage to support these practices.

It is incumbent upon the Program Manager and Contracting Officer to fully understand the terms of each data rights license, including the specific rights and limitations, if any, proposed by the Offeror. License agreements should be in the Contract.

Program Managers should consider including a requirement to have real-time access into the Offeror's (or an associated sub-contractor's) software and hardware development environment, providing the Government with continuous online access to work products under development commencing at the start of work. Collaborative tools to support this access must be adopted, tailored, and applied by the Program Manager in a manner consistent with its specific requirements and circumstances. Note: While the Government will have access to these work products and may be able to download them, the Contractor and the Government may not consider all of the accessible materials to be contract deliverables in the traditional sense (e.g., subject to formal DFARS marking requirements), and thus the contract must address the parties' agreed-upon use and release restrictions, and restrictive notice or marking procedures, on such information²⁵.

To help clearly understand the data rights to be provided to the Government, the Government should ensure that the list of asserted data rights restrictions²⁶ a table listing all the CDRLs should be inserted as an attachment to the proposal which includes a column wherein the Offeror states the data rights to be provided upon delivery.

The program plan and directive documentation shall specify that anything the Government paid to develop is available for delivery to the Government with all of the developmental artifacts and requisite usage rights. To ensure a level competitive playing field, the program shall require that the deliverables be provided to (or deposited in) the appropriate repository. Programs must ensure that potential Offerors who do not have access to reuse repositories/libraries because they lack a current contractual vehicle are informed of the contents of the repositories and allowed to access and download artifacts as appropriate. Please see Appendix 9: Better Buying Power: Understanding and Leveraging Data Rights in DoD Acquisition for further information.

When citing regulations such as the DFARS and FAR, current clause effective dates are included where possible to reflect the most recent

²⁵ See, e.g., Chapter I, section 2.c.

²⁶ Required by DFARS 252.227-7017 for noncommercial technologies, and the solicitation should also include a similar assertion list for commercial technologies, such as recommended at Chapter III, Section 3, *infra*.

version of this Guidebook. However, Contracting Officers and PMs need to check for current clause dates before using the language in this Guidebook.

Definitions of some terms used in this Guidebook are provided as a reference in Appendix 6: Glossary of Terms. However, to avoid any uncertainty or ambiguity in contracts, these definitions should be included in the solicitations, and resulting contracts.]

[Technical Notes to Preparers:

PEOs and Program Managers are invited to adapt and supplement the language in this Guidebook with technical requirements appropriate for the component or system being acquired. A goal of OSA is that these technical requirements be based, to the extent practicable, on open standards. At a minimum, technical standards and related specifications, requirements, source code, metadata, interface control documents (ICDs), and any other implementation or design artifacts that are necessary for any qualified contractor to successfully perform combat system work for the Government will be made available to potential vendors.

Use of the recommended solicitation language in this Guidebook does not require programs adopt specific technical language; however, this language does require contractors to explain their use of proprietary or vendor-unique solutions and to emphasize any such use preferably at the lowest component or subsystem level.

Not all developments or programs will need to address or emphasize enterprise level interoperability. Program Managers – working with their PEO, Resource Sponsors, and other stakeholders – must evaluate their need and ability to interface across the enterprise using the appropriate guidance documents.

The requirements of Section C of the solicitation should use the language to require that the contractor deliver to the Government the software in a standalone fashion, i.e., not encumbered by any particular configuration management tool. Future sites/locations/programs that ultimately will use the software or artifacts should have the ability to use whatever configuration management tool they desire without any overt or hidden dependencies on a given tool.]

Chapter I: RECOMMENDATIONS FOR SECTION C DESCRIPTION/SPECIFICATIONS STATEMENT OF WORK OR STATEMENT OF OBJECTIVES

Section C of the Request for Proposal (RFP) and the resulting contract contains the detailed description of the products to be delivered or the work to be performed under the contract. Section C includes a Statement of Objectives (SOO) or a Statement of Work (SOW).

The SOO is a government-prepared document incorporated into the solicitation that states the overall performance objectives. It is used in solicitation when the Government intends to provide the maximum flexibility to each Offeror to propose an innovative approach (FAR 2.101). It is a clear and concise statement that delineates the program objectives and the overall program approach, including the outcome desired.

A SOW, specifications, or other description, is a government-prepared document that reasonably describes the general scope, nature, complexity, and purpose of the supplies or services the Government will acquire under the contract in a manner that will enable a prospective Offeror to decide whether to submit an offer (FAR 16). An additional helpful reference is the *Department of Defense Handbook for Preparation of Statement of Work (SOW)*.²⁷

Although the *Guidebook* was developed for mixed systems comprised of hardware, middleware and software elements, the recommended language can be easily tailored to reflect hardware- or software-only acquisitions.

The following contains recommended language for inclusion in Section C of the RFP/contract:

1. Open Systems Approach and Goals

The Government intends to procure system(s) having an Open System Architecture and corresponding components. As part of this contract, the contractor shall 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 shall demonstrate compliance with that plan

²⁷ The DoD Handbook for Preparation of Statement of Work (SOW) is available on the web at:
https://www.acquisition.gov/comp/seven_steps/library/DODhandbook.pdf.

during all design reviews. As part of an Open System Management Plan, the contractor shall identify in a listing contained in its proposal to the Government all Commercial-Off-the-Shelf/Non-development Item (COTS/NDI) components²⁸, 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 digital (or development) environment (IDE) and the ability to download artifacts throughout the term of the contract. The Government reserves the right to witness all Contractor efforts to accomplish the SOW requirements and maintains the right to comment on processes. The Contractor shall provide 30 days' advance notice of any events, tests, or activity that the Government identifies as a specific item of interest.

[Note to Preparers: *While the Government will have access to and the ability to download work products contained in the integrated digital (or development) environment, the Government cannot effectively exercise its data rights unless these items are formally required to be delivered and accepted by the Government. Access to the environment does not in any way affect or replace data delivery requirements and data rights determinations.*]

Program Managers should consider including a requirement to have real-time access to the Offeror's (or an associated sub-contractor's) software development environment, providing the government with continuous online access to and the ability to download work products under development commencing at the start of work. See section titled "Data Management and Integrated Digital Environment (IDE)" below. Collaborative tools to support this access must be adopted, tailored, and applied by the program in a manner consistent with its specific requirements and circumstances.

[Note to Preparers: *While the Government can also separately contract for access to and the ability to download from the IDE beyond*

²⁸ The appropriate definition should be included in Section C. In this case, we define "component" consistent with the Institute of Electrical and Electronics Engineers (IEEE) definition from IEEE Std 610.12-1990, "one of the parts that make up a system. A component may be hardware or software and may be subdivided into other components."

the life of the development contract, such access is no substitute for delivery and acceptance of the work products, including technical data and software, associated with the acquisition. In any event, the Government's rights for technical data and software must be assessed, including validation of any asserted restrictions.]

In satisfying the Government's requirements, the following system architecture approach characteristics shall be utilized:

- 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.
 - i. Ensure that external information exchange requirements are implemented in a standard and open manner as part of this effort. These actions shall include planning that identifies the contractor's specific approach to ensuring system and interface data is well-defined, available to all programs, and uses a standards-based tool for definition within the context of DoD and Service upgrade programs. The contractor shall develop system upgrades, IT system capabilities and business rules that ensure that: 1) data will be posted to shared spaces for users to access and download except when limited by security, policy, or regulations; 2) data shall provide for interoperability with many-to-many exchanges of data, and verified trust and integrity of users and applications; and 3) data shall be transmitted through well and openly defined interfaces.
 - ii. The contractor shall ensure that its projects, at the architectural and operational level, continue to promote the use of an open architecture as well as adoption of other standards and requirements, tailored to meet its specific Service and Joint requirements.
 - b. Modular, Open Design – The contractor shall develop an architecture that is layered and modular and uses standards-based COTS/NDI hardware, operating systems, and middleware that all utilize either non-proprietary or non-vendor-unique key module or component interfaces. The contractor's design approach shall be applied to all subsystems and components. As part of its Open System Management Plan, the contractor shall, at a minimum, - describe how the proposed system architecture meets these goals, including the steps taken to use non-proprietary or non-vendor unique COTS or reusable NDI components wherever practicable.
-

- i. **Module Coupling** – The contractor’s design approach shall result in modules that have minimal dependencies on other modules (loose 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.
- ii. **Module Cohesion** – The contractor’s design shall result in modules that are characterized by the singular assignment of identifiable and 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.
- c. **System Requirements Accountability** – The contractor shall 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.
- d. **Inter-component Dependencies** – 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 the technical data describing the interface shall be available to the Government with at least Government Purpose Rights. The system architecture shall minimize inter-component dependencies to allow components to be decoupled and reused, where appropriate, across various DoD or Service programs and platforms.

[Note to Preparers: *PMs should seek assistance from Legal Counsel when dealing with small businesses performing work under SBIR contracts. DoD policy, particularly that set forth in the SBIR data rights clause, DFARS 252.227-7018, should be reviewed by PMs, including the SBA's SBIR Policy Directive.²⁹ The entire policy is worth reviewing, but in particular Section 8 sets forth controlling policy on data rights for SBIR contracts.]*

- e. Modular Open Systems Approach (MOSA) – 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 reused. The contractor's rationale shall explicitly address any tradeoffs performed, particularly those that compromise the modular and open nature of the system.

[Note to Preparers: *These provisions can be implemented using suitable Data Item Descriptions (DIDs) and Contract Data Requirements Lists (CDRLs). If this is a follow-on development, the Program Manager should identify the components of interest. The contractor should then document the rationale for those components; however, it is not intended that the contractor document historical decisions made for the entire system.]*

- f. 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: (1) technology obsolescence, (2) being locked into proprietary or vendor-unique technology, and (3) reliance on a single source of supply over the life of the system.
- h. Design Information Documentation – The contractor shall document and model the system or component (e.g., software,

²⁹ See <http://www.sbir.gov/about/about-sbir> for more information.

hardware, middleware) design information using industry standard formats (e.g., Unified Modeling Language). It shall also document and model 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 the design information and models are current with the as-built system.

- i. Technology Insertion – 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.
- j. Life Cycle Sustainability – The contractor shall consider use of COTS/NDI and open standards to enhance the system’s life cycle sustainability by implementing performance-based logistics (PBL) arrangements to sustain the components through their life cycle.

[Note to Preparers: *Program sustainment strategies such as PBL should be tailored to program-specific hardware, software and middleware requirements. A Business Case Analysis (BCA) should be done in conjunction with development of these strategies to ensure that the strategies are appropriate for the business and technical model being incorporated in the program.*]

- k. Interface Design and Management – The contractor shall:
 - 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,³⁰ and hardware interfaces;
- 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 [*Insert any PEO-specified documents*];
 - 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” teams in an integrated team approach to effectively identify how individual changes impact the system’s internal or external interfaces and information exchange standards.³¹
- l. Treatment of Proprietary or Vendor-Unique Elements – The contractor shall explain the use of proprietary, vendor-unique or closed components or interfaces. If applicable, the contractor shall define its process for identifying and justifying proprietary, vendor-unique or closed interfaces, code modules, hardware, firmware, or software to be used. When interfaces, hardware, firmware, or modules that are proprietary or vendor-unique are required, the contractor shall demonstrate to the Government that those proprietary elements do not preclude or hinder other component or module developers from interfacing with or otherwise developing, replacing, or upgrading open parts of the system.

³⁰ “Firmware” is considered to be a category of “Computer Software” as defined in the DFARS.

³¹ “Community of Interest (COI)” means a collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes, and therefore must have shared vocabulary for the information it exchanges. [*DoD 8320-2*]

- m. As Built Configuration List Identification of Modification Items and Funding Source – The contractor shall prepare and deliver a comprehensive list of items (to include parts, components, sub-assemblies, assemblies, SRUs and LRUs) that during or in connection with the performance of the contract that are new or have been redesigned, modified, or otherwise changed. Such list shall be specific as to description, nomenclature, part number, higher order subassembly or assembly, the nature of the redesign, modification or other change. (DI-CMAN-81516/T, As Built Configuration (ABCL) – Modified Item and Funding Source, A001; DID: DI-CMAN-81516). In addition, and as specific and discrete task requirements of this contract, the contractor shall further identify in the ABCL, with respect to each such listed new, redesigned, modified, or changed item, the purpose of the redesign, modification or other change and the source of both the requirement and the funding for such redesign, modification or other change. In identifying the funding source, the contractor shall, in the case of each redesign modification, or other change funded in whole or in part with government funding, specifically identify the contract, line item, and ACRN which funded or partially funded the redesign, modification, or other change.
- n. Open Business Practices – The contractor shall demonstrate that the modularity of the system design promotes the identification of multiple sources of supply and/or repair, and supports flexible business strategies that enhance subcontractor competition. The contractor shall conduct a market survey to identify candidate COTS, proprietary, open source software (OSS) and other reusable NDI capable of achieving the performance requirements of solutions that it proposes to custom build. The survey results shall be provided to support each major review. COTS and other reusable NDI selection criteria shall address the following factors, at a minimum: Electrostatic Sensitive Device (ESD) immunity; Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC); Integrated Logistics Support requirements; safety; reliability 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. Decisions leading to the selection of specific COTS, NDI, proprietary or OSS products
-

should be supported by appropriate analysis (e.g., with test results, architectural suitability, “best value” assessments, etc.).

- o. Reuse of Pre-existing or Common Items – The contractor shall reuse pre-existing or common items unless a determination is made to not reuse. 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 a common system and/or common elements or components which meet the performance requirements of the various DoD or Service platform missions, where commonality offers the greatest technical and cost benefits.

[Note to Preparers: *The specific repositories/libraries that the contractor will review for components should be identified.*]

- p. Third-Party Development – 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.
- q. Life Cycle Management and Open Systems – The contractor’s architecture shall provide for insertion of COTS into the system and demonstrate that 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 COTS and other reusable COTS or NDI products. The contractor shall establish a process to logistically support 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 COTS or NDI products. The contractor shall provide the proposed methodology for pass through of COTS warranties to the Government.
- r. Use of Standards – In designing the system(s), the contractor shall use the following standards in descending order of importance:
 - i. Standards as specified within the contract
 - ii. Commercial standards
 - a) Standards developed by international or national industry standards bodies that have been widely

adopted by industry. Examples of widely adopted standards are:

- 1) SQL for databases (e.g., SQL for databases ANSI ISO/IEC 9075-1, ISO/IEC 9075-2, ISO/IEC 9075-3, ISO/IEC 9075-4, ISO/IEC 9075-5)
 - 2) HTML for presentation layer (e.g., XML 1.0 www.webstandards.org)
 - 3) XML for data transfer
 - 4) Web services for remote system calls
- a) Standards adopted by industry consensus-based standard bodies and widely adopted in the market place.
 - b) De facto standards (those widely adopted and supported in the market place).

Note: Standards that are not specified within this contract or that are modified must be submitted to and approved by the Government Program Manager prior to use.

The following contains recommended language for the SOW in Section C of the RFP/contract:

2. **Statement of Work (SOW)** Within the SOW there shall be a “Technical Approach” section. This section describes the Government’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 the Government’s needs and the system to be acquired. Within the “Technical Approach” section, there shall be a subsection titled “Software Engineering Approach,” containing at a minimum the following language:
 - a. **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) (CDRL AOOx). The contractor shall follow this SDP for all computer software to be developed or maintained under this effort.

The 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. 12207.0. The 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. 12207.0, the 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 this task, the Offeror shall provide this detailed information so the Government can assess whether the Offeror's approach is viable.

The 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, at a minimum, specific standards, methods, tools, actions, strategies, and responsibilities associated with development and qualification.

- b. **Software Code Walkthroughs:** In addition, another step in the software development management process that supports OSA and can be included in Section C of the contract is the requirement to hold Software Code Walkthroughs. As an example, this requirement may look like this:

“The contractor shall conduct periodic code walkthroughs during the development Phase, as specified by the Statement of Work (SOW) or by Technical Instruction (TI). Senior technical personnel from the development team will review the code and unit test plans that have been developed for a Technical Design Specification (TDS). The purpose of the review is to identify that the code adheres to the program's development standards, is technically sound, meets the design articulated in the related TDS, and that the unit test plan for the code under review is documented in accordance with QA/Test standards as defined. The Government reserves the right to have one or more representatives, on a not-to-interfere basis, observe any and all code walkthroughs and create a detailed report.”

Code walkthroughs will not be conducted until the code has appropriate markings with respect to intellectual property rights. These walkthroughs help support the OSA principle of design disclosure.

- c. **Data Management and the Integrated Digital Environment (IDE):** The IDE is an integral tool for facilitating data management
-

and design disclosure. Including a requirement to maintain an IDE as part of contract performance is important to the Government's interests. The Government can gain access to technical data and computer software in an IDE. However, a requirement for an IDE is not a substitute for having formal technical data and software delivery requirements. In order to take formal delivery for deliverable items not originally identified, it is recommended that CDRLs, including the Data Accession List CDRL, in conjunction with priced option CLINs for additional deliverables and/or rights, and the Deferred Ordering clause, (DFARS 252.227-7027), be included in the contract and used to order necessary data up-front, and to preserve the Government's ability to order data that the Government anticipates may become necessary in the future. Further, as protection against failure of a contractor to maintain an IDE, for reasons such as technical failure, business failure (bankruptcy) or refusal to perform, the Government should take formal delivery, custody and control of necessary data at an appropriate time.

Including a Database Design Description Data Item Description (DBDD DID) DI - IPSC-81437 will require the Contractor to provide a textual description of the IDE instantiation, e.g., the file folders and hierarchy. Using this Data Item Description (DID) with a software DID, (e.g., DI-IPSC-81488 or DI-MCCR-80700) will allow the Government to obtain delivery of the IDE instantiation. The Database Design Description Data Item Description (DBDD DID) describes the design of a database, that is, a collection of related data stored in one or more computerized files in a manner that can be accessed by users or computer programs via a database management system (DBMS). It can also describe the software units used to access or manipulate the data. The DBDD is used as the basis for implementing the database and related software units. It provides the acquirer visibility into the design and provides information needed for software support. This DID contains the format and content preparation instructions for the data product generated by specific and discrete task requirements as delineated in the contract. This DID is used when the developer is tasked to define and record the design of one or more databases. Software units that access or manipulate the database may be described here or in Software Design Descriptions (SDDs) (DI-IPSC-81435). Interfaces may be described here or in Interface Design Descriptions (IDDs) (DI-IPSC-81436). The Contract Data Requirements List (CDRL) (DD 1423) should specify whether deliverable data are to be delivered on paper or electronic media;

are to be in a given electronic form (such as ASCII, CALS, or compatible with a specified word processor or other support software); may be delivered in developer format rather than in the format specified herein; and may reside in a computer-aided software engineering (CASE) or other automated tool rather than in the form of a traditional document.

[Note to Preparers: *Program Managers are encouraged to consult with Legal Counsel in developing this language as issues related to data rights, markings, and draft and unfinished data that arise from downloading information need to be resolved.*

The following is sample contract language for this requirement:]

“The contractor shall establish and maintain a data management program, as well as a secure Integrated Data Environment (IDE) for hosting all technical data and computer software used on or produced in the performance of this contract. Note: program management information such as cost, risk and schedule data can also be hosted in the IDE.

This purpose of the IDE is to create a seamless, collaborative data environment for the contractor and government team which contains all pertinent data about the project throughout its development and delivery. This data management program, including IDE structure, format, processes, and procedures, shall be documented as part of the contract Program Management Plan.

The contractor shall provide the Government team access to and the ability to download all data listed in the Data Accession List (DAL) DID DI-MGMT-81453A per CDRL _____ by actively using the IDE. All items posted to the IDE, including drafts of deliverables that are not final versions, shall be considered delivered for purposes of the DFARS data rights clauses (and subject to the same rights asserted for final deliveries). However, these non-final versions shall not constitute acceptance for purposes of Inspection and Acceptance requirements or the DFARS data rights clauses. The DAL shall contain the list of all data generated in support of this contract. Deliveries of data, in addition to the IDE, shall be as indicated in the CDRL attachment; delivery and subsequent distribution of technical data may be in storage media other than paper, including direct electronic exchange of data between two computers. The DAL shall be updated via a delivered data item each month, provided as an attachment and concurrently with the

Monthly Status and Progress Report, which shows the data added each month (incremental reporting), except for the _____ month deliverable report, which shall be provided as a separate data item showing the current and comprehensive listing. The procedures must provide for the identification of any portions of the data provided with restrictive legends, when appropriate. The acceptance criteria must be consistent with the authorized delivery format.

Data (technical data and computer software) shall be protected in accordance with the appropriate Program Protection Plans and Information Assurance guidelines. The Government reserves the right to witness all contractor efforts to accomplish the Statement of Work (SOW) requirements and maintains the right to comment on processes.

The contractor who operates and maintains the IDE shall indemnify the Government from any liability to data owners or licensors resulting from, or as a consequence of, a release or disclosure of technical data and computer software made by this IDE contractor or its officers, employees, agents, or representatives.

All computer software and technical data developed under this Contract and posted to the IDE shall be delivered with at least Government Purpose Rights, as defined in DFARS clauses 252.227.7013, -7014, and -7017 and appropriately marked as such unless a waiver has been submitted and approved by the Government. In this context, technical data and computer software developed under this contract do not include embedded open source software or COTS software products which must be identified to the government and the respective licenses provided. A scan report verifying the appropriate markings, including distribution statement, copyright statements, open source software, security classification and data rights shall be delivered with the data. In addition, metadata, as described in the _____ document, shall be provided with all final software and technical data for delivery into the Government's reuse repository.

The Contractor shall comply with the requirements of the DD 254 for implementation of the IDE and to ensure proper safeguarding of classified materials, events and processes. This shall include documentation developed by the Contractor or received in support of working groups and IPTs.

- d. **Product Reuse Demonstration:** Contractors shall consider use of third-party products that may be innovative or new to the program and provide compelling system performance improvements or best value. In particular, the Government's goal is to encourage contractors to reuse software and components, especially in cases where the Government has GPR or greater rights. As part of system acceptance, the contractor shall demonstrate the steps necessary to give third parties, as directed by the Government, the ability to integrate their components into the contractor's solution. This effort shall be comprehensive and require the contractor to perform the following activities:
- i. **Inventory:** A detailed inventory of all code files in the product baseline shall be conducted. This inventory shall extend to all third-party software not delivered within the terms of the contract but used in the system to form the working product. Third-party product descriptions and version information shall be required for all operating systems, applications, middleware, and device drivers.
 - ii. **Inspection:** File headers and any other company markings found in the source code shall be inspected to ensure clear indication that the Government has GPR to use the software delivered in the contract.
 - iii. **Build Procedure Development:** A build procedure shall be developed in sufficient detail to allow a third party to recreate the operational system on a compatible processing platform. This build procedure shall address the results of the code inventory and inspection to account for software that is not deliverable due to proprietary rights limitations such that the user can still complete the installation process.
 - iv. **Conduct Demonstration:** The contractor shall conduct a formal demonstration of the build process using the product baseline software and approved procedures to show the software can be successfully ported to other third-party compatible open architecture processing systems.
- e. **Technical Development Reviews:** In some cases, the Government may want to require the contractor to perform Technical Development Reviews. The purpose of these reviews includes, but is not limited to, observing that the design and other documentation is complete, complies with the established design approach, is technically sound and will satisfy the functional requirements. The following is sample contract language for this requirement:
-

f. **Perform Technical Development Reviews**

The contractor shall conduct formal technical reviews as well as periodic Technical Development Reviews for major capability upgrades. The contractor, in concert with the Government, shall develop a Design Review Plan for the conduct of formal reviews, using agreed upon tailoring of the Technical Review Manual (TRM) (Attachment J-9) and/or the System Engineering Management Plan (SEMP). The Contractor's approved Quality Assurance Program Plan (QAPP) shall also apply to documentation and CDRLs associated with the technical reviews. The purpose of these reviews is to observe that the design and other documentation is complete, complies with the established design and testing approach, is technically sound and will satisfy the functional requirements as defined in the approved Functional Design Specification documents. Senior technical personnel from the development team will review each design approach and Technical Design Specification as each is completed to ensure each has been properly documented as defined in the CDRL. The Government will establish entry/exit criteria and acceptance/rejection criteria for each formal review and will document these criteria in a Technical Instruction (TI). These Technical Reviews, both formal and informal, are to be scheduled in the Program Master Schedule so they are visible to the Government and documented in the CDRL. Technical Reviews shall include software program metrics as defined in:

TBD

i. Technical Review Objectives:

- a. Assess the development maturity based on technical development goals, systems engineering events and accomplishments, and empirical test data supporting progress to date.
- b. Ensure operational, functional, performance, information assurance, cost, schedule requirements and objectives, designs, implementations, technical performance measurements, and technical plans are being tracked, are on schedule, and are achievable within existing programmatic constraints.
- c. Assess the system requirements and allocations to ensure that requirements are unambiguous,

consistent, complete, feasible, verifiable, and traceable to top-level requirements.

- d. Demonstrate that the relationships, interactions, interdependencies, and interfaces between required items and externally interfacing items, system functions, subsystems, and system elements (including operators and maintainers), as appropriate, have been addressed.
 - e. Assess the degree of openness of the emerging system, its degree of DoD or Service-level Enterprise reuse, and critique any tradeoff decisions made.
- g. **OSA Approach to Developing to a Technical Review:** General and specific OSA objectives shall be developed to evaluate the degree of system openness as defined in the Open Architecture Assessment Tool (OAAT)³² and activities defined in the Open Systems Management Plan (OSMP).
- i. Define OSA objectives for each technical review as defined in the System Engineering Technical Review (SETR) manual.
 - ii. Tailor the OSA objectives to what can be accomplished by the time of the review and for which there is supporting technical information.
 - iii. Map OSA objectives to specific metrics from the OAAT and the results of activities defined in the OSMP.
 - iv. Record the OSA objectives and the results of the metrics and activities as an input to the technical review.
- h. **Example OSA Technical Review Objectives:**
- i. The OSA emphasis for Alternative Systems Review (ASR) is on innovation and competition. A specific focus will be to evaluate the degree to which functionality and solutions are drawn from a diversified range of large and small businesses and maximize affordable use of COTS/NDI.
 - ii. The OSA emphasis for System Requirements Review (SRR) is on collaboration and the accessibility and availability of data. A specific focus will be to evaluate the consistency between the system requirements and open system design

³² The OAAT is a Navy-developed tool that can be used to assess the openness of programs. It is available for downloading at <https://acc.dau.mil/oa>.

- considerations, ensuring that the preferred system solution does not contain design specific solutions.
- iii. The OSA emphasis for System Functional Review (SFR) is on enterprise architectures, strategic reuse, and the potential for small business participation throughout the program life cycle. A specific focus will be to evaluate whether the system functional definition follows modular design tenets and well-defined interfaces to effectively manage risks of obsolescence and dependence upon a sole source of supply.
 - iv. The emphasis of the OSA objectives for Preliminary Design Review (PDR) is on the requirements tradeoffs to meet performance. A specific focus will be to evaluate the degree to which inter-component dependencies preclude affordable and lower-risk future open system capability insertion, which will drive cycle-time for capability improvements.

Chapter II: DEVELOPING CONTRACT LINE ITEM NUMBERS (CLINs) – RESERVED

This section is being developed and will be revised in the future.

[Note to Preparers: *Establish separate Contract Line Item Numbers (CLINs) for technical data/computer software to be delivered under a contract as required by DFARS 227.7103-1(b)(3) and 227.7203-1(b)(3). Solicitations and contracts should also include priced contract option CLINs for future delivery of technical data and computer software that were not acquired upon initial contract award. Although the Deferred Ordering clause at DFARS 252.227-7027 should be included in contracts, the Government should not overestimate the scope of that clause, e.g., it does not cover technical data or computer software that were not generated under the contract.³³ Priced contract option CLINs should also be included for technical data rights licenses or computer software licenses when the Government desires additional rights in technical data/computer software. Consult with the cognizant contracting officer for preparation of CLINs and option CLINs.]*

³³ Note that Section 815 of the NDAA for Fiscal Year 2012 (Pub. L. 112-81) added new paragraph (b)(9) to 10 U.S.C. § 2320, which creates a new deferred ordering scheme that will be implemented in the DFARS (see pending DFARS case 2012-D022).

Chapter III: EXAMPLES OF SECTION H SPECIAL CONTRACT REQUIREMENTS

Section H of the Request for Proposal (RFP) and the resulting contract contains special clauses that can be incorporated into contracts as appropriate. The following are examples taken from contracts that may be useful to programs. An additional helpful reference is the Department of Defense Handbook for Preparation of Statement of Work (SOW).³⁴ These clauses may not be required as mandatory for use unless a class deviation is acquired in accordance with FAR Clause 1.404.

[Note to Preparers: *Appendix 8 contains information on “Clickwrap” license issues and suggested clauses that can be used to prevent contractor use of “Clickwrap” licenses to circumvent Government Purpose Rights.*]

[Note to Preparers: *“Section H Special Provisions” should only be developed and used in close coordination with Legal Counsel. Legal Counsel should review and advise all Section H Special Provisions.*]

[Note to Preparers: *The program should consider developing a “Section H Special Provision” that, at a minimum, incorporates the Contractor’s proposal relating to an Open System Management Plan into the resultant contracts and requires Government concurrence prior to any change in that plan.*]

[Note to Preparers: *When citing regulations such as the DFARS and FAR, dates are included where possible to reflect the most recent version of this Guidebook. However, Contracting Officers and PMs need to check for current clause dates before using the language in this Guidebook.*]

The following clauses have been used successfully in individual procurements, however, the clauses have not been through the formal vetting process and are not approved for general use. Any clause similar to or substantially the same as the samples that follow, must go through local legal review prior to inclusion in any request for proposal or contract.

This section contains only recommended guidance, and is offered with the understanding that individual PEOs and Program Managers can be flexible in selecting those items needed to meet their needs.

³⁴ The DoD Handbook for Preparation of Statement of Work (SOW) is available on the web at <https://acc.dau.mil/CommunityBrowser.aspx?id=46583>.

1. REQUIREMENT FOR AN OPEN SYSTEM MANAGEMENT PLAN

The contractor shall submit to the Government an Open System Management Plan as set forth in the Contract Data Requirements List (CDRL). At a minimum, the plan shall address the following:

Technical Approach and Processes

Open Systems Approach and Goals. The contractor shall prepare and submit for Government approval its Open System Management Plan which shall include its approach for using modular design, standards-based interfaces, and widely-supported, consensus-based standards to achieve the following goals:

- a. **Resource Sponsor OSA Requirements** – A detailed description of the contractor’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 Contractor’s approach to facilitate the sharing of system or component, e.g., software, hardware, middleware design information. The Contractor 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 Contractor shall identify the proposed standards and formats to be used.
- c. **Technology Insertion and Refresh** – A detailed description of how the contractor’s proposed system will allow for rapid and affordable technology insertion and refresh. At a minimum, the contractor shall 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 contractor’s architectural approach will support this requirement including how components from third-party providers and other potential 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 contractor shall describe what artifacts from

repositories or libraries, or common components it intends to use within its proposed solution.

[Note to Preparers: *Insert the specific asset reuse repositories/libraries that will be made available to Contractors.*]

[Note to Preparers: *Common components may be specified by the PEO or Program Manager.*]

- e. **Modular Open Systems Approach (MOSA)** – A detailed description of the contractor’s modular, open systems approach. At a minimum, the contractor shall address the following:
 - i. Plans for integrating the systems both internally and with external systems;
 - ii. The means for ensuring conformance to open standards and profiles throughout the development process, as discussed in Section C;
 - 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 COTS or reusable NDI insertion, technology refresh strategies, and other appropriate means); and
 - v. Identification of processes for the following:
 - a) Isolating functionality through the use of modular design;
 - b) Evaluating modular open system baseline standards, defining and updating profiles, and evaluating and justifying new or vendor-unique profiles;
 - c) Validating implementation conformance to selected profiles;
 - d) Managing application conformance to selected profiles; and
 - e) Training in use of profiles.
 - f. **MOSA as an Enabler of OSA Objectives** – A detailed description of how the contractor 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 not be limited to, technology obsolescence and dependence on proprietary or vendor-unique technology.
- g. **Life Cycle Supportability** – A detailed description of how the contractor intends to enhance life cycle supportability by using or enabling proven cost-saving methods such as performance-based logistics arrangements to sustain the components through their life cycle.

[Note to Preparers: *Program sustainment strategies such as PBL should be tailored to program-specific hardware, software and middleware requirements. A Business Case Analysis (BCA) should be done in conjunction with development of these strategies to ensure that the strategies are appropriate for the business and technical model being incorporated in the program.*]

- h. **Employ a Layered, Modular Architecture** – A detailed description of how the proposed system architecture is layered, modular, and makes maximum use of Commercial-Off-the-Shelf/Non-developmental Item (COTS/NDI) hardware, operating systems, and middleware that utilize non-proprietary key interfaces whenever practicable.
- i. **Traceability of System Requirements** – A detailed description of the contractor's approach for ensuring that all system requirements (including those contained in the Initial Capabilities Document, Capabilities Development Document, and in Section C) 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 contractor’s approach for designing a system that, to the maximum extent practicable, minimizes inter-component dependencies and allows components to be decoupled and reused, where appropriate, across various DoD or Service programs or replaced by competitive alternatives.
- k. **Rationale for Modularization Choices** – A detailed description of the contractor’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 plan, at a minimum, must demonstrate how the modular design strategy applies, and the effect it will have on future systems upgrades. The contractor shall describe how it proposes to work with the Government to incorporate periodic Government requests for inserting new technologies or capabilities without adversely impacting the modular design strategy.
 - ii. The contractor 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 contractor’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.
- m. **Interface Design and Management.** The contractor shall describe how it will clearly define component and system interfaces. At a minimum, the contractor shall address the following:
 - i. The contractor shall describe how it will define and document all subsystem and configuration item (CI) level interfaces to provide fully functional, physical and electrical specifications.

- a) The contractor 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.
 - b) Interfaces described shall include, but not be limited to, mechanical, electrical, e.g., power and signal wiring, software, e.g., APIs, firmware, and hardware.
 - c) The contractor shall address the interface and data exchange standards between the component, module, or system and the interconnecting or underlying information exchange medium.
 - d) The contractor shall state how these interfaces support an overall Information Assurance strategy that provides a defense in depth in accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI 3170.01E "Joint Capabilities Integration and Development System" 11 May 2005³⁵ and [Add appropriate PEO-specified requirements. Additional information can be found at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf].
 - e) The contractor shall state how form, fit, and function (FFF) data deliverables and data rights will be provided to the Government. (See U.S. Code Title 10 § 2320.)
- ii. The contractor 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 contractor 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.
 - iii. The contractor shall describe how its system will allow for the following:
 - a) Quickly interconnecting, reconfiguring, and assembling existing systems, subsystems, and components;

³⁵ <https://acc.dau.mil/adl/en-US/132122/file/26664/CJCSI%203170.01E.pdf>

- b) Interchanging and using information, services and/or physical items among components within a system;
 - c) Interchanging and using information, services and/or physical items among systems within an integrated architecture, platform, PEO, Community of Interest, or a DoD component;
 - d) Supporting reuse of software and the common use of components across various product lines; and
 - e) Transferring a system, component, or data, from one hardware or software environment to another.
- iv. The contractor 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 "Information Assurance (IA) Implementation" (dated February 6, 2003)³⁶ and [Add appropriate PEO-specified requirements. Additional information can be found at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf].
- v. The contractor shall describe the degree to which proposed interfaces use defined commercial or Government standards as called for in Section C.
- n. **Treatment of Proprietary or Vendor-Unique Elements.** The contractor shall justify any use of proprietary, vendor-unique, or closed components, including but not limited to COTS, and interfaces in current or future designs. The contractor shall define its process for identifying and justifying proprietary, vendor-unique or closed interfaces, code modules, hardware, firmware, or software to be used.
- i. The contractor 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.
 - ii. The contractor shall include documentation to support the rationale for a decision to integrate proprietary, vendor-unique or closed system hardware and/or software functions within the proposed system.

³⁶ <http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>

- iii. The contractor 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.
- iv. The contractor 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.
- v. The contractor 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 sub-contractor competition.
 - a) The contractor shall conduct a market survey to identify candidate COTS and other reusable NDI, including Government IP assets, capable of achieving the performance requirements of solutions that it has proposed to custom build. Sound “market research” will help to identify opportunities to use COTS or reuse existing components. The 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, e.g. 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; and adequacy of available technical data, computer software, and intellectual property, including the extent to which the Government will have a right to use the technical data, computer software and intellectual property in future competitive acquisitions.

- b) The contractor shall describe the adequacy of available technical and intellectual property data and procurement data rights on the product; and Merits of the software supported by the product.
 - c) The Contractor shall identify those pre-existing items (Government IP assets, NDI, and COTS) it will evaluate for reuse. At a minimum, the Contractor shall describe what artifacts from the [**Note to Preparers:** *insert the specific asset reuse repositories/libraries that will be made available to Contractors*] it intends to use within its proposed solution. 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.
- vi. The contractor 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 Integrated Product Teams (IPTs), and to facilitate competition for component suppliers. The Contractor will provide a list of those proprietary or vendor-unique elements that it requests be exempt from this review.
- o. **Life Cycle Management and Open Systems.** The contractor shall describe and address the strategy for reducing product or system and associated supportability costs through insertion of COTS or reusable NDI products.
- i. The contractor shall identify and address a strategy to insert COTS technologies and other reusable NDI into the system and demonstrate that COTS, other reusable NDI, and other components are logistically supported throughout the system's life cycle.
 - a) The contractor shall identify specific hardware and software elements of the subsystem designs that are planned for COTS and other reusable NDI replacement and the supportability plans for those elements.
 - b) The contractor shall address how the subsystem design allows for timely and cost-effective replacement of subsystem elements or modules. The COTS/NDI selection processes shall be specifically addressed, including validation of those processes.
-

- ii. The contractor shall provide a description of processes that will be established and show that COTS and other reusable NDI products are logistically supported.
- iii. The contractor shall describe the availability of commercial repair parts and repair services, facilities and manpower required for life cycle support and illustrate that they are adequate to ensure long term support for COTS and other reusable NDI products. The Contractor shall provide the proposed methodology for pass through of COTS warranties to the Government.

2. EARLY AND OFTEN TECHNICAL DISCLOSURE

The contractor shall submit a detailed plan for making design and interface information available as soon as possible after it is defined or established. The contractor shall establish and maintain a process that will provide “early and often” design disclosure available to the Government and third-party contractors via Government-established access (e.g., the Naval Sea Systems Command Software/Hardware Asset Reuse Enterprise (SHARE) library or other DoD repository/library resources, such as the Forge.mil Program (<http://www.forge.mil/>)) to in-process design documentation and computer software. Access to and the ability to download this information shall be supported using industry standards and made available to the Government. The information contents of the repository shall be clearly visible. The exchange of information shall be structured so as to protect the Contractor's and third-party developers' proprietary or vendor-unique rights in the information. The plan shall address how comments from the Government and third-party contractors are resolved. The plan shall describe a schedule of when non-proprietary licenses, source code, drawings, repair and engineering documentation will be provided to the Government and third-party contractors at specified key events or at defined intervals.

[Note to Preparers: *Use this clause in consultation with Legal Counsel as issues related to data rights, markings, and draft and unfinished data that arise from downloading information need to be resolved.*]

3. IDENTIFICATION AND ASSERTION OF RESTRICTIONS ON COMMERCIAL TECHNICAL DATA AND COMPUTER SOFTWARE

[Note to Preparers: *This and the following H Clause present two alternatives that have been used by past programs for addressing the identification of Open Source Software (OSS) in items delivered to the Government by contractors.*]

- a. **Definitions.** The terms used in this special contract requirement and associated CLINs are defined in the following clauses or sources:
 - i. DFARS 252.227-7013 RIGHTS IN TECHNICAL DATA-NONCOMMERCIAL ITEMS (FEB2012);
 - ii. DFARS 252.227-7014 RIGHTS IN NONCOMMERCIAL COMPUTER SOFTWARE AND NONCOMMERCIAL COMPUTER SOFTWARE DOCUMENTATION (FEB2012);
 - iii. DFARS 252.227-7015 TECHNICAL DATA-COMMERCIAL ITEMS (DEC2011); or,
 - iv. DFARS 252.227-7017 IDENTIFICATION AND ASSERTION OF USE, RELEASE, OR DISCLOSURE RESTRICTIONS (JAN2011).
- b. **Identification and Assertion of Restrictions.** The Contractor shall not deliver or otherwise provide to the Government any technical data or computer software with restrictive markings (or otherwise subject to restrictions on access, use, modification, reproduction, release, performance, display, or disclosure) unless the technical data or computer software are identified in accordance with the following requirements:
 - i. **Pre-Award Identification and Assertion.** The Contractor (including its subcontractors or suppliers, or potential subcontractors or suppliers, at any tier) shall identify all technical data and computer software that it proposes will be delivered or otherwise provided (including all Option CLINs as if the Option was exercised) with less than Unlimited Rights as follows:
 - a) **Noncommercial Technologies.** Restrictions on noncommercial technical data and noncommercial computer software shall be identified pursuant to DFARS 252.227-7017.
 - b) **Commercial Technologies.** The contractor shall also identify and assert any restrictions for all commercial computer software, including Open Source Software, and commercial technical data, i.e., technical data pertaining to a commercial item, using the format provided below at paragraph f of this clause.

- c) An Contractor's failure to submit, complete, or sign the identification and assertions required by paragraphs b.i.a) or b.i.b) of this clause with its offer may render the offer ineligible for award.
 - d) If the Contractor is awarded a contract, the assertions identified in paragraphs b.i.a) and b.i.b) shall be listed in an Attachment to that contract. Upon request by the Contracting Officer, the Contractor shall provide sufficient information to enable the Contracting Officer to evaluate any listed assertion.
- ii. Post-Award Updates to the Pre-Award Identification and Assertions. Except as provided in this paragraph, the Contractor (including its subcontractors or suppliers at any tier) shall not supplement or revise the pre-award listings or notices required by paragraph b.1 of this clause after contract award.
 - a) Noncommercial Technologies. Post-award identification and assertion of restrictions on noncommercial technical data and noncommercial computer software are governed by paragraph (e) of DFARS 252.227-7013 and DFARS 252.227-7014, respectively.
 - b) Commercial Technologies. The contractor may supplement or revise its pre-award identification and assertion of restrictions on commercial computer software and commercial technical data only if such an expansion or revision would be permitted for noncommercial computer software or noncommercial technical data pursuant to paragraph b.ii.a) of this clause, i.e., based on new information, or inadvertent omissions that would not have materially affected source selection.
 - c) Specific Identification of Technical Data and Computer Software. When identifying and asserting restrictions on technical data and computer software pursuant to paragraph b of this clause, the Offeror/Contractor shall:
 - 1) Ensure that the technical data and computer software are identified by specific reference to the requirement to deliver or provide that technical data or computer software in the contract, e.g. by referencing the associated CLINs, CDRLs, or paragraphs in the statement of work.

- 2) Include the relevant information for all technical data and computer software that are or may be required to be delivered or otherwise provided under the contract - including all Option CLINs or other optional or contingent delivery requirements (i.e., presuming that the Government will exercise the option to require delivery), online or remote access to information, and firmware or other computer software to be embedded in hardware deliverables.
- c. Copies of Negotiated, Commercial, and Other Non-Standard Licenses. The Contractor shall provide copies of all proposed specially negotiated license(s), commercial license(s), and any other asserted restrictions other than Government purpose rights; limited rights; restricted rights; SBIR data rights for which the protection period has not expired; or Government’s minimum rights as specified in the clause at 252.227-7015.
- d. Use of Open Source Software Without Delivery. The Government treats Open Source Software (OSS) as a category of commercial computer software. If the Contractor proposes to use OSS while performing under the contract, the Contractor shall follow the same rules prescribed in the Contract for commercial computer software. Additionally, the Contractor must ensure that its use thereof does not: (i) create, or purport to create, any Government distribution obligations with respect to the computer software deliverables; or (ii) grant, or purport to grant, to any third party any rights to or immunities under Government intellectual property or Government data rights to the Government computer software deliverables.
- e. Table Format for Identification and Assertion of Restrictions. A suggested format required by paragraph b.i.b) for identifying the commercial technical data/commercial computer software restrictions is as follows:

Commercial Technical Data/Computer Software Title and Version # *	If Open Source Software, Open Source License and Version # **	Name of Contractor Delivering Commercial Software ***	Technical Use/Implementing Approach ****	If OSS, Was OSS modified by contractor? *****	If OSS and OSS was modified, was OSS modified by incorporation into a third party's software? *****

* The complete title and version number of the Commercial Software should be listed. If the line item is Open Source Software that was downloaded from a website, the website address should also be provided.

** The Open Source Software license and version number should be listed. If a version number is not available, the contractor should state no version number.

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

**** The contractor should describe the functionality of the Commercial (Open Source) Software, and where it is being used within the larger computer software deliverable (if applicable).

***** If the contractor is delivering OSS, the contractor should state whether it has modified the Open Source Software.

***** If the contractor is delivering OSS that it has modified, the contractor should state whether the Open Source Software was modified by combining with another party's non-open source software. If the other party is a third party, the third party's non-open source computer software may be licensed with distribution restrictions which would not allow the Government to accept delivery of the software combination.

4. CONTRACTOR USE OF COMMERCIAL COMPUTER SOFTWARE, INCLUDING OPEN SOURCE SOFTWARE

[Note to Preparers: *This and the previous H Clause present two alternatives for addressing the identification of OSS in items delivered to the Government by contractors. The first clause has been in use for several years and served as a first attempt to help programs understand the OSS they may be acquiring in their contractor-delivered items. This second clause is a recent update that incorporates “lessons learned.”*]

- a. Contractor Use of Commercial Computer Software, including Open Source Software. Open source software is often licensed under terms that require a user to make user's modifications to the open source software or any software that the user combines with the open source software freely available in source code form pursuant to distribution obligations in the license.
 - i. In cases where the Contractor proposes to use open source software while performing under a Government contract, regardless of whether the open source software is delivered, the Contractor shall not create, or purport to create, any Government distribution obligation with respect to Government computer software deliverables.
 - ii. Prior to using any commercial computer software, the Contractor shall additionally evaluate each license for commercial computer software, including open source software which is considered commercial computer software, and confirm that each of the following requirements is satisfied:
 - a) A license for a particular commercial computer software shall be compatible with all licenses for other commercial computer software that are or will be linked to, adapted to, integrated, combined or merged with the particular commercial computer software, including when the particular commercial computer software and the other commercial computer software are used with another computer program;
 - b) A license for commercial computer software shall not impose a future Government distribution obligation that is foreseeable by the Contractor;
 - c) A license for commercial computer software shall not be terminated by the Contractor's use of the commercial computer software in performing under the contract; and

- d) Contractor's cost to comply with this requirement presents no additional cost to the Government.
- b. If, as a result of the Contractor's evaluation, the Contractor satisfies all of the requirements in paragraphs a.ii.a) through a.ii.d) above, then the Contractor shall provide a written summary report of the above findings to the Government Contracting officer stating that the Contractor has evaluated the commercial computer software use and the commercial computer software license, and made each determination required in paragraphs a.ii.a) through a.ii.d) above. The contractor shall request permission from the Government Contracting Officer to use the proposed commercial computer software. This notification shall also include all information regarding the identification and proposed use(s) of the commercial computer software in the format required by the contract in section [_____].

[Note to Preparers: *The program should clearly define where in the contract or elsewhere the commercial computer software format is defined.*]

- c. If the Contractor is unable to satisfy all of the requirements in paragraphs a.ii.a) through a.ii.d) above for a particular commercial computer software license, then the Contractor may not use the commercial computer software covered by the particular license without prior approval by the Contracting Officer. If the Contractor wants to use the Commercial Computer Software for which the requirements of paragraph a.ii.a) through a.ii.d) are not satisfied, the Contractor shall request approval to use the otherwise prohibited subject commercial computer software from the Contracting Officer by providing a written notification address the following: (i) the name and version number of the software; (ii) the name of the applicable license(s); (iii) a brief description of the technical use and implementing approach; (iv) a "yes/no" indication as to whether the Contractor has made, or will make, any modifications to the source code; (v) the software website; and in addition (vi) an identification of the reason(s) that the Contractor was unable to make the determinations in paragraphs a.ii.a) through a.ii.d) above.

For definition of "Commercial Computer Software" see DFARS 252.227-7014 and DoD CIO memorandum dated October 16, 2009 (ATTACHMENT 2).

[Note to Preparers: *"Section H Special Provisions" should only be developed and used in close coordination with Legal Counsel. Legal Counsel should review all Section H Special Provisions. The following*

are three examples of special licenses – there are many other versions. Program Managers should consider using a triggering event to change the rights associated with data if that will provide an incentive for Contractors to pursue the Government’s project opportunity, e.g., data can be delivered with restrictive rights for a period of time but convert to GPR upon reaching a defined milestone. By definition, any Special Negotiated License rights must be negotiated by both parties.]

5. SPECIAL LICENSE [Fill in based on the Section B Data Rights Table.]

EXAMPLE 1

- a. The United States Government has Specially Negotiated License Rights in the Data. Specially Negotiated License Rights means the right to:
 - i. Use, modify, reproduce, perform, display, or disclose the Data within the Government without restriction; and
 - ii. Release or disclose the Data outside the Government and authorize persons to whom the release or disclosure has been made to use, modify, release, perform, display, or disclose that Data for United States Government Purposes.
- b. Data, as used in this clause, means all the information delivered to the Government as required by CDRL.
- c. United States Government Purposes, as used in this clause, has the same definition as Government Purpose found at DFARS 252.227-7013 and DFARS 252.227-7014, except the following:
 - i. It does not include foreign military sales (FMS) and Foreign Military Funded (FMF); and
 - ii. It does not include allowing states and/or local governments to directly procure equipment utilizing the [*Complete based on the program specifics*] for any purpose or to authorize parties other than the Federal Government to do so.

EXAMPLE 2

- a. License Grant. Contractor hereby grants, or shall obtain for the Government, the following royalty-free, i.e., paid-up, worldwide, nonexclusive, irrevocable license rights:
 - i. The Government shall have Government Purpose Rights in all data; however, the Government Purpose Rights shall not include the right to use the data for reprourement.

- ii. The Government Purpose Rights cited above will expire on _____, after which the government shall have Unlimited Rights in the data.
- iii. All noncommercial technical data and noncommercial computer software other than the data that are delivered under the contract shall be delivered with Unlimited Rights. However, Contractor may deliver any updates to the data under the terms of this agreement.
- b. Title. Title to the data is not affected or altered in any way by this agreement.
- c. Marking Requirements.
 - i. Contractor shall mark all noncommercial technical data delivered under the contract with special license rights markings in accordance with paragraph (f)(4) of DFARS 252.227-7013, as follows:

“Special License Rights
The Government’s rights to use, modify, reproduce, release, perform, display or disclose these data are restricted by Contract No. _____, License No. X. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings.”
 - ii. Contractor shall mark all noncommercial computer software/computer software documentation products delivered under the contract with special license rights markings, in accordance with paragraph (f)(4) of DFARS 252.227-7014, as follows:

“Special License Rights
The Government’s rights to use, modify, reproduce, release, perform, display or disclose this software are restricted by Contract No. _____, License No. X. Any reproduction of computer software, computer software documentation, or portions thereof marked with this legend must also reproduce the markings”
- d. Disclosure Requirements. The Government shall follow the requirements of DFARS 252.227-7013 and DFARS 252.227-7014 with respect to disclosure of any technical data and computer software. Specifically, before disclosing any technical data and computer software to a recipient outside of Government, the Government shall require the recipient to execute the non-disclosure agreement specified at DFARS 227.7103-7, *Use and*

Non-Disclosure Agreement. The executed Non-Disclosure Agreement (NDA) shall be incorporated into Section J of the contract, and a copy of the executed NDA shall be provided to Contractor. The NDA shall also specifically name Contractor as a third-party beneficiary.

e. Marking Remedies.

- i. The rights of the parties concerning removal of unjustified or nonconforming markings on data under the contract shall be as set forth in paragraph (h) of the 7013 clause and paragraph (h) of the 7014 clause, as applicable.
- ii. All other disputes arising under this agreement shall be governed by the disputes clause of the contract, FAR 52.233-1.

f. General.

- i. This agreement is an attachment to the contract, and together they shall be the entire agreement between the parties in relation to the subject matter hereof, to the exclusion of all antecedent or present representations, undertakings, agreements or warranties, express or implied. In case of conflicts between the agreement and the contract, the contract shall take precedence over the agreement.
- ii. A failure or omission by either party to enforce any remedy for any breach of any term or condition of this agreement shall not be construed as a waiver of such term or condition.
- iii. The division of this agreement into articles, sections, and/or paragraphs and the insertion of paragraph headings are for convenience of reference only and shall not affect the construction or interpretation of the terms of this agreement.

EXAMPLE 3

a. License Grant.

- i. Access Rights. Upon the issuance of an order for ____ Access Rights under CLIN ____ (and, if options are exercised, ____), the Contractor shall grant the Government the right to access, use and reproduce the ____ IP, but only within the Department of the Defense (“DoD”) to generate internal DoD planning documents that are not to be disclosed outside of the DoD, and only for planning purposes. The Access Rights do not include the right to use the Project IP in the operation, management or delivery of network services, or the right to disclose Project IP (or materials derived from Project IP) to third parties for any purpose, including but not limited to competitive purposes, but the DoD may continue to allow access by the support contractors previously approved by the Contractor, as of the date of the order for Project IP Access Rights. Access shall be provided in accordance with Section _____. Under no circumstances will the Government be entitled to access rights without issuing the appropriate Task Order under CLIN ____ (and, if options are exercised, _____).
 - ii. Upon the issuance of an order for Government Purpose Rights (GPR) under CLIN ____ (and, if options are exercised, ____), Contractor grants GPR to the Government (whether embodied in TD, CS, trade secrets, copyright, or patents) in all Project IP. Inspection and Acceptance shall commence in accordance with Sections _____. In the event an order for GPR in Project IP is not issued, the Government’s rights shall continue to be governed by 1.1.1. Under no circumstances will the Government be entitled to GPR without issuing the appropriate Task Order under CLIN ____ (and, if options are exercised, _____).
- b. Other Forms of IP Protection. Contractor shall not assert any form of intellectual property protection, either against Government or against third parties, which would limit the Government’s full exercise of the rights granted in Section 1.1 of this agreement, provided Government is a licensee in good standing and Government and third party(ies) are in compliance with the terms of this license.
- c. License Restrictions. The Government acknowledges that title to and ownership of all intellectual property rights in the Project IP are and shall remain with Contractor and its licensors. The
-

Government acquires only the rights to the Project IP as defined herein and in accordance with Section 1.1 of this agreement, and does not acquire any ownership rights or title in or to the Project IP or that of Contractor's licensors. Accordingly, Government shall:

- i. not alter, publish, republish, perform, distribute, assign, sublicense, sell, adapt, lease, rent, reverse compile, reverse engineer, reverse assemble, transmit, display, decompile, translate, or use the Project IP other than as expressly permitted by this agreement;
- ii. take appropriate action by instruction, agreement, or otherwise, to ensure that the Project IP is used solely in the manner permitted under this agreement;
- iii. act promptly to prevent any breach hereof of the License Grant by any of its employees, agents or contractors;
- iv. immediately notify Contractor of any material violation of this License Grant; and
- v. reproduce and include the proprietary rights notice called for in section _____ on any copies of the Project IP, including partial copies and copied materials in derivative works.

Chapter IV: RECOMMENDATIONS FOR SECTION L INSTRUCTIONS CONDITIONS, AND NOTICES TO OFFERORS OR RESPONDENTS

[Note to Preparers: *Section L of the RFP provides proposal instructions, conditions and notices to Offerors. Section L should be carefully structured to address only those elements determined to be keys to success. The “Guide for Integrating Systems Engineering into DoD Acquisition Contracts,” (v.1.0, 12/11/2006) also calls for Section L to consider documentation of system interface requirements and incorporation of MOSA design considerations. The Guide also recommends that the Offeror describe its integration approach in terms of the degree that the technology insertion/obsolescence planning processes are integrated with overall program management processes and reflect the technical approach.]*

[Note to Preparers: *This section contains only recommended guidance, and is offered with the understanding that individual PEOs and Program Managers can be flexible in selecting and weighting those items needed to meet their needs. Programs should not feel that they need to address all of the items contained in these recommendations.]*

[Note to Preparers: *When citing regulations such as the DFARS and FAR, dates are included where possible to reflect the most recent version of this Guidebook. Contracting Officers and PMs need to check for current clause dates before using the language in this Guidebook.]*

Although the *Guidebook* was developed for mixed systems comprised of hardware, middleware and software elements, the recommended language can be easily tailored to reflect hardware- or software-only acquisitions.

Open System Architecture Guidance

[Note to Preparers: *The following is an extensive list of factors and subfactors that can be tailored and incorporated into Section L. Programs can delete the items they feel are redundant or not applicable for their specific acquisition requirements. Preparers need to include the factors and subfactors that will be determinant in the selection process and delete the factors and subfactors that are of minor or no importance. In particular, Program office personnel should be aware of asking for the same information in multiple places – the decision to do so should be deliberate and the evaluation of Offeror’s response done carefully.]*

1. Factor: Technical Approach and Processes

The Offeror shall describe its proposed Open Systems Architecture (OSA) technical approach and processes to be employed in performing this contract. At a minimum, the Offeror shall describe its OSA technical approach and processes in the following areas:

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:

- a. Address Program Sponsor OSA 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.

[Note to Preparers: *It is recommended that this proposed Open System Management Plan, which includes guidance for life cycle management, be incorporated into the resultant contract.*]

- 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 incremental development process. **[Note to Offerors:** *“Design Disclosure” can be enabled through a variety of mechanisms including keeping data, code and design artifacts in a repository either maintained by or overseen by the Government (such as DoD’s Forge.mil Program (<http://www.forge.mil/>)); providing the artifacts electronically upon requests made via the Government; or allowing requesting parties to obtain them directly from the Contractor through a process involving review and approval from the Government. Each program has the flexibility to establish the most appropriate mechanism for its specific needs; with a goal of establishing a process that is both cost-effective and responsive to requests.*] 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 system 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 [**Note to Preparers:** *insert the specific asset reuse repositories/libraries that will be made available to Offerors*] or common components [**Note to Preparers:** *these may be specified by the PEO or Program Manager*] it intends to use within its proposed solution. [**Note to Preparers:** *Programs must ensure that potential Offerors who do not have access to reuse repositories/libraries because they lack a current contractual vehicle are informed of the contents of the repositories and allowed access to artifacts as appropriate.*]
 - e. Modular Open Systems Approach (MOSA) – A detailed description of the Offeror's modular open systems approach. At a minimum, the Offeror shall address the following:
 - i. Plans/approaches 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 that enhances interoperability and the ability to integrate new capabilities without redesign of entire systems or large portions thereof;
 - iv. A description how risks associated with reliance on a single source of supply over the life of the system will be mitigated; to include but not be limited to, technology obsolescence and dependence on proprietary or vendor unique technology;
 - v. A description of the strategy for maintaining the currency of technology, e.g., through COTS or reusable NDI insertion, technology refresh strategies, and other appropriate means to reduce the development cycle time and total life-cycle cost; and
-

- vi. Identification of processes for:
 - a) Isolating functionality through the use of modular design;
 - b) Evaluating modular open system baseline standards, defining and updating profiles, and evaluating and justifying new or vendor-unique profiles;
 - c) Validating implementation conformance to selected profiles;
 - d) Managing application conformance to selected profiles; and
 - e) Training in use of profiles.
- f. MOSA as an Enabler of OSA 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 life cycle.

[Note to Preparers: *Program sustainment strategies such as PBL should be tailored to its specific hardware, software and middleware requirements. A Business Case Analysis (BCA) should be done in conjunction with development of these strategies to ensure that they are appropriate for the business and technical model being incorporated in the program.*]

- h. Employ a Layered Modular Architecture – A detailed description on how the proposed system architecture is layered, is modular, and makes maximum use of Commercial-Off-the-Shelf/Non-Developmental Item (COTS/NDI) hardware, operating systems, and middleware that utilize non-proprietary key interfaces 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 reused, where appropriate, across various DoD or Service 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.
[Note to Preparers: *If this is a follow-on development, the Program Manager should identify the components of interest. The Offeror should then document the rationale for those components; it is not intended that the Offeror document historical decisions made for the entire 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.

Subfactor 2. 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 [**Note to Preparers:** *Add appropriate PEO-specified requirements. Additional information can be found at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.]*
 - 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;
 - iii. Interchanging and using information, services and/or physical items among systems within an integrated architecture, platform, PEO, Community of Interest, or a DoD component;
 - iv. Supporting reuse of software and the common use of components across various product lines;
 - v. 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 and **[Note to Preparers: Add appropriate PEO-specified requirements.]**
- e. The Offeror shall describe the degree to which proposed interfaces use defined commercial or Government standards as called for in Section C.

Subfactor 3. Treatment of Proprietary or Vendor-Unique

Elements. The Offeror shall justify any use of proprietary, vendor-unique, or closed components, including but not limited to COTS, and interfaces in current or future designs. This justification shall include documentation of the decision leading to the selection of specific 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.

- 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 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 sub-contractor competition.
 - i. The Offeror shall conduct a market survey to identify candidate COTS and other reusable NDI, including Government-owned assets, capable of achieving the performance requirements of solutions that it has proposed to custom build. 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 data and computer software, and rights in technical data and computer software including the right to procure competitively; intellectual property rights; and an analysis of the merits of the software. The Offeror shall provide documentation of the decision leading to the selection of specific COTS products, *e.g.*, test results, architectural suitability, "best value" assessments, etc. The Offeror shall identify in a listing contained in its proposal to the Government all COTS/NDI

components³⁷, 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.

- ii. The Offeror shall identify those pre-existing items (Government intellectual property assets, NDI, open source software, and COTS) it intends to evaluate for reuse. At a minimum, the Offeror shall describe what artifacts from the **[Note to Preparers: insert the specific asset reuse repositories/libraries that will be made available to Offerors.]** 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. **[Note to Preparers: Programs must ensure that potential Offerors who do not have access to reuse repositories/libraries because they lack a current contractual vehicle are informed of the contents of the repositories and allowed access to artifacts as appropriate.]**
- 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 Integrated Product Teams (IPTs), 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.

Subfactor 4. Life Cycle Management and Open Systems. The Offeror shall describe and demonstrate the strategy for reducing product or system and associated supportability costs through insertion of COTS or reusable NDI products.

- a. The Offeror shall identify and demonstrate a strategy to insert COTS technologies and other reusable NDI into the system and demonstrate that COTS, other reusable NDI, and other components are logistically supported throughout the system's life cycle.

³⁷ The appropriate definition should be included in Section C. In this case, we define "component" consistent with the Institute of Electrical and Electronics Engineers (IEEE) definition from IEEE Std 610.12-1990, "one of the parts that make up a system. A component may be hardware or software and may be subdivided into other components."

- i. The proposal shall identify specific hardware and software elements of the subsystem designs that are planned for 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 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 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 COTS and other reusable NDI products are supportable.
 - 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 COTS and other reusable NDI products. The Offeror shall provide the proposed methodology for pass through of COTS warranties to the Government.

2. Factor: System Compliance with DoD or Service OSA Guidance

[Note to Preparers: *The language used in this section will be specified by the Service, Community of Interest or PEO. The material that follows should be tailored by each PEO/Community of Interest to meet its specific technical requirements, when enterprise-wide Service or Departmental requirements do not exist. The language should also be tailored to address different types of contracts, levels of systems acquisition, and phases in the acquisition life cycle.]*

- a. Each Offeror shall provide a narrative to the Government entitled “Open System Architecture Technical Guidance Narrative” (hereinafter referenced to as the “Narrative”). In preparation for drafting the Narrative, Offerors are requested to thoroughly review the [PEO-specified] technical guidance points provided in Table A below. The technical guidance points represent the critical technical characteristics required to implement the OSA design for deliverables under the contract awarded pursuant to this RFP.
 - i. Each Offeror shall provide a Narrative explaining how each technical guidance point in Table A is addressed in the proposal. For those technical guidance points in Table A that

the Offeror asserts are not applicable or not relevant to deliverables under the contract, the Offeror shall, in the Narrative, explain its basis for asserting non-applicability or non-relevance.

- ii. The OSA Compliance subfactor is directed to each of the technical guidance points in Table A below, and the Offeror’s ability to provide a Narrative explaining how its proposal meets each technical guidance point as defined by the [insert relevant reference]. A detailed description of each of the technical guidance points in Table A is provided in the [**Note to Preparers:** *PEO/Community of Interest-specified references and Guidance Points should be used in this table. Table A contains examples of technical guidance points from the Navy’s Surface Domain.*]

Table A

[PEO-specified] Technical Guidance Points	[PEO-specified] Reference Document Citation
Component design	
Portability	
Location transparency	
Client server	
Data distribution	
State data coherency	
Computational flow	
Fault tolerance	
Scalability	
Real-time performance	
Process, thread & memory management	
Data brokers	
Cabling and Cabinets	
Information Transfer	
Computing Resources	
Peripherals	
Operating Systems	
Adaptation Middleware	
Distribution Middleware	
Frameworks	

[PEO-specified] Technical Guidance Points	[PEO-specified] Reference Document Citation
Dynamic Resource Management	
Instrumentation	
Failure Management	
Information Assurance	
Time Service	
Programming Language Facilities	
Displays	
System Test and Certification	
Selection of Standards	

3. Factor: Management Approach

[Note to Preparers: *The first paragraph below is standard contract language with some modification to reflect the objective of facilitating competition at appropriate system or subsystem levels. While the number of contractors or subcontractors working on a contract is not necessarily a guaranty of openness, effective competition at the component-level is facilitated by OSA. The second paragraph articulates the view that true competition cannot be measured by the percentage of work awarded but rather the significance of their contributions. The third paragraph establishes the requirement for the contractor to establish and manage useful metrics that will effectively measure OSA achievements. These metrics can then be used to structure an incentive strategy that rewards the contractor for achieving OSA implementation success (or vice versa). A contractor tends to focus on what is incentivized.]*

- a. The Offeror shall describe the management structure, processes and procedures proposed for planning, monitoring, controlling, and delivering the required contract deliverables, artifacts, and data items required for delivery under the Contract Data Requirements List (CDRL.) The Offeror shall describe its approach to managing the efforts required for this contract. Of particular interest to the Government is the Offeror’s approach for facilitating competition at various levels (tiers) of the logical or modular subdivisions or tasks and for awarding significant portions of the overall system to third-party sources.
- b. The Offeror shall describe its approach for using Integrated Product Teams (IPTs) to improve processes, proactively manage

risk and increase efficiency. The Offeror shall describe the steps it shall take to educate IPT members and others involved in the project on the importance and principles of OSA.

- c. The Offeror shall describe their metrics approach to measure OSA performance and reuse efficiency. The Offeror shall describe the process they will utilize for measuring the development of the [insert program description] assets. The Offeror shall describe how the results of the proposed measure will inform project decisions or recommendations and provide for future competitions across multiple systems and platforms.

4. Factor: Data Rights and Patent Rights

[Note to Preparers: The Government always has the flexibility to negotiate for the Data Rights and Patent Rights it requires. Depending upon the potential for reuse, the Government has flexibility to attempt to purchase outright (rarely necessary) or enter into licensing agreements, depending upon the percentage of development costs originally paid for by the Government (up to 100%) and the willingness of the contractor to sell or license. Per 10 U.S.C. Section 2320(a)(2)(F): “As a condition of being responsive to a solicitation or as a condition for the award of a contract, the Government cannot require the Offeror to sell or otherwise relinquish to the United States any rights in technical data developed by a contractor or subcontractor exclusively at private expense or require the Offeror to refrain using an item or process to which the contractor is entitled to restrict rights in data.”]

- a. The Offeror shall propose 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. The Offeror shall also propose the TD, CSD, and CS reuse portability for use on other systems or platforms.

[Note to Preparers: The Government should include a formal analysis of its data rights requirements in a Technical Data Rights Strategy (TDRS) as part of the Acquisition Strategy and use this information to develop the solicitation.]

- b. The Offeror shall describe its plan for making design and interface information available as soon as possible after it is defined or established. The Offeror shall establish and maintain a process that will provide “early and often” design disclosure directly to the Government or to third-party contractors via Government-established access, e.g., the Naval Sea Systems Command Software/Hardware Asset Reuse Enterprise (SHARE) library or through capabilities made available through the Forge.mil Program (<http://www.forge.mil/>), to in-process design documentation and computer software. Access and the ability to download this information shall be supported using industry standards. The information products available in the repository shall be easily discovered and accessed. The exchange of information shall be structured so as to protect the Offeror’s and third-party developers’ proprietary rights in the information. The Offeror shall address how it intends to resolve any comments from the Government and third-party contractors. The Offeror shall describe how it intends to provide all non-proprietary licenses, source code, drawings, repair and engineering documentation to the Government and third-party contractors at specified key events or at defined intervals.

[Note to Preparers: *Design Disclosure can be enabled through a variety of mechanisms including keeping data, code and design artifacts in a repository either maintained by or overseen by the Government. In addition, the Government can require that contractors allow the program to have continuous, real-time visibility, access and the ability to download the artifacts from the contractor’s development environment. Note: While the Government will have access to these work products, the Government cannot exercise its intellectual property rights until these items are formally delivered to and accepted by the Government. Each program has the flexibility to establish the most appropriate mechanism for its needs; with a goal of establishing a process that is both cost-effective and responsive to requests.*]

[Note to Preparers: *It is recommended that the Government use the CDRL as the basis for identifying specific TD, CS, and CSD data rights it intends to pursue. The incorporation of a Data Accession List DI-MGMT-81453A is also a best practice to require the contractor to formally identify TD, CSD, and CS that may be available for subsequent ordering by the Government (via Deferred Ordering procedures in accordance with DFARS 252.227-7027).*]

[Notes to Preparers: *If the Offeror is awarded a contract, any of the following lists can be attached to the contract if needed. If the specific list changes during negotiations then the final negotiated version shall be the one attached.*]

- c. The Data Rights and Licenses offered shall be provided as attachments to the proposal. The Offeror shall cite specific examples of the Government's IPR that illustrate the tenets of the offer, including an overview of the information provided in the following required attachments, as well as a discussion of how the information contained in the attachments impacts or illustrates the tenets of the proposal:
- d. The Offeror shall provide the following information as attachments to its offer:
 - i. Rights in Noncommercial TD, Noncommercial CS, and Noncommercial CSD.
 - a) The 7017 List. The Offeror shall attach to its offer a list identifying all noncommercial TD, CS, and CSD that it asserts should be delivered with other than unlimited rights. Specific instructions and requirements concerning this list are set forth in the DFARS 252.227-7017 "Identification and Assertion of Use, Release, or Disclosure Restrictions" (January 2011) provision incorporated at Section K of this solicitation. If the Offeror is awarded a contract, the 7017 List shall be attached to the contract. **[Note to Preparers:** *Anything not on the 7017 list should appear on the 7013 or 7014 lists. If the Offeror has not selected a performer for a portion of the SOW, the Offeror must identify the functionality of those components that would be developed or delivered by the performer (whether prime or subcontractor).*]
 - b) The 7028 List. The Offeror shall attach to its offer a list identifying all noncommercial TD, CS, and CSD that it intends to deliver with other than unlimited rights and that are identical or substantially similar to TD, CS, or CSD that the Offeror has delivered to, or is obligated to deliver to, the Government under any contract or subcontract. Specific instructions and requirements concerning this list are set forth in the DFARS 252.227-7028 "Technical Data or Computer Software Previously Delivered to the Government" (June 1995) provision incorporated at Section K of this solicitation. Additionally, if there is no

technical data or software to be identified in the 7028 list, the Offeror shall submit the list and enter “None” as the body of the list. If the Offeror is awarded a contract, the 7028 List shall be attached to the contract.

- c) Supplemental Information. The Offeror shall attach to its offer a statement, entitled “Supplemental Information— Noncommercial Technical Data, Noncommercial Computer Software, Noncommercial Computer Software Documentation” (the statement) that, for each item of noncommercial TD, CS, or CSD that the Offeror asserts should be delivered with specifically negotiated license rights or other non-standard rights (as discussed at DFARS 252.227-7013 “Rights in Technical Data – Noncommercial Items” (March 2011) and/or DFARS 252.227-7014 “Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation” (March 2011)), sets forth a complete description of all such proposed non-standard restrictions on the Government’s ability to use, modify, release, perform, display, or disclose such TD, CS, or CSD. This information may be provided by referencing any proposed non-standard license agreement that is attached to the statement. The Offeror shall submit the statement as an attachment to its offer, dated and signed by an official authorized to contractually obligate the Offeror. If no information is to be included in the statement, the Offeror need not submit the statement. If the Offeror is awarded a contract, any statement provided will be attached to the contract.
- ii. Rights in Commercial Technical Data (TD), Commercial Computer Software (CD), and Commercial Computer Software Documentation (CSD).
 - a) The Offeror shall attach to its offer a list, entitled “Commercial Technical Data, Commercial Computer Software, and Commercial Computer Software Documentation-Government Use Restrictions” (the Commercial Restrictions List), that provides the following information regarding all commercial TD, CS, and CSD that the Offeror (including its sub-Offerors or suppliers, or potential sub-Offerors or suppliers, at any tier) intends to deliver with other than unlimited rights: (1) identification of the technical data or software; (2)

basis for asserting restrictions, such as licensed products including open source software; and (3) name of the entity asserting restrictions. For any item designated as NDI, the Offeror is requested to provide details of the Agency and level therein that paid for development and the contract number(s) and dates wherein payments were received. For each entry in the list citing an asserted rights category other than the standard license rights applicable to commercial TD as set forth in the DFARS 252.227-7015 “Technical Data – Commercial Items” (March 2011) clause, the Offeror shall provide a complete description of the asserted rights, e.g., a specially negotiated license, open source software license, or any license customarily offered to the public; this information may be provided by referencing any proposed non-standard or commercial license agreement that is attached to the list, but in all cases, the non-standard or commercial license will be attached for Government review. The Offeror shall submit the Commercial Restrictions List as an attachment to its offer, dated and signed by an official authorized to contractually obligate the Offeror. If there is no information to be included in the Commercial Restrictions List, the Offeror shall submit the list and enter “None” as the body of the list. If the Offeror is awarded a contract, the Commercial Restrictions List shall be attached to the contract.

iii. Rights in Background Inventions.

- a) The Offeror shall attach to its offer a list, entitled “Background Inventions—Identification and Licensing” (the BIIL List), providing information concerning all background inventions. A “background invention” is any invention, other than a subject invention, that is covered by any patent or pending patent application in which the Offeror (including its sub-Offerors or suppliers, or potential sub-Offerors or suppliers, at any tier) (1) has any right, title, or interest; and (2) proposes to incorporate into any items, components, or processes (ICP) to be developed or delivered, or that will be described or disclosed in any TD, CS, or CSD to be developed or delivered, under the resulting contract. For each background invention, the BIIL List shall identify (1) the invention, by serial number, title, and date of the patent

application or issued patent; (2) the ICP, TD, CS, and CSD that will incorporate or disclose the invention; and (3) the nature of the Offeror's right, title, or interest in the invention. The Offeror shall submit the BIIL List as an attachment to its offer, dated and signed by an official authorized to contractually obligate the Offeror. If there is no information to be included in the BIIL List, the Offeror shall submit the list and enter "None" as the body of the list. If the Offeror is awarded a contract, the BIIL List shall be attached to the contract.

- b) The Offeror shall attach to its offer a list, entitled "Third-Party Patent Rights – Identification and Licensing" (the 3PRIL List), providing information concerning all third-party patent rights for which it intends to pay royalties and the amount of the royalties in order to perform under the contract. The Offeror shall submit the 3PRIL List as an attachment to its offer, dated and signed by an official authorized to contractually obligate the Offeror. If there is no information to be included in the 3PRIL List, the Offeror shall submit the list and enter "None" as the body of the list. If the Offeror is awarded a contract, the 3PRIL List shall be attached to the contract.

[Note to Preparers: See FAR Clause 52.227-6 for specific guidance on Royalties. This language must be included if a third-party patent is included in the solution.]

5. Factor: OSA Past Performance

- a. The Offeror shall demonstrate, through its use of previously developed similar technologies, the Offeror's ability to meet the design, development, testing, and production requirements of this solicitation, in particular its approach to a modular open system design, in the quantities and schedules specified. The Offeror shall provide a list of all relevant contracts and subcontracts of similar work scope or technical complexity to the efforts described herein within the last five (5) years. **[Note to Preparers:** Past performance is in all solicitations (FAR 15.304) unless specifically excluded and documented by the Contracting Officer.]

[Note to Preparers: Offerors should be encouraged to clearly demonstrate, through their use of similar technologies previously developed, the ability to meet the design, development, testing, and production requirements of the solicitation, in particular its

approach to a modular open system design, in the quantities and schedules specified in the RFP.]

In addition to contracts and subcontracts performed by the Offeror, relevant contracts and subcontracts of an acquired company, division, or subsidiary shall be identified. The Offeror shall place particular emphasis on DoD or Government contracts and subcontracts, especially those that involved a modular open systems approach.

If the Offeror did not perform [**Note to Preparers:** *describe the type of project here, e.g., “submarine combat control”*] projects during the last five years, the Offeror may discuss other related projects that demonstrate the Offeror’s capabilities to perform work of similar nature and magnitude. Note, if the Offeror omits projects or contracts of which the Government evaluation team is aware or becomes aware, then customer assessments may be sought from the relevant program and technical support offices. Offerors are advised that (1) the Government may contact any or all references listed in the proposal and other third parties, unreferenced customers, agencies, Offerors, consumer protection organizations, etc., for performance information, or use any other data available (such as contractor Performance Assessment Reporting System (CPARS)); (2) the Government reserves the right to use any such information received as part of its evaluation of the Offeror’s past performance; and (3) if the Offeror omits projects of which the Government evaluation team is aware or becomes aware, customer assessments may be sought from the relevant organizations.

For each listed contract, the Offeror shall prepare a synopsis that includes a narrative self-assessment of the contract and specific details describing why the contract was, or was not, successful. Each synopsis shall be in the following format:

- i. Contract number;
- ii. Customer’s name, address, telephone number, and a point of contact (whether Government or Commercial), and whether the Offeror was the prime Offeror or a sub-Offeror;
- iii. Contract type;
- iv. Cost information;
- v. Brief product description, including quantities, hours, and state of acquisition (i.e., development or production);

- vi. Self-Assessment. The Offeror shall provide a self-assessment of its performance under each contract identified above. The self-assessment shall address the following: (a) the degree to which the Offeror demonstrated its design approach, plans for technology insertion, and sustainment strategy were consistent with the modular open systems requirements, (b) 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, (c) 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, and (d) 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 (COTS or reusable) evolve. Cost growth, material problems, manufacturing problems, quality problems, labor problems, facility problems, and delivery delays shall be disclosed and fully explained. The Offeror shall demonstrate how it was able to resolve (or why it could not resolve) special or unexplained problems as well as difficulties in meeting delivery schedule, performance, or cost parameters. Emphasis shall be placed on the Offeror's ability to solve problems associated with critical testing, quality control, and production. Furthermore, the Offeror shall indicate any quality awards or recognition received.
- vii. Customer References. The Offeror shall request Customer questionnaires to be submitted directly to the Procurement Contracting Officer's (PCO's) representative and/or copies submitted with the Offeror's proposal and provide the following information for each described contract:
- a) The Procuring Contracting Officer's name, address, and telephone number.
 - b) The Administrative Contracting Officer's name, address, and telephone number.
 - c) The Government and Offeror's Program Managers' names, addresses, and telephone numbers.
 - d) The names, addresses, and telephone numbers of other individuals having knowledge of the Offeror's performance under each contract.

- b. **[Note to Preparers:** At a minimum, the Government’s questionnaire for assessing an Offeror’s OSA past performance must address the following:]
- i. The degree to which the Offeror demonstrated its design approach, plans for technology insertion, and sustainment strategy were consistent with the modular open systems requirements.
 - ii. 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.
 - iii. 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.
 - iv. 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 (COTS or reusable) evolve.

6. Factor: Cost Proposal (OSA Related)

- a. Supplemental Information Concerning Cost/Price of Noncommercial Technical Data (TD), Noncommercial Computer Software (CS), and Noncommercial Computer Software Documentation (CSD)
- i. **Cost/Price Information.** In addition to the submission requirement of DFARS 252.227-7017, the Offeror shall provide a list entitled “Supplemental Information Concerning Cost/Price of Noncommercial Technical Data (TD), Noncommercial Computer Software (CS), and Noncommercial Computer Software Documentation (CSD)” (hereinafter the Supplemental 7017 Cost/Price List). This list shall be provided as an attachment to proposal. This list shall provide supplemental information concerning the noncommercial TD, CS, or CSD identified in the DFARS 252.227-7017 “Identification and Assertion of Use, Release, or Disclosure Restriction” list (hereinafter 7017 List), as follows:
 - a) License Option Price Information. For each item of noncommercial TD, CS, and/or CSD that the Offeror asserts should be delivered with less than Government Purpose Rights (GPR) (as defined in (DFARS 252.227-

7013 “Rights in Technical Data – Noncommercial Items” (March 2011) and/or DFARS 252.227-7014 “Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation” (March 2011))³⁸, and for which the Offeror is willing to sell to the Government greater rights than those identified in the 7017 List, the Offeror shall identify those greater rights, provide an option price at which the Government may purchase such greater rights, and identify the period of time during which the option is available for the Government to exercise. **[Note to Preparers: Evaluation of options should be addressed in Sections B and M of the RFP.]**

- b) **Government Preferences.** The Offeror may state any license option price as a firm fixed price, a percentage royalty rate (or use fee), or any other comparable compensation scheme, provided that the Government can reasonably calculate a sum-certain price for the license option using the price information and terms and conditions information the Offeror provided. The Government prefers that any license option prices the Offeror provides in the Supplemental 7017 Cost/Price List cover all noncommercial CS, noncommercial CSD, and noncommercial TD included in any affected software and that the Offeror states license option prices on a price-per-system basis.

[Note to Preparers: Recommend the inclusion of FAR 52.227-6 ROYALTY INFORMATION (APR1984) when applicable to the solicitation.]

- ii. **Duty to Submit Negative List.** If there is no supplemental information to be submitted in the Supplemental 7017 Cost/Price List, the Offeror shall submit the list and enter “None” as the body of the list. Failure to provide a list may render the Offeror ineligible for award.
- iii. **Use During Source Selection.** Information provided in the Supplemental 7017 Cost/Price List, as well as the information provided in the 7017 List, may be used in the source selection process as part of the Government’s best value analysis to

³⁸ The March 2011 dates are correct in both instances; however, they will be changing again soon as the litigation support contractor rule is incorporated.

evaluate the impact on the Government's ability to use, reuse, or disclose the TD, CS, and/or CSD for government purposes.

7. Factor: Supplemental Information Concerning Cost/Price of Commercial Computer Software (CS), and Commercial Computer Software Documentation (CSD) and Commercial Technical Data (TD)

- a. **Cost/Price Information.** The Offeror shall provide a list to the Government, entitled "Commercial Restrictions List – Cost/Price Information" (hereinafter the CRLCPI List). This list shall be provided as an attachment to proposal. The CRLCPI List shall state a license option price for all commercial CS, commercial CSD, and commercial TD on the CRL List for which the Offeror is willing to provide the Government with greater license rights than the level of rights to which the Government would otherwise be entitled. If the Offeror is willing to provide a license option, the Offeror shall identify the specific rights it is willing to grant, and the period of time during which the option is available for the Government to exercise.

[Note to Preparers: *It is incumbent upon the Program Manager and Contracting Officer to fully understand the terms of the license including the specific rights and limitations (if any) proposed by the Offeror. Open Source Software licenses may or may not have associated costs, but will have specific terms with which the Government must comply. Another option is to negotiate a modified Open Source Software License that best reflects the OSA concepts necessary to implement the contract requirements. Recommend license agreements should be included in Section J of the Contract. Recommend consulting with the appropriate Legal Counsel. See Appendix 5 for additional details.]*

- b. **License Option Pricing:** Government Preferences. The Offeror may state any license option price as a firm fixed price, a percentage royalty rate (or use rate), or any other comparable compensation scheme, provided that the Government can reasonably calculate a sum-certain price for the license option using the price information the Offeror provided. The Government prefers that any license option prices the Offeror provides in the CRLCPI List cover all commercial CS, commercial CSD, and commercial TD included in any affected software and that the Offeror states

any license option prices on a price-per-system basis. [**Note to Preparers:** *Evaluation of options should be addressed in Sections B and M of the RFP.*]

- c. **Duty to Submit Negative List.** If the Offeror has no Option License Pricing to provide in the CRLCPI List, the Offeror shall still submit the CRLCPI List and enter “None” in the body of the List. Failure to provide a list may render the Offeror ineligible for award.

8. Factor: Supplemental Information Concerning Cost/Price of Background Inventions

[**Note to Preparers:** *Programs should investigate whether the Government has funded the development of inventions that an Offeror is proposing to use. If the Government has provided funding, Programs should be prepared to secure the appropriate license rights.*]

- a. **License Option Pricing: Government Preferences.** The Offeror may state any license option price as a firm fixed price, a percentage royalty rate (or use rate), or any other comparable compensation scheme, provided the Government can reasonably calculate a sum-certain price for the license using the price information provided by the Offeror. The Government prefers that any license option prices stated by the Offeror in the Background Inventions List – Cost/Price Information (BICPI List) cover all background inventions included in any affected software, and the Offeror states license option prices on a price-per-system basis.
- b. **Duty to Submit Negative List.** If the Offeror has no Option License Pricing to provide in the BICPI List, the Offeror shall still submit the BICPI List and enter “None” in the body of the list. Failure to provide a list may render the Offeror ineligible for award.

9. Factor: Software (Acquisition) Process Improvement Initiative Guidance³⁹

There are many parallel and related efforts underway with the Department of Defense that address improvement in the acquisition of

³⁹ Assistant Secretary of the Navy (Research, Development and Acquisition)’s Memorandum on *Software Process Improvement Initiative Contract Language*, dated November 17, 2006.

software products: mandates such as Public Law 107-314 Section 804 and the Clinger-Cohen Act; initiatives such as Software Assurance and Open Architecture (OA); and the development of best practice models such as the Capability Maturity Model Integration (CMMI) for Acquisition.⁴⁰

The Government shall request that Offerors submit a draft version of their Software Development Plan (SDP) as a part of their proposal package as well as a rationale justifying the Government's selection of their process. Recommended language:

- a. As a part of the proposal, Offerors shall submit a draft version of their SDP in accordance with the content defined in the SOW. The SDP may be formatted as desired by the Offeror but must contain the information described by the SDP DID. The SDP is not page limited. An SDP, if it is to-the-point and appropriate, may be preferable to a SDP that is excessively wordy and contains non-essential material.
- b. Offerors shall also submit, as a part of their proposal, an 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.
- c. 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.
- d. 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.

⁴⁰ Assistant Secretary of the Navy (Research, Development and Acquisition)'s Memorandum on *Software Process Improvement Initiative*, dated May 15, 2006.

Chapter V: RECOMMENDATIONS FOR SECTION M EVALUATION FACTORS FOR AWARD

[Note to Preparers: *This section contains only recommended guidance, and is offered with the understanding that individual PEOs and Program Managers can be flexible in selecting and weighting those items needed to meet their needs. Programs should not feel that they need to address all of the items contained in these recommendations.]*

[Note to Preparers: *The following is an extensive list of factors and subfactors that can be tailored and incorporated into Section M. Programs can delete the items they feel are redundant or not important for their specific acquisition requirements. Preparers need to include the factors and subfactors that will be determinant in the selection process and delete the factors and subfactors that are of minor or no importance. In particular, Programs should be aware of asking for the same information in multiple places – the decision to do so should be deliberate and the evaluation of Offeror’s response done carefully evaluated in a consistent manner.]*

Although the *Guidebook* was developed for mixed systems comprised of hardware, middleware and software elements, the recommended language can be easily tailored to reflect hardware- or software-only acquisitions.

EVALUATION FACTORS

[Note to Preparers: *There is additional guidance to DoD acquisition managers intended to provide improved visibility into Offeror’s and contractor’s software development processes to ensure there are well-documented, effective software processes and continuous process improvement practices in place during contract performance. The guidance and requirements are contained in Service-specific implementation guides and instructions. See the Introduction for additional details.]*

[Note to Preparers: *It is recommended that the following factors be ordered from the most heavily weighted to the least (descending order of importance) with a note to that effect in this paragraph. Program Managers are encouraged to prioritize these to meet the objectives of their programs.]*

The Government will evaluate the Offeror’s proposal in accordance with the factors and subfactors set forth below:

Open Systems Architecture Guidance

1. Factor: Technical Approach and Processes

The Government will evaluate the Offeror's ability to demonstrate a thorough understanding of the complete range of tasks in the RFP and implementation of OSA Technical Approaches and Processes the Government will evaluate the Offeror's:

- a. Approach for accomplishing the tasks set forth in the Statement of Work
- b. Ability to overcome the technical challenges with must be addressed to fulfill the [*Program Name*] requirements
- c. Solutions for clarity, completeness, and feasibility
- d. Approach to seamlessly provide the services and capabilities described in accordance with [insert Agency/organizational standards, policies and processes as applicable]
- e. The Government will use information provided in the proposal to assess the Offeror's ability to execute:

Subfactor 1. Open Systems Approach and Goals

The Government will evaluate the extent to which the Offeror's open system architecture approach incorporates hardware and software open system architecture design requirements, as documented in the Offeror's Open Systems Management Plan (OSMP), is thorough, complete, adequate, feasible, and represents an understanding of the RFP requirements.

Subfactor 2. Interface Design and Management

The Government will evaluate the extent to which the Offeror's open system architecture approach, as documented in the Offeror's Open Systems Management Plan (OSMP), clearly defines and describes all component and system interfaces; defines and documents all subsystem and configuration item (CI) level interfaces to provide full functional, logical, and physical specifications; 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 identifies the interface and data exchange standards between the component, module or system and the interconnectivity or underlying information exchange medium.

Subfactor 3. Treatment of Proprietary or Vendor-Unique Elements

The Government will evaluate the extent to which the Offeror's Life Cycle Management and Open Systems Strategy, as documented in the Offeror's Open Systems Management Plan

(OSMP), explains the use of proprietary, vendor-unique or closed components or interfaces; defines its process for identifying and justifying use of proprietary, vendor-unique or closed interfaces, code modules, hardware, firmware, or software; and demonstrates to the Government that proprietary elements do not preclude or hinder other component or module developers from interfacing with or otherwise developing, replacing, or upgrading open parts of the system.

Subfactor 4. Life Cycle Management and Open Systems

The Government will evaluate the extent to which the Offeror's Life Cycle Management and Open Systems Strategy, both of which should be documented in the Offeror's Open Systems Management Plan (OSMP), demonstrates a thorough, adequate, and feasible, strategy for the insertion of COTS technologies and other reusable NDI into the SYSTEM NAME and demonstrates that COTS, other reusable NDI, and other components can be logistically supported throughout the system's life cycle.

2. Factor: System Compliance with OSA Guidance

In evaluating the System Compliance with OSA Guidance, the Government will use information in the proposal to assess the degree to which the Offeror's approach complies with PEO-specified (or Service Enterprise) Technical Guidance Points as identified in Table A of Section L.

3. 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 Integrated Product Teams (IPT) to improve processes, manage risk, and increase efficiency. The Government will also assess the metrics approach proposed to measure OSA performance and reuse efficiency.

4. Factor: Data Rights, Computer Software Rights and Patent Rights

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.

5. Factor: Data, Software and Patent Rights

The Government will evaluate Data, Software and Patent Rights using 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 [SYSTEM NAME] TD, CSD and CS to other systems or platforms.

Proposals will not be rated as less than ACCEPTABLE on this factor solely because an Offeror does not offer a price for the Government Purpose Rights Option CLIN. However, ratings on this factor for proposals to deliver TD, CSD, or SW with less than the minimum rights specified for the Government by applicable statute (10 U.S.C. 2320) and regulation (DFARS 252.227-7013, 252.227-7014, and 252.227-7015) may be negatively impacted. For noncommercial acquisitions, these rights include: Unlimited Rights in TD (as specified in DFARS 252.227-7013(b)(1)) and CS and CSD (as specified in DFARS 252.227-7014(b)(1)); Limited Rights in TD (as specified in DFARS 252.227-7013(b)(3)); and Restricted Rights in CS (as specified in DFARS 252.227-7014(b)(3)). The minimum rights considered for TD associated with commercial item acquisitions are specified in DFARS 252.227-7015(b)(1). For commercial SW acquisitions, evaluation of the offered rights will assess their consistency with Federal procurement law and satisfaction of Government user needs in accordance with the policy in DFARS 227.7202-1(a).

Ratings on this factor for proposals to deliver TD, CSD, or SW with more than the minimum rights specified for the Government by applicable statute and regulation may be positively impacted.

[Note to Preparers: *Program Managers should seek to encourage Offerors to reuse components and sub-components where cost-effective or when overall system performance will be enhanced, accelerated*

delivery schedules supported, or system development risks reduced. Reuse should be supported by an appropriate business case.]

6. Factor: Reuse of Existing Components, Sub-components or Software

In evaluating the Offeror's proposal, the Government will assess the extent that the proposed solution reuses existing, proven components, subcomponents and COTS in a cost-effective manner. The Offeror should quantify the cost savings and schedule impacts associated with reuse of existing components. The Government values cost-effective reuse of products that have already been developed by the Government or by Contractors using Government funding (and where the Government has at least Government Purpose Rights). Other candidates for reuse include commercially available products that offer proven system performance or cost advantages over potential newly developed products. Offers that maximize reuse of proven components are more likely to reduce project cost and schedule and performance risks. Proposals demonstrating cost-effective reuse of products that have already been developed by the Government or cost-attractive commercial products that have been previously accepted by the Government and that have been validated and verified by DoD Information Assurance Certification and Accreditation Process (DIACAP) as meeting all Information Assurance requirements already will receive a more favorable rating. Proof of reuse will be based on evidence presented in the response showing how those modules will be incorporated into the system architecture. Additional information should be provided on the evaluation of prospective components and subcomponents, including how existing components were found in Government libraries/sites like DISA's Forge.mil, Navy's SHARE, the Navy PEO C4I's NESI, etc.

[Note to Preparers: *Program Managers should include a subfactor for evaluating the completeness and adequacy of the delivered data. See "Intellectual Property Rights and Data Rights" discussion in Chapter I. Program Managers should consider evaluation of the data rights packages offered as part of best value determinations. An Offeror who proposes only those rights required by statute and states their intention to provide technical data developed exclusively at private expense with limited rights cannot be rated "Unacceptable". Those who offer more favorable data rights packages can be positively rewarded by being graded with adjectival ratings such as "Good", "Excellent", and "Superior." Offering the rights to which the Government is statutorily entitled should result in an "Acceptable" technical data rights*

evaluation score -- offering less than the rights statutorily entitled would result in an "Unacceptable" rating.]

7. Factor: Past Performance

[Note to Preparers: *The following are only suggested OSA-specific past performance evaluation criteria. Other past performance criteria should be added as appropriate as additional subfactors.]*

Subfactor 1. Offeror's OSA Past Performance

- i. In assessing the Offeror's past performance submissions on similar contracts, the Government will consider how well the Offeror implemented Open System Architecture principles and used a modular open system approach, including: 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.⁴¹
- ii. The Offeror's previous experience in developing software of the same nature as that being acquired with this solicitation.
- iii. 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 evaluated.
- iv. 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.
- v. 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.
- vi. 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.
- vii. The degree to which the Offeror's approach contains capabilities to easily and quickly update, revise, and change

⁴¹ Potential criteria can be found in IEEE/EIA Std. 12207.1, Section 4.2.3, H.3 - Characteristics of Life Cycle Data.

the system as threats (warfighting and information assurance threats) or technologies (COTS or reusable) evolve.

8. Factor: Cost Proposal (OSA Related)

The Government will evaluate the following costs with respect to how they further Open System Architecture goals:

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

[Note to Preparers: *For ACAT I and ACAT II programs, 10 U.S.C. Section 2320(e), as implemented in DODI 5000.02 and DFARS 207.106 (S-70) for software as well, requires that Program Managers assess the long-term data needs of such systems and subsystems and establish corresponding acquisition strategies that provide for data rights needed to sustain such systems and subsystems over their life cycle. Such strategies may include the development of maintenance capabilities within the Department of Defense or conducting competitions for contracts for sustainment of such systems or subsystems. Assessments and corresponding acquisition strategies developed under this section with respect to a weapon system or subsystem shall address the merits of including a priced contract option for the future delivery of technical data, computer software, and associated license rights that were not acquired upon initial contract award. As previously mentioned, assessment of data needs is a sound practice for all acquisition programs.*

These assessment/acquisition strategy requirements can be particularly important for FAR Part 12 procurements where the Offeror is not required to provide certified cost or pricing data for TD/CS, or in non-commercial “stovepipe” systems where the incumbent contractor has cost and pricing data for its TD/CS, but offers an cost-prohibitive option price for GPR or other competitive data rights to its TD/CS, typically because there is no competition. In these cases, Program Managers may want to use their own third-party IP valuation analyst (either Government or contractor) to verify an Offeror’s/Contractor’s

valuation of intellectual property when the Government is assessing whether it should acquire Government Purpose Rights or other special license rights that permit competitive uses. Alternatively, Program Managers may want to consider adding RFP language that requires Offerors to have a qualified third-party valuation analyst experienced in IP valuations value the TD/CS, using a valuation method that is generally accepted by the IP valuation industry. The decision to proceed with this type of assessment should be taken after weighing the potential reduction in fees against the cost of retaining the IP valuation services. The National Association of Certified Valuators and Analysts (NACVA) (<http://www.nacva.com/>) is one source of information regarding certification of IP valuation analysts and standard valuation industry approaches. Services of suitable third-party vendors may be obtained from sources such as GSA Schedules and other vehicles.]

Chapter VI: RECOMMENDATIONS FOR INCENTIVIZING CONTRACTORS

Incentivizing cost management, collaboration with associate contractors, technical excellence, and schedule performance in the program encourage exceptional contractor performance through the adoption of and adherence to OSA business and technical principles. Incentive mechanisms must be based on the requirements described in the contract. The most effective criteria are objective in nature, though some subjective measures can be effective.

Most sophisticated weapons systems development programs deal with maturing designs and challenging integration problems. As a result, the government often will and should provide technical guidance and make tradeoff decisions during development. In EMD, the Government will work closely with the prime contractor to achieve the best outcome. While it is possible to negotiate changes in a fixed-price contract environment, the nature of development is such that informed decisions need to be made quickly and in close cooperation with industry.

Therefore, when performing new product development, as is often the case for creating open systems architecture products, cost contracts with incentive mechanisms are appropriate for new product development:

- Cost Plus Incentive Fee (CPIF) for constant work that is spread out over the duration of the contract (e.g. 3 years), such as sustainment and upgrading of delivered capability; Similarly incentive fee type contracts can be used to manage cost and schedule adherence for the full duration of the contract vehicle. This type of incentive can be very effective when managing total cost over a specified period of time.
- Cost Plus Award Fee (CPAF) for engineering development of large scale open systems where the volume of effort varies over the contract period (e.g. 5 years) and technical risk needs to be managed across specific milestones. Award fee determinations can help motivate the completion of development tasks or to focus contractor attention on high risk activities early in the development cycle, by establishing measurable development milestones such as entrance criteria for technical reviews or achieving scheduled deliveries against

published development time frames. The use of this type of incentive strategy increases the likelihood of on-time and on-cost completion through financial rewards.

- Cost Plus Award Term (CPAT) for integration contracts for bringing together multiple products from an array of third parties over a longer period of time (up to 10 years) and motivation of industry investment is mutually beneficial. Award term contracts should be used only where long-term incumbency is valuable to the Government. An appropriate business model should be developed where both parties benefit from corporate investment to establish specific long-term activities that require stability and commitment. Integration and depot repair services are examples. For integration services, the Government derives value from the integration of new capabilities developed by other contractors and the integrator is made responsible for ensuring 1) that the full product performs as required and 2) that technical and business environments are open and accessible for bringing third-party innovations into the final product. For depot repair, investment in infrastructure, tooling, processes, etc. are barriers to entry for competition, but long-term business stability can provide motivation to invest and the Government benefits through competitively reducing overall repair and sustainment costs over the long-term. In all cases, the Government shall capture the deliverables and enforce data rights to provide for periodic competition, even if that periodicity could be as long as ten years. Long-term relationships can benefit from the structure provided in CPATs so long as service continues to be satisfactory and metrics are defined and adhered to as the basis for awarding additional terms.

Whenever possible, development contracts should be separated from production activities. Prototypes or EDM systems should transition to Production or LRIP on separate contracts, preferably competitively awarded, and as early as possible. The adherence to OSA practices, especially using the right set of deliverables (such as the ones prescribed in this Guidebook) and assertion of data rights, greatly reduces the risk for handing off the work from a development contract to a production contract, even if the production contract is executed by a company different than the company that did the development.

The use of Fixed-Price Incentive Firm (FPIF) and Firm Fixed Price contracts in development and production is only appropriate for

activities like early or low rate production as long as the following conditions can be met:

- **Firm requirements:** Cost vs. performance trades are essentially complete. There is a very clear understanding of what the contractor should build, and that the Government is confident that the conditions exist to permit the design of an affordable product that the user will be able to afford and is committed to acquiring.
- **Low technical risk:** Design content is established and the components are mature technologies. There are no significant unresolved design issues, no major integration risk, the external interfaces are well defined, and no serious risk exists of unknowns surfacing in developmental testing and causing major redesign.
- **Qualified suppliers:** Bidders will be firms that have experience with this kind of product and can be expected to bid rationally and perform to plan.
- **Financial capacity to absorb overruns:** An additional consideration would be to select contractors that have the capacity to continue and deliver the product despite potential overruns that may not have been foreseeable.
- **Motivation to continue:** If development milestones are breached, there is still a business case for some financial return such that it is unlikely that large losses will be incurred by the contractor.⁴²

Early or low-rate production have similar considerations, but here is where greater use of FPI contract vehicles makes the most sense as an alternative to cost-plus vehicles. Unlike an FFP contract, there needs to be a fair sharing of the risk—and the rewards—of performance.

Fixed-price vehicle for early production should only be used when:

- Firm requirements (as explained)
- Design proven through developmental testing
- Established manufacturing processes
- Qualified suppliers
- Suppliers with the resources to absorb some degree of overrun
- Adequate business case for suppliers to continue work if they get in trouble.

⁴²*Use of Fixed-Price Incentive Firm (FPIF) Contracts in Development and Production*, Kendall, Defense AT&L magazine, March-April 2013

The above apply to FPIF procurements for which proposals are solicited at or near the end of EMD after Critical Design Review, built production representative prototypes, and completed some significant fraction of developmental test (DT).⁴³

Although this *Guidebook* was developed for mixed systems comprised of hardware, middleware and software elements, these recommendations can be easily tailored to reflect hardware- or software-only acquisitions.

This chapter is intended to serve as a guide for those programs seeking to incentivize their contractors to implement OSA business and technical principles in both development and production contracts. Programs should attempt to link awards to outcomes wherever possible – moving from rewarding compliance with technical or process requirements towards achievements of desirable outcome.

Better Buying Power 2.0 will be developing and deploying more detailed guidance on the use of contract incentives.

⁴³ Much of the above content *Use of Fixed-Price Incentive Firm (FPIF) Contracts in Development and Production*. Kendall. March-April 2013.

Appendix Table of Contents

Appendix 1: RECOMMENDED CDRL AND DELIVERABLE ITEMS	83
Appendix 2: OSA CHECKLIST (short)	97
Appendix 3: OSA CHECKLIST (long)	101
Appendix 4: RECOMMENDED DATA LANGUAGE FOR CODE HEADERS	107
Appendix 5: OPEN SOURCE SOFTWARE	113
Appendix 6: GLOSSARY OF TERMS	129
Appendix 7: ASSESSING A PROGRAM'S INTELLECTUAL PROPERTY RIGHTS NEEDS AND DEVELOPING A TECHNICAL DATA RIGHTS STRATEGY (TDRS)	147
Appendix 8: CLICKWRAP OR EMBEDDED LICENSE ISSUES ..	157
Appendix 9: BETTER BUYING POWER: UNDERSTANDING AND LEVERAGING DATA RIGHTS IN DOD ACQUISITIONS	161
Appendix 10: BREAKING AND AVOIDING VENDOR LOCK	167
Appendix 11: SAMPLE CONTRACT DATA REQUIREMENTS LISTS (CDRLs)	177

Appendix 1: RECOMMENDED CDRL AND DELIVERABLE ITEMS

The following are examples of Contract Data Requirements Lists (CDRLs) and deliverable items, as directed by the Statement of Work, which support OSA and can be incorporated into contracts. This is not intended to be an exhaustive list of all potential deliverable items, but is an attempt to list only those deliverables we believe significantly support Open Systems Architecture, and can be augmented/reduced as the Program Manager believes is appropriate. The frequency and delivery dates of the deliverables must be specified, along with a list of deliverable recipients.

[Note to Preparer: *The program plan and directive documentation should specify that anything the government paid to develop is available for delivery to the Government with all of the developmental artifacts and unlimited usage rights. In addition, the program should require that the deliverables be provided (or deposited) in the appropriate repository (if established) such as the Navy's SHARE Repository or those made available through the DoD's Forge.mil Program (<http://www.forge.mil/>).]*

[Note to Preparers: *To help clearly understand the data rights to be provided to the Government, the Government recommends that a table listing all the CDRLs be inserted as an attachment to the proposal which includes a column wherein the Offeror states the data rights to be provided with that CDRL when delivered. As defined in Section L, Subfactor 1(b) on p. 45.]*

[Note to Preparers: *Software should be delivered in a standalone fashion, i.e., not encumbered by any particular configuration management tool. Future sites/locations/programs that ultimately will use the software or artifacts should have the ability to use whatever configuration management tool they desire without any overt or hidden dependencies on a given tool.]*

[Note to Preparers: *When citing regulations such as the DFARS and FAR, dates are included where possible to reflect the most recent version of this Guidebook. However, Contracting Officers and PMs need to check for current clause dates before using the language in this Guidebook.]*

1. Deferred Ordering of Technical Data or Computer Software (Including Design and Development Artifacts)

[Note to Preparer: *There may be instances where the Government would like to have access and the ability to download design artifacts*

and other materials that are produced during the development of software but which have not been specifically identified in the CDRLs and Data Item Descriptions (DIDs). These materials may be located in an Integrated Digital Design Environment (IDE). If the Government anticipates that it may need to require delivery of any such items in the future, it should use priced contract option CLINs for such potential delivery needs. In addition, it is recommended that the Program Manager use DFARS 252.227-7027, regarding deferred ordering of technical data, to obtain these materials. Reference to DFARS 252.227-7027, like reference to other FAR and DFARS clauses, should be included in Section I of the contract.]

a. DFARS 227.7103-8(b) Deferred Delivery and Deferred Ordering of Technical Data

Deferred Ordering. Use the clause at 252.227-7027, Deferred Ordering of Technical Data or Computer Software, when a firm requirement for a particular data item(s) has not been established prior to contract award but there is a potential need for the data. Under this clause, the contracting officer may order any data that has been generated in the performance of the contract or any subcontract thereunder at any time until three years after acceptance of all items (other than technical data or computer software) under the contract or contract termination, whichever is later. The obligation of subcontractors to deliver such data expires three years after the date the contractor accepts the last item under the subcontract. When the data are ordered, the delivery dates shall be negotiated and the contractor compensated only for converting the data into the prescribed form, reproduction costs, and delivery costs.

The software development process to be used by the winning contractor team is to be defined and documented in the developer's SDP which shall be designated as a CDRL. Contractor teams are to submit an initial delivery of the SDP with the proposal. After contract award, an updated version is to be delivered based on discussion and negotiations with the Government regarding approval of SDP content.

Specifically, the SDP should:

- i. Document all processes applicable to the system to be acquired, including the Primary, Supporting, and Organizational life cycle processes as defined by IEEE/EIA Std. 12207 as appropriate.
- ii. Contain the content defined by all information items listed in Table 1 of IEEE/EIA Std. 12207.1, as appropriate for the

system and be consistent with the processes proposed by the developers. If any information item is not relevant to either the system or to the proposed process, that item need not be required.

- iii. Adhere to the characteristics defined in section 4.2.3 of IEEE/EIA Std. 12207, as appropriate.
- iv. Contain information at a detail sufficient to allow the use of the SDP as the full guidance for the developers. In accordance with section 6.5.3a of IEEE/EIA Std. 12207.1, it should contain, “specific standards, methods, tools, actions, reuse strategy, and responsibility associated with the development and qualification of all requirements, including safety and security.”

b. Open System Architecture Products

It is recommended that the Program Office perform an assessment of its Intellectual Property Rights needs (See Appendix 7 to this Guidebook) and craft its CDRL and Deliverable requirements accordingly. If the Program Office, PEO, Domain or Sponsor believes that the program deliverables would be of such interest that they warrant inclusion in the appropriate repository (such as the Navy’s SHARE or those provided under the Forge.mil Program (<http://www.forge.mil/>)) then the CDRL and deliverables should include those design, developmental, or diagnostic items needed to reproduce or recreate the asset.

The ideal asset would have artifacts in most or all of the following categories. The key to obtaining these artifacts is to require that they be delivered as part of the terms of the contract. In order to facilitate reuse of these artifacts, these items must be delivered with the appropriate data or license rights, e.g., Government Purpose Rights (GPR) or suitable special license rights. In order to facilitate reuse, the asset should bundle the following or their equivalent:

- i. Requirements (e.g., Word documents, DOORS file or Excel or XML export or other file endings that apply.)
- ii. Architecture models (e.g., System Architect files, including Department of Defense Architecture Framework (DoDAF) views where required or other file endings that apply.)
- iii. Functional models (e.g., CORE file in native format or XML export) Software models (e.g., Rose/Rhapsody/iUML (Unified Modeling Language)/Artisan models in native or XMI format; minimum diagrams Class and State or Interaction/Sequence or other file endings that apply.)

- iv. Hardware models (e.g., CAD DXF, IEGS files or other file endings that apply.)
- v. Human systems engineering models (e.g., IPME or Envision Ergo files or other file endings that apply.)
- vi. Cost models (e.g., PRICE, SEER, COMET, VAMOSOC, Excel files or other file endings that apply.)
- vii. Modeling and Simulation data (e.g., NETWARS/OPNET, NSS, GCAM -scenarios, environmental, platforms, tactics, MOEs, MOPs in XMI format following JC3IEDM or XMSF standards or other file endings that apply.)
- viii. Test plans and results (e.g., QA Run, Quality Center files or Word or Excel export or other file endings that apply.)
- ix. Logistics data (e.g., COMPASS, CASA, PowerLOG in native or XML/CSV format or other file endings that apply.)

c. Recommended OSA CDRL and Deliverable Items

The following recommended deliverables for open architecture systems have official Deliverable Item Descriptions (DIDs) accepted by the Department of Defense's Defense Standardization Program. The official DIDs are available from the Document Automation and Production Service (DAPS) Acquisition Streamlining and Standardization Information System (ASSIST) database at <http://assist.daps.dla.mil>. To obtain these DIDs simply search the database using either the DID's title or its ID number listed below in the brief descriptions.

[Note to Preparers: *Program Managers should use their business judgment and a business case analysis in defining the deliverables that will be specified. Generally, programs should identify those items they believe would be necessary for a third-party vendor to be able to replace a system component and successfully integrate it within the overall system. Larger programs (e.g., ACAT I and II programs) should consider their overall sustainability strategy and be more expansive when identifying deliverables. At a minimum, the items annotated with an asterisk (*) should be strongly considered for inclusion.*]

- i. Software Development Plan (SDP): The SDP describes a developer's plans for conducting a software development effort. The term "software development" is meant to include new development, modification, reuse, reengineering, maintenance, and all other activities resulting in software products. [DID ID: DI-IPSC-81427A]
- ii. * Software Requirements Specification (SRS): The SRS specifies the requirements for a Computer Software

Configuration Item (CSCI) and the methods to be used to ensure that each requirement has been met. Requirements pertaining to the CSCI's external interfaces may be presented in the SRS or in one or more Interface Requirements Specifications (IRSs) (DI-IPSC-81434A) referenced from the SRS [DID ID: DI-IPSC-81433A]. It has also been defined as a complete description of the behavior of the software to be developed. It includes a set of use cases that describe all of the interactions that the users will have with the software. It also contains functional requirements, which define the internal workings of the software: that is, the calculations, technical details, data manipulation and processing, and other specific functionality that shows how the use cases are to be satisfied. It also contains nonfunctional requirements, which impose constraints on the design or implementation (such as performance requirements, quality standards or design constraints). [Stellman & Greene Consulting; <http://www.stellman-greene.com>] [**Note to Preparers:** *For many programs, it is not necessary for the SRS to describe the internal workings of the software unless it is part of implementation (design) constraints. The main purpose of the SRS is to define desired externally-visible behavior.*]

- iii. * Software Version Description (SVD): The Software Version Description (SVD) identifies and describes a software version consisting of one or more Computer Software Configuration Items (CSCIs). It is used to release, track, and control software versions. [DID ID: DI-IPSC-81442A]
- iv. * Software Product Specification (SPS): The SPS contains or references the executable software, source files, and software support information, including "as built" design information and compilation, build, and modification procedures, for a Computer Software Configuration Item (CSCI). [DID ID: DI-IPSC-81441A] It is the detailed design and description of Software Items (SIs) comprising the product baseline. Analogous to the Item Detail Specification of a hardware Configuration Item (CI) in the product baseline of a hardware system. [Defense Acquisition University]
- v. Software Installation Plan (SIP): The SIP is a plan for installing software at user sites, including preparations, user training, and conversion from existing systems. [DID ID: DI-IPSC81428A]

- vi. * Software Test Plan (STP): The Software Test Plan (STP) describes plans for qualification testing of Computer Software Configuration Items (CSCIs) and software systems. It describes the software test environment to be used for the testing, identifies the tests to be performed, and provides schedules for test activities. There is usually a single STP for a project. The STP enables the acquirer to assess the adequacy of planning for CSCI and, if applicable, software system qualification testing. [DID ID: DI-IPSC-81438A]
 - vii. * Software Test Report (STR): The Software Test Report (STR) is a record of the qualification testing performed on a Computer Software Configuration Item (CSCI), a software system or subsystem, or other software-related item. The STR enables the acquirer to assess the testing and its results. [DID ID: DI-IPSC-81440A]
 - viii. * Software Test Description: The Software Test Description (STD) describes the test preparations, test cases, and test procedures to be used to perform qualification testing of a Computer Software Configuration Item (CSCI) or a software system or subsystem. [DID ID: DI-IPSC-81439A]
 - ix. * Software Design Description: The Software Design Description (SDD) describes the design of a Computer Software Configuration Item (CSCI). It describes the CSCI-wide design decisions, the CSCI architectural design, and the detailed design needed to implement the software. The SDD may be supplemented by the Interface Design Descriptions (IDDs) and Database Design Descriptions (DBDDs). [DID ID: DI-IPSC-81435A]
 - x. * Interface Requirements Specification: The Interface Requirements Specification (IRS) specifies the requirements imposed on one or more systems, subsystems, Hardware Configuration Items (HWCIs), Software Configuration Items (SWCIs), manual operations, or other system components to achieve on or more interfaces among these entities. [DID ID: DI-IPSC-81434A]
 - xi. Software Transition Plan (STrP): The developer shall identify all software development resources that will be needed by the support agency to fulfill the support concept specified in the contract. The developer shall develop and record plans identifying these resources and describing the approach to be followed for transitioning deliverable items to the support agency. [DID ID: DI-IPSC-81429A]
-

- xii. * Interface Design Description: An Interface Design Description (IDD) describes the interface characteristics of one or more systems, subsystems, hardware configuration items (HWCIs), computer software configuration items (CSCIs), manual operations, or other system components. [DID ID: DI-IPSC-81436A]
- xiii. * Data Accession List (DAL): The purpose of the DAL is to provide a medium for identifying contractor internal data which has been generated by the contractor in compliance with the work effort described in the Statement of Work (SOW). The DAL is an index of the generated data that is made available upon request. [DID ID: DI-MGMT-81453A]
- xiv. Computer Software Product End Items: Provides data formatted for review or maintenance to ensure significant milestones are met. Data produced under this requirement will be used during the life cycle for development, operation and maintenance. [DID ID: DI-MCCR-80700]
- xv. * Product Drawings/Models and Associated Lists: These data items provide engineering data to support competitive procurement and maintenance for items interchangeable with the original items. This data represents the highest level of design disclosure. [DID ID: DI-SESS-81000C]
- xvi. * Commercial Drawings/Models and Associated Lists: These data items define commercial items acquired by the Department of Defense. [DID ID: DI-SESS-81003C]
- xvii. Drawing Number Assignment Report: This data item provides the information necessary to maintain the Government's drawing number usage records. [DID ID: DI-SESS-81011C]
- xviii. Proposed Critical Manufacturing Process Description (PCMPD): The PCMPD identifies processes which are proposed for inclusion in the technical data package (TDP) as mandatory to meet the engineering requirements of the item or component part thereof for which the TDP is being prepared. [DID ID: DI-81012C]
- xix. Special Inspection Equipment (SIE) Drawings/Models and Associated Lists: These data items provide the data required for the limited production of SIE which duplicates the physical and performance characteristics of the original SIE. [DID ID: DI-SESS-81004C]
- xx. Special Tooling (ST) Drawings/Models and Associated Lists: These data items provided the data required for the limited

production of ST which duplicates the physical and performance characteristics of the original ST. [DID ID: DI-SESS-81008C]

- xxi. Source Control Drawing Approval Request: This data item provides the Government with a means for approving and disapproving the use of source control drawings for specific items selected for use in the equipment. [DID ID: DI-SESS-810100C]
- xxii. * Detail Specification Documents: A detail specification will be used to specify design requirements for items used in multiple programs or applications, in terms of materials to be used, how a requirement is to be achieved or how an item is to be fabricated or constructed. Detail specification documents are intended for reference in acquisition contracts. [DID ID: ID-SDMP-81464A]
- xxiii. * Program-Unique Specification Documents: A program-unique specification will be used to specify functional and performance requirements and, where applicable, design solutions for systems, items, software, processes, and materials developed and manufactured for use with a single system, product, or application. Requirements are stated, as applicable, in terms of required results, the environment in which it must operate, interface, and interchange characteristics; materials to be used; how the item is to be fabricated or constructed; and criteria for verifying compliance. Program-unique specification documents are intended for reference in contracts. [DID ID: ID-SDMP-81493]
- xxiv. Integrated Master Schedule (IMS): The IMS is an integrated schedule containing the networked, detailed tasks necessary to ensure successful program execution. The IMS is vertically traceable to the Integrated Master Plan (IMP) (if applicable), the Contract Work Breakdown Structure (CWBS), and the Statement of Work (SOW). The IMS shall be used to verify attainability of contract objectives, to evaluate progress toward meeting program objectives, and to integrate the program schedule activities with all related components. This DID is applicable to development, major modification, and low rate initial production efforts; it is not typically applied to full rate production efforts. [DID ID: DI-MGMT-81650]
- xxv. * Reuse Management Report (ReMR): The Reuse Management Report (ReMR) provides information about

existing software products intended to be reused as-is or modified as part of the delivered operational software. The report also provides the acquirer insight into the current status of the activities associated with the reuse of these products as compared to the planned activities, and alternative approaches. [DID ID: DI-SESS-81771]

The following recommended deliverables for open architecture systems do not have official Data Item Descriptions (DIDs) maintained by DoD. However, we have listed them and provided brief descriptions to help programs understand the additional types of data they should acquire during system acquisition [*with an asterisk (*) denoting those items that should be given strong consideration for inclusion.*]:

- xxvi. * An Open System Management Plan addressing architecture openness that describes, but is not limited to: the Offeror's approach to open system architecture, modular, open design; inter-component dependencies; design information documentation; technology insertion; life cycle sustainability; interface design and management; treatment of proprietary or vendor-unique elements; and, reuse of pre-existing items including all Commercial-Off-the-Shelf/Non-developmental Item (COTS/NDI) components, their functionality and proposed function in the system, and copies of license agreements related to the use of these components for Government approval. The Open System Management Plan shall also include a statement explaining why each COTS/NDI was selected for use. The initial plan shall be submitted with the CDRL.
- xxvii. * Results of [*periodic or milestone-based*] OSA assessments using Government-specified tools and methodologies, e.g., OAAT or MOSA PART.
- xxviii. Results of [*periodic or milestone-based*] market surveys conducted to identify candidate Government IP assets, COTS and other reusable NDI capable of achieving the performance requirements of solutions that it has proposed to custom build.
- xxix. * [*Semi-annual, annual, etc.*] Open Systems Architecture-related updates to the System Management Plan.
- xxx. * Results of regular [*semi-annual, annual, etc.*] reviews of the contractor's plan for addressing exceptions to reuse.

- xxxi. * Results of regular [*semi-annual, annual, etc.*] reviews of the contractor's plan for addressing (and minimizing the use of) proprietary or vendor-unique elements.
- xxxii. Documented results of product demonstrations that exhibit the OSA aspects of the system or component.
- xxxiii. * Regular [*semi-annual, annual, etc.*] review and update of the contractor's rationale for the modularization choices made to generate the design. These updates shall explicitly address any tradeoffs performed, particularly those that compromise the modular and open nature of the system.
- xxxiv. * Documents that provide a detailed tracing of all system requirements (including those contained in the Initial Capabilities Document, Capabilities Development Document, and in Section C of this Solicitation) to one or more design modules. [*See Section L, Paragraph 1, subparagraph 1.*]
- xxxv. * The Offeror shall provide documentation demonstrating that their system design meets MOSA and other requirements identified in Section C/SOW and can facilitate component reuse by conducting a series of demonstrations.
- xxxvi. * The Offeror shall deliver a notional test plan, test protocol, test design, testing software, testing tools, etc., necessary to support the independent Government testing and assessment of the _____ components and demonstration of the interoperability of the components.
- xxxvii. * The Offeror shall deliver to the Government, specifically the activity _____ a copy of the _____ software application(s) including all testing devices, testing software, results and materials, along with all supporting documentation, for the Government to use for testing.
- xxxviii. * The Offeror will develop and maintain a Common Data Model for the system and will provide the Government with updates at [*monthly, quarterly, etc.*] intervals.
- xxxix. * Executable source code and binaries (including the specified programming languages, libraries, and tools). This is applicable to software and firmware.
- xl. * Package description: makefiles. "Makefiles" is a set of software code that performs a set of actions in a sequence. Normally a "makefile" is a (plain text) script file that a compiler uses to compile and link files to make an executable. The file lets the compiler know the order to compile. Specifically, "make" is a command to use the makefile to

compile a C++ file. For example, Java uses a program called Ant (<http://ant.apache.org/>) which uses an XML file to do the same thing.

- xli. * Execution environment description. Execution environments (EEs) are symbolic representations of Java Runtime Environments (JREs). For example, rather than talking about a specific JRE, with a specific name at a specific location on your disk, you can talk about the J2SE-1.4 execution environment. The system can then be configured to use a specific JRE to implement that execution environment. Execution environments are relevant both to development (compile) time and runtime. [http://wiki.eclipse.org/Execution_Environments]
- xliv. * Installation script files in uncompressed segment installer format.
- xlv. * Software test programs and source code, including tools.
- xlii. * Software and system test report(s), test data (if available) and test metrics, including “bug reports.”
- xliii. * Software Development File (SDF): A repository for material pertinent to the development of a particular body of software. Contents typically include (either directly or by reference) considerations, rationale, and constraints related to requirements analysis, design, and implementation; developer-internal test information; and schedule and status information. [<http://sepo.spawar.navy.mil/SDF.doc>]
- xlvi. * Software Test Procedures: The Software Test Procedure describes plans for qualification testing of Computer Software Configuration Items (CSCIs) and software systems. [Pogner]
- xlvii. * Software User’s Manual (SUM): The Software User Manual (SUM) tells a hands-on software user how to install and use a Computer Software Configuration Item (CSCI), a group of related CSCIs, or a software system or subsystem. [University of Massachusetts; <http://www2.umassd.edu/SWPI/DOD/MIL-STD-498/SUM-DID.PDF>]
- xlviii. * Waveform: A waveform is the representation of a signal as a plot of amplitude versus time. [DAU]
- xlix. Porting Plan: A porting plan lists the main tasks of the port and some of the associated information for each task (start date, end date, elapsed time, dependencies, who is assigned, etc.). In programming, to “port” (verb) is to move an application program from an operating system environment in

which it was developed to another operating system environment so it can be run there. Porting implies some work, but not nearly as much as redeveloping the program in the new environment. Open standard programming interface (such as those specified in X/Open's 1170 C language specification and Sun Microsystem's Java programming language) minimize or eliminate the work required to "port a program." [SearchNetworking.com; http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gc1212807,00.html]

- i. Waveform Port Report. The information required to add, update, or enhance functional capabilities of the radio system through software without incurring the cost to change the underlying hardware.
- ii. Waveform Description Document. A waveform is the pictorial representation of the form or shape of a wave, obtained by plotting the amplitude of the wave with respect to time. This document describes simulation input vectors and simulation output vectors as graphical waveforms.
- iii. Security Engine: A security engine is a software resource that enforces security policies designed to help ensure that a vulnerability of an application or operating system cannot be exploited. Security engine provides security functions such as packet filtering, authentication, access control, intrusion analysis and audit trail in the kernel region of routers and other devices. They help systems detect intrusions and cope with an intrusion in real time.
- liii. Software Estimation File: The software estimate file contains the estimation of the software size, cost, schedule, and critical computer resources critical to the effective planning and tracking of a software-intensive project. [http://sepo.spawar.navy.mil/SW_Estimation_Process_Expert_Mode.doc]
- liv. * Software Security Report is a document that provides an analysis of possible security concerns for the system, component or subcomponent of concern.
- lv. Software Metrics Report: The software metrics report presents guidelines for establishing a software measurement process as part of an organization's overall software process. [IT Metrics & Productivity Institute; <http://www.itmpi.org/default.aspx?pageid=235>]

- lvi. * Software Configuration Management (SCM) Plan: The SCM Plan documents what SCM activities are to be done, how they are to be done, who is responsible for doing specific activities, when they are to happen, and what resources are required. It can address SCM activities over any portion of a software product's life cycle. [IEEE Standard 828-2005 for Software Configuration Management Plans]
- lvii. * Product Reuse Demonstration Inventory List: A detailed list of all code files in the product baseline, including all third-party software (operating systems, middleware, applications, and device drivers) not delivered within the terms of the contract but used in the system to form the working product.
- lviii. * Product Reuse Demonstration Inspection Report: A detailed list of all company markings found in the source code to ensure the Government has GPR to use the software delivered in the contract.
- lix. * Product Reuse Demonstration Build Procedure Development Report: A report containing a build procedure in sufficient detail to allow a third party to recreate the operational system on a compatible processing platform. It shall address the results of the code inventory and inspection to account for software that is not deliverable due to proprietary rights limitations such that the user can complete the installation process.
- lx. * Product Reuse Demonstration Report: A report detailing the results of the formal demonstration of the build process using the product baseline software and approved procedures showing the software can be successfully ported to other third-party compatible open architecture processing systems.
- lxi. * Technical description of the Integrated Digital Environment (IDE) (if applicable) proposed or being used by the contractor to develop and store project assets. This information should include the IDE construct, file structure, instantiation and other information necessary to provide life cycle support for the assets.

Appendix 2: OSA CHECKLIST (short)

The items below are intended to be a quick check on a system's programmatics that, when properly applied, will yield the benefits of an open system.

- ✓ For components which are expected to evolve to meet new or unforeseen performance requirements, does the Government have at least Government Purpose Rights (GPR) in any software or documentation being developed or used to build the system?
- ✓ Are proprietary components well-defined, limited in scope, and designed so that others are not precluded from interfacing with the component or other parts of the system or from developing and providing components with comparable or improved performance and form, fit and function?
- ✓ Are your program's design artifacts disclosed "early and often" and freely available for reuse by another program or third parties?
- ✓ Is design disclosure enabled by keeping data, code and design artifacts in a repository either maintained by or overseen by the Government, or those made available through the Forge.mil Program (<http://www.forge.mil/>); providing the artifacts electronically upon requests made via the Government; allowing requesting parties to obtain them directly from the source firm through a process involving review and approval from the Government; or requiring that contractors allow the program to have continuous, real-time visibility, access to and the ability to download artifacts from the development environment?
- ✓ Does the program use widely-accepted and supported standards to define interface definitions or key interfaces that are published and maintained by recognized organizations?
- ✓ Does your program encourage continuous competition for components, modules, and tasks? Is it easy for your follow on contract to go to anyone other than the incumbent?
- ✓ Does your program utilize commodity products (i.e., COTS products with a large user base)? Can the decision leading to the selection of specific COTS products be supported with test results, architectural suitability, "best value" assessments, etc.?
- ✓ Does your program reuse modules or components that are also being used by other programs with different product vendors?
- ✓ Does the program plan and directive documentation specify that anything the Government paid to develop be made available for

- delivery to the Government with all of the developmental artifacts and unlimited usage rights?
- ✓ Does your program use an integrated team/peer review approach to identify how changes affect the system?
 - ✓ Is the infrastructure of your system open? (Operating System, Databases, Communications, Interfaces, Tools)
 - ✓ Does porting to a new hardware platform require minimal time and resources?
 - ✓ Has the program completed an open architecture return on investment analysis to determine which components might yield the greatest benefits from OSA?

CHECKLIST OF REQUIRED FAR AND DFARS CLAUSES

[Note to Preparers: *When citing regulations such as the DFARS and FAR, dates are included where possible to reflect the most recent version of this Guidebook. However, Contracting Officers and PMs need to check for current clause dates before using the language in this Guidebook.*]

A. IP Clauses for Government Contracts

When reviewing a draft contract, first determine if it is primarily for commercial items or noncommercial items. This will typically be apparent from the contract cover sheet - the SF-33 form is used for noncommercial procurements and the SF-1449 is used for commercial item procurements. Images of blanks of both forms are available in FAR Part 53.3, at <http://www.arnet.gov/far/loadmainre.html>. If you are in doubt whether commercial or noncommercial data or software is being acquired, it is helpful to review the definition of "commercial item" at FAR 2.101.

For Contracts that are research and development (R&D) contracts, include the following IP related FAR clauses in accordance with their prescriptions:

FAR
52.227-1 Authorization and Consent (Not limited to R&D contracts; it generally goes in all contracts except as noted in 27.201.)
52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement (Used when 52.227-1 is used).
52.227-11 or -13 (-11 for Small Businesses and Non Profits; DFARS 252.227-7038 for large businesses; and -13 for Foreign-owned/located businesses where the contract work is being performed overseas)

Except as noted, all the FAR clauses go in Section I of the contract.

Also include the following clauses in acquisition contracts:

DFARS	
252.227-7013	Rights in Technical Data—Noncommercial Items
252.227-7014	in Noncommercial Computer Software and Noncommercial Computer Software Documentation
252.227-7015	Technical Data—Commercial Items
252.227-7016	Rights in Bid or Proposal Information
252.227-7017	Identification and Assertion of Use, Release, or Disclosure Restrictions (Note: RFPs only, Section K)
252.227-7019	Validation of Asserted Restrictions—Computer Software
252.227-7025	Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends
252.227-7027	Deferred Ordering of Technical Data or Computer Software
252.227-7028	Technical Data or Computer Software Previously Delivered to Government (Note: RFPs only, Section K)
252.227-7030	Technical Data—Withholding of Payment
252.227-7037	Validation of Restrictive Markings on Technical Data
252.227-7038	Patent Rights—Ownership by the Contractor (Note: Large Business)
252.227-7039	Patents—Reporting of Subject Inventions (Note: Use only when FAR 52.227-11 is used)

All the DFARS clauses go in Section I of the contract, except as noted above.

For SBIR contracts, substitute DFARS 252.227-7018 for 252.227-7013 and 7014.

For Contracts that are procuring commercial technical data and/or commercial software, add the patent indemnity clause, FAR 52.227-3.

B. SBA Policy on SBIR contracts

For programs that are leveraging the Small Business Innovative Research (SBIR) program, the DoD SBIR data rights clause is at DFARS 252.227-7018, which implements the Small Business Innovation Research Policy Directive.⁴⁴

⁴⁴ See <http://www.sbir.gov/about/about-sbir> for more information. The SBA Policy Directive was published in the Federal Register Vol. 67, No. 185, Tuesday, September 24, 2002. More specifically, Section 8 of the Directive provides direction for all federal agencies regarding IP/data rights. As of this

publication, the Small Business Administration has published a proposed update of its SBIR Policy Directive. Those concerned with SBIR contracts should monitor developments on the Directive.

Appendix 3: OSA CHECKLIST (long)

There are five main principles of Department of Defense Open Systems Architecture (OSA) that form the basis for system design and program management of weapons systems. The items below are intended to be a quick check on a system's programmatics that, when properly applied, will yield the benefits of an open system.

Modular designs with loose coupling and high cohesion that allow for independent acquisition of system components:

- ✓ Does the system design de-couple hardware, operating system and middleware from applications?
- ✓ Are the system's applications functionally segregated to function as independent entities?
- ✓ Can the computing hardware be upgraded without the necessity to change operating system, middleware or applications?
- ✓ Are the functional components of the system well defined with clearly specified behaviors and interfaces?
- ✓ Have unique or proprietary solutions been used where widely-accepted standards are available?
- ✓ Are the development environment tools for each application "industry standard", and openly available as a set of products?

Enterprise investment strategies, based on collaboration and trust, that maximize reuse of proven system designs and ensure we spend the least to get the best:

- ✓ Has the program investigated potential reusable/modify-able components from other programs?
- ✓ Does the contract/RFP require the prospective integrator and developer to conduct market research to identify potential reuse candidates from a broad spectrum of providers? This activity should involve the PM for final decision.
- ✓ Does the program participate in Domain/Community of Interest asset reuse repository/library capabilities?
- ✓ Has the program ensured that potential Offerors who do not have access to reuse repositories/libraries are allowed access to artifacts as appropriate?
- ✓ Has the acquisition planned for separate contracts for the various components of the system?

- ✓ Have incentive structures been built into the program plan and contracts to reward cooperation and collaboration among the architect, integrator, and component providers?
- ✓ Did the program develop an Open Architecture Business Case using the appropriate guidance?
- ✓ Has the program completed an Open Architecture return on investment (ROI) analysis to determine which system components might yield the greatest benefits from the application of OSA?

Aggressively transform our life-cycle sustainment strategies for software intensive systems through proven technology insertion and product upgrade techniques:

- ✓ Has the program built in incentive structures to reward reduction in total ownership cost over the life cycle?
- ✓ Has the system design reduced life cycle cost by leveraging modularity to reduce the effort and cycle time of system modernization?
- ✓ Has the program made use of commodity COTS computing and networking hardware to reduce procurement and maintenance cost? Can the decision leading to the selection of specific COTS products be supported with test results, architectural suitability, “best value” assessments, etc.?
- ✓ Has the program used the Key Open Subsystem Tool or another tool to identify those components which might have opportunities for frequent technology insertion?

Dramatically lower development risk through transparency of system designs, continuous design disclosure, and Government, academia, and industry peer reviews:

- ✓ Are the system/subsystem/component/application specifications and design data available to a broad cross section of potential providers?
- ✓ Is the end user included in the system design and upgrade process as well as the training definition?
- ✓ Has a transparent peer group process been established to provide for independent evaluation of alternative components and selection of best of breed components for the system?
- ✓ Has the peer group been utilized to the maximum extent practicable to aid in technical and business planning for the system acquisition?

Strategic use of data rights to ensure a level competitive playing field and access to alternative solutions and sources, across the life cycle:

- ✓ Are design details available throughout the development process?
- ✓ Have the appropriate data rights been obtained with each application (normally Government Purpose Rights)?
- ✓ If a product contains proprietary elements, are the license requirements for use clearly documented, and those proprietary elements segregated with well-defined interfaces such that modification of another component will not require modification of the proprietary product?
- ✓ Have the asset packages (i.e., the deliverables) been reviewed prior to Government acceptance to ensure that they reflect the agreed upon licenses and data rights markings?
- ✓ Has the program leveraged the Science and Technology (S&T) program to identify innovative concepts and new participants?

CHECKLIST OF REQUIRED FAR AND DFARS CLAUSES

[Note to Preparers: *When citing regulations such as the DFARS and FAR, dates are included where possible to reflect the most recent version of this Guidebook. However, Contracting Officers and PMs need to check for current clause dates before using the language in this Guidebook.*]

A. IP Clauses for Government Contracts

When reviewing a draft contract, first determine if it is for commercial items or noncommercial items. This will typically be apparent from the contract cover sheet - the SF-33 form is used for noncommercial procurements and the SF-1449 is used for commercial item procurements. Images of blanks of both forms are available in FAR Part 53.3, at <http://www.arnet.gov/far/loadmainre.html>. If you are in doubt whether commercial or noncommercial data or software is being acquired, it is helpful to review the definition of "commercial item" at FAR 2.101.

For Contracts that are research and development (R&D) contracts, include the following IP related FAR clauses in accordance with their prescriptions:

FAR

52.227-1 Authorization and Consent (Not limited to R&D contracts; it generally goes in all contracts except as noted in 27.201.)

52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement (Used when 52.227-1 is used).
(DFARS 252.227-7010 License to Other Government Agencies)
52.227-11 or -13 (-11 for Small Businesses and Non Profits; DFARS 252.227-7038 for large businesses; and -13 for Foreign-owned/located businesses where the contract work is being performed overseas)

Except as noted, all the FAR clauses go in Section I of the contract.
Also include the following clauses:

DFARS
252.227-7013 Rights in Technical Data—Noncommercial Items
252.227-7014 in Noncommercial Computer Software and Noncommercial Computer Software Documentation
252.227-7015 Technical Data—Commercial Items
252.227-7016 Rights in Bid or Proposal Information
252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions (Note: RFPs only, Section K)
252.227-7019 Validation of Asserted Restrictions—Computer Software
252.227-7025 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends
252.227-7027 Deferred Ordering of Technical Data or Computer Software
252.227-7028 Technical Data or Computer Software Previously Delivered to Government (Note: RFPs only, Section K)
252.227-7030 Technical Data—Withholding of Payment
252.227-7037 Validation of Restrictive Markings on Technical Data
252.227-7038 Patent Rights—Ownership by the Contractor (Note: Large Business)
252.227-7039 Patents—Reporting of Subject Inventions (Note: Use only when FAR 52.227-11 is used)

All the DFARS clauses go in Section I of the contract, except as noted above.

For SBIR contracts, substitute DFARS 252.227-7018 for 252.227-7013 and -7014.

For Contracts that are procuring commercial data and/or commercial software, add the patent indemnity clause, FAR 52.227-3.

B. SBA Policy on SBIR contracts

For programs that are leveraging the Small Business Innovative Research (SBIR) program, the DoD SBIR data rights clause is at

DFARS 252.227-7018, which implements the Small Business Innovation Research Policy Directive.⁴⁵

⁴⁵ The SBA Policy Directive was published in the Federal Register Vol. 67, No. 185, Tuesday, September 24, 2002. More specifically, Section 8 of the Directive provides direction for all federal agencies regarding IP/data rights. As of this publication, the Small Business Administration has published a proposed update of its SBIR Policy Directive. Those concerned with SBIR contracts should monitor developments on the Directive.

Appendix 4: RECOMMENDED DATA LANGUAGE FOR CODE HEADERS

Deliverable artifacts should include embedded data or language in code headers or in other locations that provides key information for those seeking to use these items in the future. The following are suggestions that can be used as appropriate for artifacts delivered under Unlimited, GPR, and Specially Negotiated License Rights.

[Note to Preparers: *Distribution Statements required by DoD Directive 5230.25 do not correlate to specific data rights categories and vice versa. Data rights allocate the intellectual property interests of both Government and industry according to the type of data, the use of the data, and the source of funding used to develop the item, component, process or computer software pertaining to the deliverable. Distribution Statements may be based upon a number of additional restrictions including information security and export control. There are scenarios where a DoD program would have Unlimited Rights in a deliverable, but would not want to authorize uncontrolled distribution of the deliverable because of such other restrictions and these would be reflected in Distribution Statement limitations. Conversely, a Limited Rights deliverable might have no security or export control reasons for limited distribution. However, since the deliverable was delivered with Limited Rights, the DoD program cannot distribute the deliverable outside the Government generally without the developing contractor's written permission.*]

a. Recommended Language Regarding Restrictive Rights

The Government must be vigilant in identifying and challenging any restrictive markings on deliverables that are inconsistent with the rights the Government has acquired under the contract. For example, if the Government has contracted for GPR in a particular deliverable, the contractor shall not mark that deliverable with any legend that would limit or contradict that GPR license.

To protect against this occurrence, if an individual supporting the [specific] program identifies any restrictive markings on a deliverable, that individual shall immediately notify the cognizant Program Manager and Contracting Officer to ensure that any such restrictive markings are consistent with the terms of the contract. If those markings are not consistent with the terms of the contract, the Government shall not accept the deliverables, the Program Manager shall promptly notify the [PEO], and the Contracting Officer shall promptly follow the procedures in DFARS 252.227-7013, DFARS

252.227-7014 and DFARS 252.227-7018 for handling nonconforming markings and the procedures in DFARS 252.227-7019 and DFARS 252.227-7037 for handling unjustified markings.

[Note to Preparers: *The following are examples of Code Headers – the exact language for rights markings, Distribution Statements and warnings such as the Arms Export Control Act need to be determined separately. For example, code can be classified and should be appropriately marked, consistent with existing guidance. Distribution Statements should be consistent with DoD Directive 5230.25. This directive can be found at*

http://jitc.fhu.disa.mil/jitc_dri/pdfs/d523025p.pdf.]

Unlimited

////////////////////////////////////
/// SECURITY CLASSIFICATION: UNCLASSIFIED
////////////////////////////////////
/// Copyright © (Name of work's owner and date published if applicable)

[Note to Preparer: *If required, use this Statement. Notwithstanding any copyright notice, U.S. Government rights in this work are defined by DFARS 252.227-7013 or DFARS 252.227-7014 as detailed below. Use of this work other than as specifically authorized by the U.S. Government may violate any copyrights that exist in this work.]*

[Note to Preparer: *There are currently no authorized markings in the DFARS for Unlimited Rights data or software. Further, noncommercial data or software delivered to the Government without markings is considered to be delivered with Unlimited Rights. Consult your counsel for specific guidance regarding Unlimited Rights markings.]*

/// UNLIMITED RIGHTS
/// DFARS Clause reference: 252.227-7013 (a)(16) and 252.227-7014 (a)(16)
/// Unlimited Rights. The Government has the right to use, modify, reproduce, perform,
/// display, release or disclose this (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.
///
/// Distribution Statement D. Distribution authorized to the Department of Defense and
/// U.S. DoD contractors only in support of US DoD efforts. Other requests shall be
/// referred to [PEO].
///
/// Warning: - This document contains data whose export is restricted by the Arms Export
/// Control Act (Title 22, U.S.C., Section 2751, et seq.) as amended, or the Export
Administration
/// Act (Title 50, U.S.C., App 2401 et seq.) as amended. Violations of these export laws
/// are subject to severe criminal and civil penalties. Disseminate in accordance with
/// provisions of DoD Directive 5230.25.

[Note to Preparers: *This is an example of a Code Header -- the exact language for rights markings, Distribution Statements and warnings such as the Arms Export Control Act need to be determined separately. For example, code can be classified and should be appropriately marked, consistent with existing guidance. Distribution Statements should be consistent with DoD Directive 5230.25. This directive can be found at http://jtc.fhu.disa.mil/jtc_dri/pdfs/d523025p.pdf.]*

Government Purpose Rights

////////////////////////////////////
/// SECURITY CLASSIFICATION: UNCLASSIFIED
////////////////////////////////////

/// Copyright © (Name of work's owner and date published if applicable)

[Note to Preparer: *If required, use this Statement. Notwithstanding any copyright notice, U.S. Government rights in this work are defined by DFARS 252.227-7013 or DFARS 252.227-7014 as detailed below. Use of this work other than as specifically authorized by the U.S. Government may violate any copyrights that exist in this work.]*

/// GOVERNMENT PURPOSE RIGHTS

///Rights in Technical Data, computer software & documentation in non-commercial items
///DFARS Clause: 252.227-7013 (f)(2) and 252.227-7014 (f)(2)

Government Purpose Rights. 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 Technical Data-Noncommercial Items clause contained in the below identified contract. No restrictions apply after the expiration date shown below. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings.

- Contract No.
- Contractor Name
- Contractor Address
- Expiration Date

///
/// Distribution Statement D. Distribution authorized to the Department of Defense and
/// U.S. DoD contractors only in support of US DoD efforts. Other requests shall be
/// referred to [PEO].

///
/// Warning: - This document contains data whose export is restricted by the Arms Export
/// Control Act (Title 22, U.S.C., Section 2751, et seq.) as amended, or the Export
/// Administration
/// Act (Title 50, U.S.C., App 2401 et seq.) as amended. Violations of these export laws
/// are subject to severe criminal and civil penalties. Disseminate in accordance with
/// provisions of DoD Directive 5230.25.

[Note to Preparers: *This is an example of a Code Header -- the exact language for rights markings, Distribution Statements and warnings such as the Arms Export Control Act need to be determined separately. For example, code can be classified and should be appropriately marked, consistent with existing guidance. Distribution Statements should be consistent with DoD Directive 5230.25. This directive can be found at http://jitc.fhu.disa.mil/jitc_dri/pdfs/d523025p.pdf.]*

Specially Negotiated License Rights

////////////////////////////////////
/// SECURITY CLASSIFICATION: UNCLASSIFIED
////////////////////////////////////

/// Copyright © (Name of work's owner and date published if applicable)

[Note to Preparer: *If required, use this Statement. Notwithstanding any copyright notice, U.S. Government rights in this work are defined by DFARS 252.227-7013 or DFARS 252.227-7014 as detailed below. Use of this work other than as specifically authorized by the U.S. Government may violate any copyrights that exist in this work.]*

/// Specially Negotiated License Rights

///Rights in Technical Data, computer software & documentation in non-commercial items
///DFARS Clause: 252.227-7013 (f)(2) and 252.227-7014 (f)(2)

The Government's rights to use, modify, reproduce, release, perform, display, or disclose these technical data and computer software are restricted by the specially negotiated Government Purpose Rights license contained in the below identified agreement. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings.

Contract No.
Contractor Name:
Contractor Address:
Expiration Date:

///
/// Distribution Statement D. Distribution authorized to the Department of Defense and
/// U.S. DoD contractors only in support of US DoD efforts. Other requests shall be
/// referred to JPEO JTRS.

///
/// Warning: - This document contains data whose export is restricted by the Arms Export
/// Control Act (Title 22, U.S.C., Section 2751, et seq.) as amended, or the Export
/// Administration Act (Title 50, U.S.C., App 2401 et seq.) as amended. Violations of
/// these export laws are subject to severe criminal and civil penalties. Disseminate in
/// accordance with provisions of DoD Directive 5230.25.

[Note to Preparers: *This is an example of a Code Header -- the exact language for rights markings, Distribution Statements and warnings such as the Arms Export Control Act need to be determined separately. For example, code can be classified and should be appropriately marked, consistent with existing guidance. Distribution Statements should be consistent with DoD Directive 5230.25. This directive can be found at http://jtc.fhu.disa.mil/jtc_dri/pdfs/d523025p.pdf.]*

Appendix 5: OPEN SOURCE SOFTWARE

There is a strong relationship between Open Source Software (OSS) and Open Architecture (OA), or Open Systems Architecture (OSA). The terms “open source” and “open architecture” are often confused and at times even incorrectly used interchangeably. However, these terms are distinct and different:

* Open Source Software is software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by the users of that software.⁴⁶ [DoD CIO Memorandum, “Clarifying Guidance Regarding Open Source Software (OSS)”, 16 Oct 2009⁴⁷]

* “Open architecture” is a type of architecture (or design) whose specifications are made public by its designers which allows users to make modifications to various components. The Open Systems Joint Task Force (OSJTF) defines “open system architecture” as a system that employs modular design, uses widely supported and consensus based standards for its key interfaces, and has been subjected to successful validation and verification tests to ensure the openness of its key interfaces.

By definition, the source code to OSS is available for examination, modification and redistribution. For software, the source code is the ultimate level of design specification, so at that level, OSS is always “open architecture” in some sense. However, the source code is not the only level of design specification, and may not be the most important level to consider. Likewise, OSS software may not be the only component of a system. Some OSS *might not* employ modular design, *might not* use widely supported and consensus based standards for its key interfaces, or *might not* have been subjected to successful validation and verification tests to ensure the openness of its key interfaces. For example, “Netatalk” is an open *implementation* of the proprietary protocol AppleTalk. Thus, just because a system includes “Open Source Software” does not automatically give it an “Open Systems Architecture.” That said, much of the business value of Open

⁴⁶ See also, the Open Source Initiative’s more robust and detailed definition of open source, including 10 open source criteria, at <http://www.opensource.org>.

⁴⁷ Readers may also want to refer to the definition developed by the Open Source Initiative (<http://www.opensource.org>) and the definition of “free software” developed by the Free Software Foundation (<http://www.fsf.org>).

Systems Architecture – agility, reduced vendor lock-in, reuse, modularity, and otherwise promoting real competition in the acquisition of goods and services, is also a value of Open Source Software.

The following is recommended guidance for DoD and Service Program Managers who choose to use open source software in their systems.

1. General Information:

a. DoD Memorandum Clarifying Guidance Regarding Open Source Software (OSS)

On October 16, 2009, the Assistant Secretary of Defense (Networks and Information Integration) / DoD Chief Information Officer (CIO) issued a Memorandum for Secretaries of the Military Departments on Clarifying Guidance Regarding Open Source Software (OSS). The memo stated that “there have been misconceptions and misinterpretations of the existing laws, policies and regulations that deal with software and apply to OSS, that have hampered effective DoD use and development of OSS.”

The DoD guidance acknowledges that in “almost all cases, OSS meets the definition of ‘commercial computer software’.” It also details some positive aspects of OSS to be considered when conducting market research into commercial computer software:

- i. Continuous and broad peer-review supports software reliability efforts;
- ii. Unrestricted ability to modify source code enables rapid responses to changing situations;
- iii. Reduced reliance on a particular software developer or vendor;
- iv. Lack of restrictions, usually, on who can use the software and in what fields of endeavor it can be used, thus enabling a net-centric licensing model;
- v. A cost advantage due to its typical lack of a per-seat or per processor licensing cost;
- vi. Reduced total ownership cost due to shared maintenance responsibility; and
- vii. Suitability for rapid prototyping and experimentation due to the ability to “test drive” the software with minimal costs and delays.

Additionally, the guidance highlights the common “misconception that the Government is always obligated to distribute the source code of any modified OSS to the public, and therefore that OSS should not be integrated or modified for use in classified or other sensitive DoD systems. In contrast, many open source licenses

permit the user to modify OSS *for internal use* without being obligated to distribute source code to the public.”

More information on the DoD’s policies with respect to OSS is available at

<http://dodcio.defense.gov/Home/Topics/UseofFreeOpenSourceSoftwareFOSS.aspx> The October 16 memo is available at <http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf>

As the DoD guidance states, open source software is generally regarded as commercial computer software for which the source code is publicly available to all users under specific licensing terms and conditions that provide a user the right to use, modify, and redistribute the modified open source software to the public. Some open source software licenses require that, if further distributed, the modified open source software be distributed under the terms and conditions of the original license.

b. Issues to Consider When Using Open Source Software

Open source software almost always meets the definition of commercial computer software under the Defense Federal Acquisition Regulations Supplement (DFARS).⁴⁸ As such, the same DFARS policies that apply to procurement of commercial computer software would also apply to open source software. That is, the Government shall have only the rights specified in the license under which the commercial computer software was obtained. If the Government has a need for rights not normally conveyed to the public, then the Government must negotiate with the commercial computer software vendor. See DFARS 227.7202-3, “Rights in Commercial Computer Software or Commercial Computer Software Documentation.” As with other commercial computer software or software documentation, while the Government should accept licenses customarily provided to the public, acceptable licenses must be consistent with Federal procurement law and satisfy user needs. See DFARS 227.7202-1, “Policy.” For open source software, in some cases these may present special challenges as detailed below:

⁴⁸ See DFARS 252.227-7014(a)(1), and FAR 2.101 (“ ‘Commercial computer software’ means any computer software that is a commercial item.”).

i. **Inability to Negotiate**

The copyright holder(s) of the open source software often are not available for negotiating lesser or greater rights than those rights provided by the license that governs the open source software. Accordingly, the Government may have to consider accepting open source software under the terms and conditions dictated by the open source software license with the knowledge that the Government will not be able to negotiate the open source software license terms. Most OSS licenses do not require express agreement by a licensee, but purport to become binding if one were to use the software. Many argue that these OSS licenses are just that—licenses—and not contracts (“Enforcing the GPL”, Eben Moglen, 10 September 2001). Even if they would be considered contracts, state contract laws may permit such an implied-in-fact contract to be created by the conduct of a non-Federal Government entity. Since Federal law limits contracting authority to certain officials and usually requires certain formalities, there is a presently an open legal question of whether mere use by the Government would constitute agreement to the terms of an OSS license. This is significant because without a valid contract, if the Government uses OSS software but is unable or unwilling to comply with some license term, the copyright holder/licensor may be limited to remedies under 28 U.S.C. Section 1498 (as discussed further below) and not have a cause of action under contract law. This aspect should be considered further with legal counsel if non-negotiable and unacceptable terms exist in a prospective OSS license.

Some commercial software licenses, including open source software licenses, include terms unacceptable to the Government, such as, certain kinds of indemnification, choice of law (agreeing to be bound by the law of a particular state or country other than the United States), choice of forum (agreeing that disputes will be adjudicated in a particular forum such as courts of a particular state, nation or nongovernmental entity), reimbursement of attorneys fees, etc. Some licenses have choice of law and/or choice of forum provisions, e.g., EU Public License, Sun, Public License. Some licenses have loser pays provisions in the event of litigation including payment of attorneys fees, e.g., Common Development and Distribution License. Further, some licenses may permissively allow the specifying of terms which

may be problematic for the Government. The mere fact that software is open source does not mitigate the unacceptability of such terms when they are mandatory. When clearly legally unacceptable terms are mandatory in a license, not purely optional or electable, the license and the software may be completely unacceptable. DoD has not issued blanket guidance regarding the legal sufficiency of any OSS license nor should the mention of any specific OSS license in this Guide be taken as signifying that any license is legally acceptable or not in any or all circumstances. Licenses may be acceptable or not depending on any license tailoring upstream as well as the intended uses by the Government or its contractors.

Accordingly, care should be taken when considering use of commercial software (including OSS) by the Government, whether in acquisition planning and source selection or in direct use by Government employees. Due diligence in this area should always include legal counsel early in considerations.

However, in some cases, the Government, (or systems integrators on contract to the Government) *has* negotiated separate licenses with the copyright holders of open source software; so this approach should not be discounted. Since OSS is developed collaboratively, in many cases there may be simply too many copyright holders to reasonably negotiate alternative licenses. The Linux kernel, for example, is a collaborative work with thousands of copyright holders, and any attempt to negotiate alternative terms would be impractical.

ii. **License Compatibility**

Since most modern software is built of modular components distributed under licenses with conditions, any system that is a combined work (i.e., many components integrated together) must itself be distributed under terms that satisfy *all* of the conditions of *all* of the components. This concept is described as “license compatibility”. For example, the MIT/X11 license permits software to be used in any form, with only one condition: *“The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.”* The BSD-New license includes three conditions:

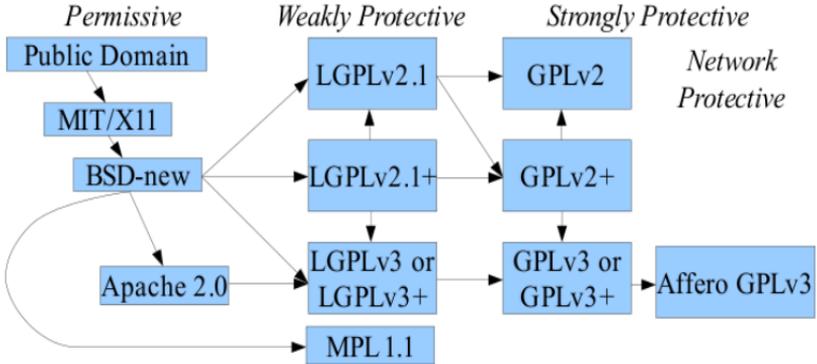
- a) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- b) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- c) Neither the name of the <organization> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Software that combines both MIT/X11 licensed code and BSD-New licensed code can be combined into a joint work, because all four of these conditions can be satisfied simultaneously.

As a counter example, the GNU General Public License version 2 (GPLv2) contains a clause that “Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. *You may not impose any further restrictions on the recipients' exercise of the rights granted herein.*” (Emphasis added) The Apache 2.0 license contains clauses for patent termination and indemnification, which are restrictions not present in GPLv2. As such, a notional computer program that included both GPLv2-licensed components and Apache2.0-only-licensed components might not be legally distributed because it may not be possible to satisfy both licenses simultaneously. This may be solved if the software using the GPL uses the license “GPL version 2 or greater,” as it is generally accepted that GPL version 3 is compatible with the Apache 2.0 license. Legal counsel should be consulted for specific analysis.

These license concerns only apply to a single, conjoined work for the purposes of copyright law. Two separate programs that are part of a single system may have incompatible licenses. Merely being present side-by-side (on the same computer, or same media) probably does not create a single work but “compilation” copyrights must be considered when appropriate. See 17 U.S.C. Section 103.

There are a large number of OSS licenses, but only a few are widely used. The widely-used licenses tend to be compatible, i.e., the software can be combined to produce a larger work. The following figure shows when software under common licenses can probably be combined:



In this figure, the shaded boxes are the names of different OSS licenses. An arrow from a first box A to a second box B means that you *can* combine software with these licenses; the combined result effectively has the license of B, possibly with additions from A. To see if software can be combined, just start at their respective licenses, and find a common box you can reach following the arrows (aka “following the slide”). For example, Apache 2.0-licensed software and GPLv2+-licensed software can both reach “GPLv3 or GPLv3+”, so they can be combined using GPLv3 or GPLv3+. This figure has been carefully crafted so following a path determines if two licenses are probably compatible. For more certain answers, the license text should be examined carefully, but this gives basic answers quickly.

At the left are the “permissive” licenses, which permit the software to become proprietary (i.e., not OSS). At the top left is “Public Domain”, which strictly speaking is not a license but in effect it works like one. *Anything* can be done with public domain software, but it is rare; the software must be explicitly donated to the public domain by the copyright owner. (Works created solely by U.S. Government employees in their official capacities are not protected by copyright in the United States, but may be protected by copyright in other

countries. See 17 U.S.C. Section 105.) Next is the so-called “MIT” or “X11” license, which is very permissive (you can do just about anything except sue the author). As described above, software under the MIT license is easily combined with the modern 3-clause Berkeley Software Distribution (BSD-new) license, which compared to the MIT license adds a clause forbidding the use of the author’s name to endorse or promote products without permission. Finally, there is the Apache version 2.0 license, which is similar, but includes patent grant provisions, and contingent indemnification clauses.

At the right are the “strongly protective” (“strong copyleft”) licenses, which prevent the software from becoming proprietary. This includes the most popular OSS license, the GNU General Public License (GPL). The GPL has a version 2 (GPLv2) and 3 (GPLv3); a “+” afterwards means “version X or later”. GPLv2-only cannot be combined with the network-protective Affero GPLv3, but GPLv2+ (“version 2 or later”) can via GPLv3. These licenses have conditions that typically require that any distribution of the software (including modified versions and compiled binary versions) also include the source code, and that the recipient of the distribution be granted the same license.

- iii. In the middle are the “weakly protective” (“weak copyleft”) licenses, a compromise between permissive and strongly protective licenses. These prevent the software component (often a software library) from becoming proprietary, yet permit it to be part of a larger proprietary program. This figure shows the rules when making other software *part* of the weakly protected component; there are other possibilities if you are only using the component as a library. The GNU Lesser General Public License (LGPL) is the most popular weakly protective license, and has a version 2.1 (LGPLv2.1) and 3 (LGPLv3). Note that LGPLv2.1 provides permission to relicense the code under any version of the GPL since GPLv2. Another such license is the Mozilla Public License version 1.1 (MPL 1.1), but the MPL has the serious drawback of being incompatible with the more common GPL. Software released solely under the MPL version 1.1 license cannot be directly combined into a larger GPL’ed program.

iv. **Protective licenses and redistribution issues**

The way that protective OSS licenses prevent open software from becoming proprietary is to require that any distribution of the software (or of derivative works) be licensed under the same license, and furthermore to require distribution of the software in source-code form. This can present issues for Government applications in some circumstances, where distribution of the source code might be required by the software license, but may be forbidden by other circumstances, such as export control, classification, proprietary data rights, or other national security interests.

For example, it is common for software for weapon systems to be restricted under the International Traffic in Arms Regulation (ITAR), in such a way that the compiled software in the weapon system may be exported, but the source code may not be exported. If the weapon system includes, for example, GPL-licensed code, then the weapon system as a whole could not be legally exported, because the source code is export-restricted, and the compiled binary code can only be distributed (per the GPL) if the source code is also provided. Since these two conditions conflict, the system itself could not be exported without violating either the ITAR or the Copyright Act.

As another example, software that is GPL-licensed can be merged with classified software, resulting in software that is both classified and open source. The resulting software could only be distributed to individuals who have the appropriate clearance. Some commentators opine that since the restrictions on distribution of classified materials are pre-existing national security policy, this is not an imposition of additional restrictions, which would be a violation of the clause in the GPLv2 which reads, "*You may not impose any further restrictions on the recipients' exercise of the rights granted herein.*" In such a circumstance, significant caution would be prudent so that individuals interacting with such software are well informed of the uncommon status of software which is both "open" and restricted at the same time, in different ways. It also must be cautioned that the view of classification as a preexisting condition is not universal. Legal counsel should be consulted.

To accept open source software, the Government must be prepared to accept delivery of open source software under the terms of the open source software license, and with the

knowledge that Government will not be able to negotiate the open source software license terms. At the same time, the Government must also comply with the licensing and operational security requirements of non-open source software. Thus, to accept delivery of open source software while complying with all computer software licensing requirements including Federal fiscal and procurement law, regardless of license, the Government must have a very good understanding of:

- a) What the software is and the licensing constraints for the software (whether it is open source software or not);
- b) How the software will be used within the system being procured;
- c) Whether it is likely the software will need to be modified and/or distributed over the life cycle of the system;
- d) The impacts on non-open source computer software, both commercial and non-commercial, if distribution under the open source software license is required when the open source software is modified; and
- e) Whether any mandatory license terms violate Federal fiscal and procurement law prohibitions regarding, e.g., unfunded contingent liabilities (e.g., through indemnification, which is generally prohibited or disfavored), choice of law or forum, or reimbursement of court costs or attorneys' fees.

v. **Authorization and Consent.**

Open source software may be covered by a patent of the United States, or by copyright under the Copyright Act (Title 17, U.S. Code). When the Government "authorizes and consents" to patent or copyright infringement under 28 U.S.C. Section 1498, the Government may be sued for money damages for the infringement but not enjoined from using the open source software. However, where the Government does not "authorize or consent," the contractor may be sued for money damages and may be enjoined from further use of the open source software.

- a) The Authorization and Consent Clause for patents, FAR § 52.227-1, should be inserted in accordance with the FAR prescriptive guidance. However, there is currently no prescriptive guidance or a contract clause in the FAR or DFARS for authorization and consent to use any

copyright including on software without a license. The Government may consider giving copyright authorization and consent to ensure that work under a Government contract is not enjoined in certain cases, such as when the quality of the open source software justifies acceptance despite the licensing constraints, where there are no acceptable substitutes, where time constraints for delivery do not allow for substitutes, etc. The assessment of need for authorization should carefully consider whether a contractor supplying OSS to the Government would be required to actually do anything inconsistent with a license. Few OSS licenses require that a contributor/modifier/licensor of OSS ensure that a downstream user assent to the license terms. In other words, just because the Government may not be able to agree to some license term, e.g., indemnification, does not necessarily mean that the supplying contractor cannot comply with the license terms. Thus, a contractor may be able to fully comply and not need authorization and consent even if the Government must consider using the OSS without full license compliance in reliance on 28 U.S.C. Section 1498 for the Government's own use.

- b) As discussed above, open source software is usually automatically licensed to a user on nonnegotiable terms. Accordingly, a contractor may accept the open source software license subjecting it to possible infringement liability; license or develop alternative software; obtain an authorization and consent clause if necessary and appropriate to shift the infringement liability to the Government; or rely on the doctrine of implied authorization and consent. If it seems necessary for the Government to authorize and consent to patent or copyright infringement for open source software, the Contracting Officer may consider granting the authorization. In the case of copyright, the Contracting Officer should consult legal counsel on the question of whether an express authorization and consent requires a Director of Defense Procurement and Acquisition Policy, Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) (OUSD(AT&L)DPAP) deviation approval in accordance with DFARS § 201.402(1)(ii) since there is no standard copyright authorization and consent clause.

vi. **Program Managers and Data Managers Actions**

Program Managers and Data Managers should know and understand what open source software is proposed for delivery or performance of work under the contract, what licenses govern the software, where software is to be used and whether the software has been or will be modified. This is true for all software, OSS or not. With this knowledge and understanding, Program Managers and Data Managers should evaluate use of the software (including open source software) in light of the issues discussed above. The following principles should guide Program and Data Managers:

- a) a license for a particular commercial computer software shall be compatible with all licenses for other commercial computer software that are or will be linked to, adapted to, integrated, combined or merged with the particular commercial computer software, including when the particular commercial computer software and the other commercial computer software are used with another computer program;
- b) a license for commercial computer software shall not impose a future Government distribution obligation that is foreseeable by the Contractor; and,
- c) a license for commercial computer software shall not be terminated by the Contractor's use of the commercial computer software in performing under the contract.

To record the due diligence described above, and to facilitate acceptance of open source software delivery, consider use of one of the H clauses in Chapter III under "Identification of Open Source Software (OSS) in contractor Deliverable Items."

vii. **Use of OSS in Performing Under a Contract**

Open source software may be proposed as part of a deliverable to the Government or merely proposed for use in performance but not delivery under a contract. In either case, Program Managers and Data Managers should take care that such use does not create Government obligations under the open source software licensing scheme. The following language is suggested for incorporation into procurement actions.

"Open source software is sometimes licensed under terms that require the user to make the user's modifications to the open source software or any software that the user 'combines' with

the open source software freely available in source code form. If the contractor uses open source software in the performance of a Government contract, it must ensure that the use thereof does not: (i) create, or purport to create, any Government distribution obligations with respect to the computer software deliverables; or (ii) grant, or purport to grant, to any third party any rights to or immunities under Government intellectual property or Government data rights to the Government computer software deliverables, unless in either case the Government affirms that it will accept delivery under those terms.

For example, the contractor may not develop a computer software deliverable using an open source program (including without limitation libraries) and non-commercial computer software program where such use results in a program file(s) that combines code from both the non-commercial computer software and open source software if the open source software is licensed under a license that requires any ‘modifications’ be made freely available unless the Government affirms that this is acceptable. Additionally, the contractor may not combine any non-commercial computer software deliverable with open source software licensed under the General Public License (GPL) or the Lesser General Public License (LGPL) in any manner where such use would cause, or could be interpreted or asserted to cause, the non-commercial computer software deliverable or any modifications thereto to become subject to the terms of the GPL or LGPL, unless the Government affirms that it will accept delivery under those terms.

Further, without express Government consent, the contractor may not use or incorporate open source software into a computer software deliverable to the Government if such use or incorporation would cause the Government to have to agree to license terms contrary to any law, including Federal procurement law, or otherwise risk use of such software without a license for all applicable copyrights.”

viii. **Additional Considerations When Using Open Source Software**

For additional information on Open Source Software, see DoD Free Open Source Software Community of Interest page at <http://dodcio.defense.gov/Home/Topics/UseofFreeOpenSourceSoftwareFOSS.aspx>, and the CENDI website at <http://www.cendi.gov>. A particularly useful source at CENDI

is the “Frequently Asked Questions about Copyright and Computer Software” (CENDI SW FAQ) at http://www.cendi.gov/publications/09-1FAQ_OpenSourceSoftware_FINAL_110109.pdf.

Security and information assurance considerations apply to all software including OSS. See DoD’s “Frequently Asked Questions regarding Open Source Software (OSS) and the Department of Defense DoD” Section 6 at <http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx> and CENDI SW FAQ 4.8 for additional information.

2. Releasing and Collaboratively developing OSS

The DoD Memorandum “Clarifying Guidance Regarding Open Source Software (OSS)” of 16 October 2009 explains that “software items, including code fixes and enhancements, developed for the Government should be released to the public (such as under an open source license) when all of the following conditions are met:

1. The project manager, program manager, or other comparable official determines that it is in the Government’s interest to do so, such as through the expectation of future enhancements by others.
2. The Government has the rights to reproduce and release the item, and to authorize others to do so. For example, the Government has public release rights when the software is developed by Government personnel, when the Government receives ‘unlimited rights’ in software developed by a contractor at Government expense, or when pre-existing OSS is modified by or for the Government.
3. The public release of the item is not restricted by other law or regulation, such as the Export Administration Regulations or the International Traffic in Arms Regulation, and the item qualifies for Distribution Statement A, per DoD Directive 5230.24.”

If the Government or its contractors take OSS and modify it, but do not submit those modifications back to the supplying OSS project, they risk creating a “project fork” (an independently-maintained project that started from a common source). Creating a project fork can cause substantial costs and delays when attempting to upgrade the OSS component, as those modifications may be difficult to re-integrate into updated versions from the OSS project. The problems

proliferate if multiple programs create independent project forks. Thus, it is often wise to submit modifications of OSS back to the OSS project, and encourage their incorporation; doing so can avoid many of these costs and delays.

For more information on how to collaboratively develop software as OSS in a military context, including a discussion of needed rights, see “Open Technology Development (OTD): Lessons Learned & Best Practices for Military Software” at <http://dodcio.defense.gov/Portals/0/Documents/FOSS/OTD-lessons-learned-military-signed.pdf>.

Appendix 6: GLOSSARY OF TERMS

Please Note: The definitions of the following terms are included as guidance for the Preparer and were compiled from the sources indicated in brackets and italics following each definition and were provided in this appendix for the user's convenience. It is not intended to be authoritative or comprehensive. For the definitions of additional terms or clarification of these definitions, please refer to the Defense Federal Acquisition Regulation Supplement (DFARS) and other source documents.

[Note to Preparers: *When citing regulations such as the DFARS and FAR, dates are included where possible to reflect the most recent version.. However, Contracting Officers and PMs need to check for current clause and clause dates before using the language in this Guidebook.*]

“Activity” is set of actions which, taken as a whole, transform inputs into outputs. [*IEEE/EIA Std. 12207/1997*]

“Application Programming Interface (API)” is a set of routines, protocols, and tools for building software applications. A good API makes it easier to develop a program by providing all the building blocks. A programmer then puts the blocks together. [*Source is Webopedia*]

“APP233/ISO 10303” – APP233 an “Application Protocol” for Systems Engineering that is based on the ISO 10303 Standard. AP233 is specific to Systems Engineering, but its purpose, like all of the 10303 standards, is to allow data exchange of SE models between tools -- it does not limit what “language” the tools use to represent a system. Neither is it meant to be a human-readable language, so using it directly for “tool neutrality” is not likely to work. ISO 10303 “is an International Standard for the computer-interpretable representation and exchange of industrial product data. The objective is to provide a mechanism that is capable of describing product data throughout the life cycle of a product, independent from any particular system. The nature of this description makes it suitable not only for neutral file exchange, but also as a basis for implementing and sharing product databases and archiving.” [*Source is Wikipedia*].

“Architecture” means the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution. [*Institute of Electrical and Electronics Engineers (IEEE) Std 1471-2000*]

“Artifact” is the result of any activity in the software life-cycle such as requirements, architecture model, design specifications, source code and test scripts. A piece of information that is used or produced by a software development process. An artifact can be a model, a description, or software. [*Source is informatics.umons.ac.be/genlog/SE/SE-contents.html*]

“Commercial component” means any component that is a commercial item. [*FAR §2.101(b)*]

“Commercial computer software” means any computer software that is a commercial item. [FAR 2.101; see also DFARS 252.227-7014(a)(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.]

“Commercial item” means:

- (1) Any item, other than real property, that is of a type customarily used by the general public or by non-governmental entities for purposes other than Governmental purposes, and:
 - (i) Has been sold, leased, or licensed to the general public; or
 - (ii) Has been offered for sale, lease, or license to the general public;
- (2) Any item that evolved from an item described in paragraph (1) of this definition through advances in technology or performance and that is not yet available in the commercial marketplace, but will be available in the commercial marketplace in time to satisfy the delivery requirements under a Government solicitation;
- (3) Any item that would satisfy a criterion expressed in paragraphs (1) or (2) of this definition, but for:
 - (i) Modifications of a type customarily available in the commercial marketplace; or
 - (ii) Minor modifications of a type not customarily available in the commercial marketplace made to meet Federal Government requirements. Minor modifications mean modifications that do not significantly alter the nongovernmental function or essential physical characteristics of an item or component, or

change the purpose of a process. Factors to be considered in determining whether a modification is minor include the value and size of the modification and the comparative value and size of the final product. Dollar values and percentages may be used as guideposts, but are not conclusive evidence that a modification is minor;

- (4) Any combination of items meeting the requirements of paragraphs (1), (2), (3), or (5) of this definition that are of a type customarily combined and sold in combination to the general public;
 - (5) Installation services, maintenance services, repair services, training services, and other services if:
 - (i) Such services are procured for support of an item referred to in paragraph (1), (2), (3), or (4) of this definition, regardless of whether such services are provided by the same source or at the same time as the item; and
 - (ii) The source of such services provides similar services contemporaneously to the general public under terms and conditions similar to those offered to the Federal Government;
 - (6) Services of a type offered and sold competitively in substantial quantities in the commercial marketplace based on established catalog or market prices for specific tasks performed or specific outcomes to be achieved and under standard commercial terms and conditions. For purposes of these services—
 - (i) “Catalog price” means a price included in a catalog, price list, schedule, or other form that is regularly maintained by the manufacturer or vendor, is either published or otherwise available for inspection by customers, and states prices at which sales are currently, or were last, made to a significant number of buyers constituting the general public; and
 - (ii) “Market prices” means current prices that are established in the course of ordinary trade between buyers and sellers free to bargain and that can be substantiated through competition or from sources independent of the Offerors.
 - (7) Any item, combination of items, or service referred to in paragraphs (1) through (6) of this definition, notwithstanding the fact that the item, combination of items, or service is transferred between or among separate divisions, subsidiaries, or affiliates of a contractor; or
 - (8) A non-developmental item, if the procuring agency determines the item was developed exclusively at private expense and sold in
-

substantial quantities, on a competitive basis, to multiple State and local governments. [*FAR Part 2.101(b)*]

“Commercial Off-the-Shelf (COTS)” or **“commercially available off-the-shelf item”** means an item that—

- (A) is a commercial item (as described in section 403 (12)(A) of this title);
- (B) is sold in substantial quantities in the commercial marketplace; and
- (C) is offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace. [*FAR Part 2.101(b)*]

“Community of Interest (COI)” means a collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes, and therefore must have shared vocabulary for the information it exchanges. [*DoD 8320-2*]

“Component” a subsystem, assembly, subassembly, or other major element of an end item. [*DAU Glossary of Defense Acquisition Acronyms and Terms, 14th Edition July 2011*]

“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. [DFARS 252.227-7014(a)]

“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. [DFARS 252.227-7014(a)(1)]

“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. [DFARS 252.227-7014(a)]

“Design Disclosure” means making data related to the design of a component, subsystem or system available to qualified recipients, with a goal of establishing and maintaining a process that will provide “early and often” design disclosure directly to the Government or to third-party contractors via Government-established access and the ability to download artifacts. This data is sufficient to allow the third party to develop and produce a competitive alternative. Design Disclosure can be enabled through a variety of mechanisms including keeping data, code and design artifacts in a repository either maintained by or

overseen by the Government such as the Navy's SHARE Repository made available through the Forge.mil Program (<http://www.forge.mil/>); providing the artifacts electronically upon requests made via the Government; or allowing requesting parties to obtain them directly from the source firm through a process involving review and approval from the Government. In addition, the Government can require that contractors allow the program to have continuous, real-time visibility and access to the development environment with access and the ability to download artifacts. Each program has the flexibility to establish the most appropriate mechanism for its specific needs; with a goal of establishing a process that is both cost-effective and responsive to requests.

“Domain (Software)” is a distinct functional area that can be supported by a class of software systems with similar requirements and capabilities. A domain may exist before there are software systems to support it. [*DAU Glossary of Acronyms and Terms, 14th Edition, July 2011*]

“Enterprise Architecture” represents the enterprise's key business, information, application, and technology strategies/trends and their impact on business functions and processes. [*Virginia Information Technologies Agency*]

“Evolving Architecture” are software development architectures that adopts changing customer needs and rapidly developing technologies. [*Carnegie Mellon University*]

“Firmware” is the combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device. The software cannot be readily modified under program control. [*DAU Glossary of Acronyms and Terms, 14th Edition, July 2011*]

“Full Design Disclosure” describes a continuum of data and software deliverables ranging from Form, Fit and Function data to detailed manufacturing and process data.

“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 for commercial purposes or authorize others to do so. [*DFARS §252.227-7013(a)(12)*]

“Government Purpose Rights” (GPR) means the rights to—

- (i) Use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction; and
- (ii) Release or disclose intellectual and technical data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data for United States Government Purposes. [DFARS §252.227-7013(a)(13)]

Note: In order for a software/technical data asset to be a viable Reuse Candidate, the Government must have at least Government Purpose Rights in the asset.

“Information Assurance” are information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. (Joint Publication 3-13) [DAU Glossary of Acronyms and Terms, 14th Edition, July 2011. Additional terms related to Information Assurance can be found in the *National Information Assurance Glossary* at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.]

“Integrated Product Team” a team composed of representatives from appropriate functional disciplines working together to build successful programs, identify and resolve issues, and make sound and timely recommendations to facilitate decision-making. There are three types of IPTs: Overarching IPTs (OIPTs) that focus on strategic guidance, program assessment, and issue resolution; Working level IPTs (WIPTs) that identify and resolve program issues, determine program status, and seek opportunities for acquisition reform; and Program-level IPTs (PIPTs) that focus on program execution and may include representatives from both government and industry after contract award. [DAU Glossary of Acronyms and Terms, 14th Edition, July 2011]

“Integrated Architecture” consists of multiple views or perspectives (Operational View (OV), Systems View (SV), Technical Standards View (TV) and All View (AV)) that facilitate integration and promote interoperability across capabilities and among related integrated architectures. [DoDAF]

“Integrated Digital Environment” implies an environment of connected knowledge workers, in which the preferred approach to performing work involves instantaneously accessing the required resources to accomplish the necessary tasks and then outputting the results into an instantaneously accessible form. Information sharing is

rewarded, and redundant data development, transmission or storage is frowned upon. The goal of developing an IDE is intended to improve current and future overall operational performance.

DoD policy requires the maximum use of digital operations throughout the system life cycle. The program IDE is part of the larger DoD IDE. It should keep pace with evolving automation technologies and provide ready access to anyone with a need-to-know, as determined by the Program Manager.

Program Managers should establish a data management system within the IDE that allows every activity involved with the program to cost-effectively create, store, access, manipulate, and exchange digital data. This includes, at minimum, the data management needs of the system engineering process, modeling and simulation activities, test and evaluation strategy, support strategy, and other periodic reporting requirements. [<https://acc.dau.mil/CommunityBrowser.aspx?id=24420>]

“Interoperability” The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information Technology (IT) and National Security System (NSS) interoperability includes both the technical exchange of information and the operational effectiveness of that exchanged information as required for mission accomplishment. (CJCSI 6212.01E)

[*DAU Glossary of Defense Acquisition Acronyms and Terms, 14th Edition*]

“Invention” means any invention or discovery which is or may be patentable or otherwise protectable under Title 35 of the United States Code or any novel variety of plant that is or may be protectable under the Plant Variety Protection Act (7 U.S.C. Section 2321, et seq.). [*FAR Section 52.227-13*]

“Layered” means a system in which components are grouped, i.e., layered, in a hierarchical arrangement, such that lower layers provide functions and services that support the functions and services of higher layers. Note: Systems of ever-increasing complexity and capability can be built by adding or changing the layers to improve overall system capability while using the components that are still in place. [*The Alliance for Telecommunications Industry Solutions (ATIS) web site, <http://www.atis.org>.*]

“Lead Systems Integrator” has no official definition in the DoD 5000 series or FAR/DFARS. The generally accepted meaning of systems integrator is:

Systems Integrator – A prime contractor, working with other associates or associate prime contractors on a system, whose function is total responsibility for integrating the products/processes/subsystems/components of the associates or associate prime contractors into the total system. This contractor may have been awarded a separate contract for the integration effort or it could be part of the contract for its part of the system being acquired. This contractor does not necessarily have to have a separate product/process/ subsystem/component of the system to be the systems integrator. The systems integrator may also be the government. [*Defense Systems Management College*]

The Office of the Undersecretary of Defense (Acquisition, Test and Logistics) in a Memorandum entitled “Limitations on contractors Acting as Lead Systems Integrators” dated 18 January 2007 provided the following definitions:

“Lead system integrator with system responsibility” means a prime contractor for the development or production of a major system if the prime contractor is not expected at the time of award to perform a substantial portion of the work on the system and the major subsystems.

“Lead system integrator without system responsibility” means a contractor under a contract for the procurement of services whose primary purpose is to perform acquisition functions closely associated with inherently governmental functions with regard to the development or production of a major system.

“Life Cycle Model” in the context of the development, operation, and maintenance of a software product, a life cycle model is a defined set of processes, activities, and tasks, and their sequencing and interrelationships, spanning the life of the system from its definition to the termination of its use. [*IEEE/EIA Std. 12207/1997*]

“Limited Rights” (LR) 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 limited rights, release or disclose the technical data outside the Government, use the technical data for manufacture, or authorize the technical data to be used by another party, except that the Government may reproduce, release, or disclose such data or authorize the use or reproduction of the data by persons

outside the Government if certain conditions are met. [DFARS §252.227.7013(a)]

“Maintainability” is the ability of an item to be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. See Mean Time to Repair (MTTR). [DAU Glossary of Acronyms and Terms, 14th Edition, July 2011]

“Markings” refers to software and other Intellectual Property Rights (IPRs) legends, Distribution Statements, security classifications, and appropriate export control Statements. It is important that Program Managers review the markings of all deliverables prior to acceptance to ensure that the Government will obtain the IPRs it has contracted for.

“Method/Technique” – The approach used to accomplish the task. [IEEE/EIA Std. 12207/1997]

“Middleware” – Middleware provides an ability to separate software components from a specific environment (e.g. a specific operating system) and allows those applications to be hosted into different environments in the future. Middleware is a technology that eases the integration and upgrades of supporting technology (e.g. hardware refresh) and reuse of those applications in other environments. Middlewares achieve this by (1) allocating communication protocols from the application layer into a system-wide managed resource and (2) providing common (ideally, open-standards-based) component interfaces that decouple software from specific communication methods and operating environments.

[<http://www.dre.vanderbilt.edu/~schmidt/PDF/middleware-encyclopedia.pdf>]

“Module” An independently compilable software component made up of one or more procedures or routines or a combination of procedures and routines. [DAU Glossary of Acronyms and Terms, 14th Edition, July 2011]

“Modular Contracting” is a contracting approach under which the need for a system is satisfied in successive acquisitions of interoperable increments. Each increment complies with common or commercially acceptable standards applicable to information technology (IT) so that the increments are compatible with the other increments of IT comprising the system. [Glossary of Defense Acquisition Acronyms & Terms, 14th Edition, June, 2011]

“Modular Design” means a design (organization) where functionality is partitioned into discrete, cohesive, and self-contained units with well-

defined, open and published interfaces that permit substitution of such units with similar components or products from alternate sources with minimum impact on existing units. [*A Modular Open Systems Approach (MOSA) to Acquisition document, (USD(AT&L)) OSJTF*]

“Modular Open Systems Approach or MOSA” is the DoD’s implementation of Open Systems. Within the MOSA context, programs should design their system based on adherence to the following five MOSA principles:

Establish an Enabling Environment;
Employ Modular Design;
Designate Key Interfaces;
Use Open Standards; and
Certify Conformance.

[*A Modular Open Systems Approach (MOSA) to Acquisition, OSJTF*]

“National Security Systems (NSS)” are any telecommunications or information systems operated by an agency or by a contractor of an agency-- (i) the function, operation, or use of which involves intelligence activities; cryptologic activities related to national security; the command and control of military forces; equipment that is an integral part of a weapons system; or criticality to the direct fulfillment of military or intelligence missions, which does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [*44 U.S.C. § 3542(b)(2)*]

“Open Architecture” means a type of architecture whose specifications are made public by its designers which allows users to make modifications to various components. [*ITtoolbox*]

Note: “Openness” can be thought of in degrees, based on the level and scope of the information provided (for example, both internal and external information on interfaces) and its availability to third parties (e.g., either to a select few or to a broad range of potential component providers).

“Open Interface” is a public standard for connecting hardware to hardware and software to software. With regard to hardware, it implies that there is more than one brand of product that can be hooked up to the device with the open interface. In the case of software, it implies that more than one program exists to interface with the application that has the open interface or that a program can be readily written to

communicate with it. See open system and open standard. [*Source is PC Magazine Encyclopedia.*]

“Open Source Software” is computer software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by the users of that software.

[“Clarifying Guidance Regarding Open Source Software (OSS),” DoD CIO, 2009]. Readers may also want to refer to the definition developed by the Open Source Initiative (<http://www.opensource.org>) and the definition of “free software” developed by the Free Software Foundation (<http://www.fsf.org>).

“Open Standards” means widely accepted and supported standards set by recognized standards organizations or the marketplace. These standards support interoperability, portability, and scalability and are equally available to the general public at no cost or with a moderate license fee. [*Glossary of Defense Acquisition Acronyms & Terms, 14th Edition, June 2011*]

“Open System” means a system that employs modular design tenets, uses widely supported and consensus based standards for its key interfaces, and is subject to validation and verification tests to ensure the openness of its key interfaces. [*A Modular Open Systems Approach (MOSA) to Acquisition, OSJTF*]

“Open Systems Approach” means an integrated business and technical strategy that employs a modular design and, where appropriate, defines key interfaces using widely supported, consensus-based standards that are published and maintained by a recognized industry standards organization. [*A Modular Open Systems Approach (MOSA) to Acquisition, OSJTF*]

“Open System Architecture” is a system that employs modular design, uses widely supported and consensus based standards for its key interfaces, and has been subjected to successful validation and verification tests to ensure the openness of its key interfaces. [*A Modular Open Systems Approach (MOSA) to Acquisition, OSJTF*] An open architecture is defined as a technical architecture that adopts open standards supporting a modular, loosely coupled and highly cohesive system structure that includes publishing of key interfaces within the system and full design disclosure. The key enabler for open architecture is the adoption of an open business model which requires doing business in a transparent way that leverages the collaborative innovation of numerous participants across the enterprise permitting shared risk, maximized asset reuse and reduced total ownership costs. The combination of open architecture and an open business model permit the acquisition of Open Systems Architectures that yield

modular, interoperable systems allowing components to be added, modified, replaced, removed and/or supported by different vendors throughout the life cycle in order to drive opportunities for enhanced competition and innovation.

The following are the core principles of the Open Systems Architecture approach:

1. Modular designs with loose coupling and high cohesion that allow for independent acquisition of system components, i.e., composability;
2. Continuous design disclosure and appropriate use of data rights allowing greater visibility into an unfolding design and flexibility in acquisition alternatives;
3. Enterprise investment strategies that maximize reuse of system designs and reduce total ownership costs (TOC);
4. Enhanced transparency of system design through Government, academia, and industry peer reviews;
5. Competition and collaboration through development of alternative solutions and sources; and
6. Analysis to determine which components will provide the best return on investment (ROI) to OSA, i.e., which components will change most often due to technology upgrades or parts obsolescence and have the highest associated cost over the life cycle.

Achievement of these six principles requires an affirmative answer to a fundamental question: *Can a qualified third party add, modify, replace, remove, or provide support for a component of a system, based on open standards and published interfaces for the component of that system?*

[Note to Preparer: *This definition is from the Department of Defense' Better Buying Power (BPP) website – a restricted access website located at: <https://acc.dau.mil/bbp>. External parties currently have to apply for access to the Government-only BPP site through this link.]*

“Peer Review” Independent management reviews of supplies and services contracts. Pre-award reviews are conducted on supplies and services contracts; post-award reviews are conducted on services contracts. The Director, Defense Procurement, Acquisition Policy and Strategic Sourcing (DPAP), in the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)), conducts peer reviews for contracts with an estimated value of \$1 billion or more (including options). DoD components conduct peer

reviews for contracts valued at less than \$1 billion. [*DAU Glossary of Acronyms and Terms, 14th Edition, July 2011*]

“Performance-Based Logistics/Performance-Based Life Cycle Product Support (PBL)” is an outcome-based product support strategy that plans and delivers an integrated, affordable, performance solution designed to optimally balance readiness and Life-Cycle Costs (LCCs) by leveraging public and private industrial base capabilities. DoDI 5000.02 introduced the term. Product-Based Life Cycle Product Support as the latest evolution of Performance-Based Logistics and states that both terms can be referred to as “PBL.” [DoDI 5000.02 and *DoD Product Support Manager’s Guidebook*]

“Portability” is the software codebase feature to be able to reuse the existing code instead of creating new code when moving software from an environment to another. [*Wikipedia*]

“Practical application” means to manufacture in the case of a composition or product, to practice in the case of a process or method, or to operate in the case of a machine or system; and, in each case, under such conditions as to establish that the invention is being utilized and that its benefits are, to the extent permitted by law or Government regulations, available to the public on reasonable terms. [*FAR Section 52.227-13*]

“Process” is a set of interrelated activities designed to accomplish a specified goal. IEEE/EIA Std. 12207/1997 Table 1 lists all 12207 processes and their associated activities. For example *Development* is a process. Within *Development* there are thirteen activities as shown in Table 1. One of these activities is *Software Coding and Testing* which has five tasks. [*IEEE/EIA Std. 12207/1997*]

“Reliability” is the probability of an item to perform a required function under stated conditions for a specified period of time. Reliability is further divided into mission reliability and logistics reliability. [*DoD Guide to Achieving Reliability Achievability and Maintainability (RAM, 5 Aug 2005)*]

“Reconfigurability” means that a system or a service’s state and behavior can be dynamically modified during its operation. [*University of Athens, Communications Networks Laboratory*]

“Reusability” is the degree to which a software module or other work product can be used in more than one computing program or software system. [*IEEE*]

“Restricted Rights” (RR) apply only to noncommercial computer software and mean the Government’s rights to: use a computer program; transfer a computer program to another Government agency;

make the minimum number of copies required; modify computer software required for urgent tactical situations; disclose the computer software to authorized person(s) in the performance of Government contracts that contain the clause at 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends. [DFARS §252.227-7014(a)(15)]

[**Note to Preparer:** *This definition is abbreviated from DFARS 252.227-7013 and DFARS 252.227-7014), and provisions therein must be adhered to when preparing and executing contracts.*]

“Scalability” is the capability of a piece of hardware or software to easily expand to meet future computing needs. [Microsoft TechNet]

“Small business concerns” means a Concern, including its affiliates, which is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria and size standards in 13 CFR part 121. [FAR Section 2.101]

“Software Architecture” of a program or computing system is the structure or structures of the system, which comprise software elements, the externally visible properties of these elements, and the relationships among them. [IEEE]

“Software Intensive System” is a system in which software represents the largest segment in one or more of the following criteria: system development cost, system development risk, system functionality, or development time. [DAU Glossary of Acronyms and Terms, 14th Edition, July 2011]

“Software Reuse” is the process of implementing or updating software systems using existing software assets. [DAU Glossary of Acronyms and Terms, 14th Edition, July 2011] The DoD 5000.1 Acquisition Guidebook states that the “Program Manager should base software systems development on robust systems engineering principles. The following best practices for software systems also apply in general to any system, “... Identifying and exploiting, where practicable, Government and commercial software reuse opportunities before developing new software.” Potential software assets include:

- 1) **Computer Software** - Computer programs, procedures, and possibly associated documentation and data, pertaining to the operation of a computer system.
- 2) **Software Development Plan (SDP)** – A management plan usually generated by the developer describing in detail the processes, activities, and tasks to be performed to accomplish the software development effort.

- 3) **Computer Software Documentation** – Technical Data (TD) information, including computer listings and printouts, that documents the requirements, design, or details of computer software, explains the capabilities and limitations of the software, or provides operation instructions for using or supporting computer software during the software's operational life.
- 4) **Software Product Specification** – Detailed design and description of Software Items (SIs) comprising the product baseline. Analogous to the Item Detail Specification of a hardware Configuration Item (CI) in the product baseline of a hardware system.
- 5) **Software Requirement Specification (SRS)** – A description of the requirements (behaviors, functions, performance, design constraints and attributes) allocated to a specific Software Configuration Item (SCI). Often accompanied by an Interface Requirements Specification (IRS) for that SCI.
- 6) **Software Specification Review (SSR)** – A life cycle review of the requirements specified for one or more Software Configuration Items (SCIs) to determine whether they form an adequate basis for proceeding into preliminary design of the reviewed item. See Software Requirement Specification (SRS) and Interface Requirement Specification (IRS).
- 7) **Interface Requirement Specification (IRS)** - A type of Item Performance Specification that defines the required software interfaces for a given Software Item (SI) in the allocated baseline, the requirements for which are described by a Software Requirements Specification (SRS). The IRS is frequently combined with the SRS.
- 8) **Computer Software Component (CSC)** - Under some software development standards, a functional or logically distinct part of a Computer Software Configuration Item (CSCI), or Software Configuration Item (SCI).
- 9) **Software Item (SI)** – An aggregation of software, such as a computer program or database that satisfies an end use function and is designated for purposes of specification, qualification, testing, interfacing, Configuration Management (CM), or other purposes. An SI is made up of Computer Software Units (CSUs).
- 10) **Software Resources Data Report (SRDR)** - SRDR is intended to improve the ability of the DoD to estimate the

costs of software intensive programs. SRDR reporting is required by DoD Instruction 5000.2, Enclosure 3, for major contracts and sub-contracts (regardless of contract type) associated with high-cost software elements within Acquisition Category I and Acquisition Category IA programs. Data collected from applicable contracts include type and size of the software application(s), schedule, and labor resources needed for the software development.

- 11) **Analysis of Alternatives** - The evaluation of the performance, operational effectiveness, operational suitability, and estimated costs of alternative systems to meet a mission capability. The analysis assesses the advantages and disadvantages of alternatives being considered to satisfy capabilities, including the sensitivity of each alternative to possible changes in key assumptions or variables. The Analysis of Alternatives (AoA) is normally conducted during the Concept Refinement phase of the Defense Acquisition Framework and the results of the AoA align with the system concept contained in the Initial Capabilities Document (ICD) approved prior to Milestone A.
- 12) **Initial Capabilities Document** – Summarizes a Capabilities-Based Assessment (CBA) and recommends materiel or non-materiel approaches or a combination of materiel and non-materiel approaches to satisfy specific capability gaps. It identifies required capabilities and defines capability gap(s) in terms of the joint capability area, the relevant range of military operations; desired effects; time; Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF); and policy implications and constraints. The ICD summarizes the results of DOTMLPF and policy analysis and the DOTMLPF approaches that may deliver the required capability. The outcome of an ICD could be one or more Joint DOTMLPF Change Recommendations (DCRs) or recommendations to pursue materiel solutions. (CJCSI 3170.01G and *JCIDS Manual*)
- 13) **Systems Engineering Plan** - A description of the program's overall technical approach including processes, resources, metrics, applicable performance incentives, and the timing, conduct, and success criteria of technical reviews.
- 14) **Test and Evaluation Master Plan** - Documents the overall structure and objectives of the Test and Evaluation (T&E) program. It provides a framework within which to generate

detailed T&E plans and it documents schedule and resource implications associated with the T&E program. The TEMP identifies the necessary Developmental Test and Evaluation (DT&E), Operational Test and Evaluation (OT&E), and Live Fire Test and Evaluation (LFT&E) activities. It relates program schedule, test management strategy and structure, and required resources to: Critical Operational Issues (COIs), Critical Technical Parameters (CTPs), objectives and thresholds documented in the Capability Development Document (CDD), evaluation criteria, and milestone decision points. For multi-service or joint programs, a single integrated TEMP is required. Component-unique content requirements, particularly evaluation criteria associated with COIs, can be addressed in a component-prepared annex to the basic TEMP. [DAU Glossary of Acronyms and Terms, 14th Edition, July 2011]

- 15) **Capability Development Document** - A document that captures the information necessary to develop a proposed program(s), preferably using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable, and technically mature capability. The CDD supports a Milestone B decision review.
- 16) **Acquisition Program Baseline** - Baseline that reflects the threshold and objective values for the minimum number of cost, schedule, and performance attributes that describe the program over its life cycle. Cost values reflect the Life Cycle Cost Estimate (LCCE); scheduled dates include key activities such as milestones and the Initial Operational Capability (IOC); and performance attributes reflect the operational performance required for the fielded system. Key Performance Parameters (KPPs) from the Capability Development Document (CDD) and Capability Production Document (CPD) are copied verbatim into the APB. The Key System Attributes (KSAs) from the CDD and CPD that support the Sustainment KPP are also reflected in the APB. Other significant performance parameters may be added by the Milestone Decision Authority (MDA). See Key Performance Parameters (KPPs), Key System Attributes (KSAs), and Initial Operational Capability (IOC). (*Defense Acquisition Guidebook* and *JCIDS Manual*)

- 17) **Training Plan** – Outlines the level of learning required to adequately perform the responsibilities designated to the function and accomplish the mission assigned to the system.

[DoD 5000.1 Acquisition Guidebook]

“Subject Invention” means any invention of the Contractor made in the performance of work under a contract. [FAR Section 52.227-11]

“System Architecture” is the composite of the design architectures for products and their life cycle processes. [IEEE 1220-1998]

“Tasks” are specific actions performed to accomplish an activity. The way that each task is performed, such as testing, is called the technique or method. [IEEE/EIA Std. 12207/1997]

“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. [DFARS 252.227-7013(a)(15)]

“Technology Insertion” is increasing a system’s or product’s Warfighting operational capability by integrating new capabilities or upgrading the system’s current capabilities with up-to-date and more capable COTS or custom technologies. [Software Engineering Institute]

“Upgradeability” is the ease with which a system or component can be modified to take advantage of new software or hardware technologies. [Software Engineering Institute]

“Unlimited rights” (UL) means rights to use, modify, reproduce, perform, display, release, or disclose technical data in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so. [DFARS Section 252.227-7013(a)(16)]

“Vendor lock-in” or just **“lock-in”**, is the situation in which customers are dependent on a single manufacturer or supplier for some product (i.e., a good or service), or products, and cannot move to another vendor without substantial costs and/or inconvenience. This dependency is typically a result of standards that are controlled by the vendor (i.e., manufacturer or supplier). It can grant the vendor some extent of monopoly power and can thus be much more profitable than would be the absence of such dependency.

[http://www.lininfo.org/vendor_lockin.html] referenced in [http://cio-nii.defense.gov/sites/oss/Open Source Software %28OSS%29 FAQ.htm](http://cio-nii.defense.gov/sites/oss/Open_Source_Software_%28OSS%29_FAQ.htm)]

Appendix 7: ASSESSING A PROGRAM'S INTELLECTUAL PROPERTY RIGHTS NEEDS AND DEVELOPING A TECHNICAL DATA RIGHTS STRATEGY (TDRS)

Goals: Programs should work within their PEOs and across their Communities of Interest in considering their life cycle needs for data and data rights in a structured, focused manner in an effort to develop a Technical Data Rights Strategy (TDRS). The TDRS addresses both technical data and computer software.

DoD Instruction 5000.02, dated December 2, 2008, directed programs to take a number of steps related to identifying and managing their intellectual property. The following is a summary of these requirements:

- a. Program Managers for Acquisition Category (ACAT) I and II programs, regardless of planned sustainment approach, shall assess the long-term technical data and computer software data needs of their systems and reflect that assessment in a Technical Data Rights Strategy. The TDRS shall:
 - i. Be integrated with other life cycle sustainment planning and included in the Acquisition Strategy (AS).
 - ii. Assess the data required to design, manufacture and sustain the system as well as to support re-competition for production, sustainment or upgrade.
 - iii. Address the merits of including a priced contract option for the future delivery of data and data rights not acquired upon initial contract award and shall consider the contractor's responsibility to verify any assertion of restricted use and release of data.

The TDRS shall be approved in the context of the AS prior to issuing a contract solicitation. A summary of the TDRS is contained in section 7.6 of the program Technology Development Strategy (TDS) and AS.⁴⁹ Subsequent language included in DFARS 207.106 (S-70), Additional Requirements for Major Systems, specifically states:

(S-70)(1) In accordance with Section 802(a) of the National Defense Authorization Act for Fiscal Year 2007 (Pub. L.

⁴⁹ http://www.acq.osd.mil/ic/IAF%20XXX%20Briefings%203%20June%202011/TDS_AS_Outline-04-20-2011.pdf

109-364) and DoD policy requirements, acquisition plans for major weapon systems and subsystems of major weapon systems shall—

- (i) Assess the long-term technical data and computer software needs of those systems and subsystems; and
 - (ii) Establish acquisition strategies that provide for the technical data and computer software deliverables and associated license rights needed to sustain those systems and subsystems over their life cycle. The strategy may include—
 - (A) The development of maintenance capabilities within DoD; or
 - (B) Competition for contracts for sustainment of the systems or subsystems.
- (2) Assessments and corresponding acquisition strategies developed under this section shall—
- (i) Be developed before issuance of a solicitation for the weapon system or subsystem;
 - (ii) Address the merits of including a priced contract option for the future delivery of technical data and computer software, and associated license rights, that were not acquired upon initial contract award;
 - (iii) Address the potential for changes in the sustainment plan over the life cycle of the weapon system or subsystem; and
 - (iv) Apply to weapon systems and subsystems that are to be supported by performance-based logistics arrangements as well as to weapon systems and subsystems that are to be supported by other sustainment approaches.

The goal of this assessment is to identify opportunities or requirements for information and information product sharing as well as “the long-term technical data (and computer software) needs of their systems” and then to structure contracts accordingly. Such an assessment should include both a cross-Domain and enterprise-wide review of the component “marketplace” – both supply and demand. The results of this analysis should guide the program in determining the data and data rights that it will require the contractor to deliver in addition to competitively priced options for additional technical data, computer software, and other IPR. For example, the Navy’s policy is to accept

only data products with GPR or less restrictive rights for incorporation in its data or software repositories/libraries. **[Note to Preparers:** *The definitions of technical data, computer software, and computer software documentation are found in DFARS 252.227-7013 and also in this Guidebook. The tables included in this Appendix summarize the different characteristics of each Rights Category along with criteria for their application.*]

[Note to Preparers: *When citing regulations such as the DFARS and FAR, dates are included where possible to reflect the most recent version of this Guidebook. However, Contracting Officers and PMs need to check for current clause dates before using the language in this Guidebook.*]

Additional guidance on data, data rights and data management issues is available from a Naval Sea Systems Command manual entitled NAVSEA SL150-AA-PRO-010/DMP, *Operations and Procedures Manual for Contractor Prepared Data*. The manual can be accessed via the NAVSEA Technical Data Management Information System (TDMIS): <https://nstdsa.nmci.navy.mil>. Another resource is *Acquiring and Enforcing the Government's Rights in Technical Data and Computer Software Under Department of Defense Contracts: A Practical Handbook for Acquisition Professionals* found at <https://acc.dau.mil/adl/en-US/431675/file/60335/Technical%20Data%20and%20Computer%20Software%20Rights%20Handbook%204th%20Edition.pdf>. This handbook is designed to provide you with a practical "cradle-to-grave" handbook to acquiring technical data and computer software rights.

[Note to Preparers: *When reviewing a contract, first determine whether it is primarily for commercial items or noncommercial items. This will typically be apparent from the contract cover sheet - the SF-33 form is used for noncommercial procurements and the SF-1449 is used for commercial item procurements. Images of blanks of both forms are available in FAR Part 53.3, and at <http://www.gsa.gov/portal/forms/type/TOP>. If you are in doubt whether commercial or noncommercial data or software is being acquired, it is helpful to review the definition of "commercial item" at FAR 2.101.*]

[Note to Preparers: *The program TDRS and directive documentation should specify that anything that the Government paid 100% of the cost to develop is available for delivery to the Government with all of the developmental artifacts and unlimited usage rights, and anything the Government contributed any amount of funding to develop should be available for delivery to the Government with at least Government Purpose usage rights. In addition, the Program Manager should*

require that the deliverables be provided to (or deposited in) the appropriate repository (if established), such as the Navy's SHARE repository or those made available through the DoD's Forge.mil Program (<http://www.forge.mil/>).

[Note to Preparers: DFARS 252.227-7017 requires that proposals include a table identifying and asserting use, release or disclosure restrictions claimed against the Government. To help clearly understand the data rights to be provided to the Government, the table should identify the technical data or software item subject to restrictions with the associated CDRL.]

- a. The basic question a data rights assessment tries to answer is: Will we be able to acquire from contractors the technical data and level of associated data rights we need to support the planned technology development, acquisition and logistics support strategies? Specific details the data rights assessment should address include the following:
 - i. Does the Government already have data rights in existing technical data, software or other deliverables that permit the Government to leverage that existing data or software for this new contracting effort?
 - ii. Will obtaining more than restricted/limited rights increase competition and lower life cycle costs? In general, the Government cannot "require" a higher level of data rights than what we are legally entitled without some form of compensation.
 - iii. Will the Government obtain at least Government Purpose Rights? If not, what is the impact upon the program AS and logistics strategies due to not being able to provide this data to contractors other than the OEM ? What is the justification for more restrictive rights than GPR?
 - iv. Does the program require the rights to modify (update, correct, enhance, etc.) the data or software deliverables now or in the future?
 - v. Will the program need to maintain configuration control over the deliverables?
 - vi. Does the Government need to have the ability to provide the information to third parties? If so, should the Government negotiate a special license for this right?
- b. There are some important points to consider when performing a data rights assessment:

- i. Data rights issues are complex and require careful examination of the program's requirements, strategies, and overall "fit" within the Enterprise.
- ii. Use proper experts to review program data rights requirements – strategy development should involve an intellectual property lawyer, a contracting officer, functional subject matter experts and the Program Manager.
- iii. It is typically very expensive to acquire a broader level of data rights or to create additional options for software maintenance after the initial contract is in place.
- iv. Insufficient data rights prevent the Government from using data and software deliverables in the most optimal way.
- v. Remember that data rights will impact weapon system sustainment and maintenance over 30 or more years of its life.

It is important to remember that assessing data and data rights needs should be done in the context of evaluating alternatives for the program technology development, acquisition and logistics support strategies. The business case analyses (BCA) conducted to select those program strategies should consider whether obtaining the desired rights is the correct business decision.

[Note to Preparer: *The following tables summarize the different characteristics of each data rights category along with criteria for their application. The definitions of technical data, computer software, and computer software documentation found in DFARS 252.227-7013 and -7014 should be referred to as the primary source of information for developing the contract language.*]

[Note to Preparers: *Distribution Statements required by DoD Instruction 5230.24 do not correlate directly to specific data rights categories and vice versa. Data rights allocate the intellectual property interests of both Government and industry according to the type of data, the use of the data, and the source of funding for the technology reflected in the deliverable. Distribution Statements may be based upon a number of additional restrictions including information security and export control. There are scenarios where a DoD program would have Unlimited Rights in a deliverable, but would not want to authorize uncontrolled distribution of the deliverable because of such other restrictions and these would be reflected in Distribution Statement limitations. Conversely, a Limited Rights deliverable might have no security or export control reasons for limited distribution. However, since the deliverable was delivered with Limited Rights, the DoD program cannot distribute the deliverable outside the Government generally without the developing contractor's written permission.*]

The reader should refer to the table and explanatory material contained in Appendix 9 that was developed for the “Better Buying Power: Understanding and Leveraging Data Rights in DoD Acquisitions” pamphlet. This document is available in its entirety at <https://acc.dau.mil/CommunityBrowser.aspx?id=436677&lang=en-US>.

Other Sources of Information about Intellectual Property Rights:

The Defense Federal Acquisition Regulation Supplement (DFARS) is the primary source of information regarding DoD data and intellectual property rights. Applicable FAR/DFARS data rights clauses are as follows:

FAR
52.227-1 Authorization and Consent
52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement
52.227-3 Patent Indemnity
52.227-6 Royalty Information
52.227-11 Patent Rights—Ownership by the contractor
52.227-13 Patent Rights—Ownership by the Government

NOTE: “DFARS 227.304-1 General” permits contractors to submit invention reports on “DD Form 882.” Suggest that the RFP, the Contract and any subcontracts include using the DD Form 882 to comply with the reporting requirement stated in FAR 52.227-11, FAR 52.227-12, DFARS 252.227-7038 and DFARS 252.227-7039.

DFARS
252.227-7004 License Grant
252.227-7006 License Grant—Running Royalty
252.227-7010 License to Other Government Agencies
252.227-7013 Rights in Technical Data—Noncommercial Items
252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation
252.227-7015 Technical Data—Commercial Items
252.227-7016 Rights in Bid or Proposal Information
252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions
252.227-7018 Rights in Noncommercial Technical Data and Computer Software—Small Business Innovation Research (SBIR) Program

DFARS

252.227-7019 Validation of Asserted Restrictions—Computer Software
252.227-7025 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends
252.227-7027 Deferred Ordering of Technical Data or Computer Software
252.227-7028 Technical Data or Computer Software Previously Delivered to Government
252.227-7030 Technical Data—Withholding of Payment
252.227-7037 Validation of Restrictive Markings on Technical Data
252.227-7038 Patent Rights—Ownership by the Contractor (Note: Large Business)
252.227-7039 Patents—Reporting of Subject Inventions

Type of Contract: Engineering Services Requiring Delivery of Data

FAR

52.227-1 Authorization and Consent
52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement
52.227-3 Patent Indemnity
52.227-11 Patent Rights—Ownership by the contractor

DFARS

252.227-7013 Rights in Technical Data—Noncommercial Items
252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation
252.227-7016 Rights in Bid or Proposal Information
252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions
252.227-7019 Validation of Asserted Restrictions—Computer Software
252.227-7025 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends
252.227-7028 Technical Data or Computer Software Previously Delivered to Government
252.227-7030 Technical Data—Withholding of Payment
252.227-7037 Validation of Restrictive Markings on Technical Data
252.227-7038 Patent Rights—Ownership by the Contractor (Note: Large Business)
252.227-7039 Patents—Reporting of Subject Inventions

Type of Contract: Support Contracts Not Requiring the Delivery of Data

FAR

52.227-1 Authorization and Consent

52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement

52.227-11 Patent Rights—Ownership by the contractor

DFARS

252.227-7025 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends

252.227-7038 Patent Rights—Ownership by the Contractor (Note: Large Business)

252.227-7039 Patents—Reporting of Subject Inventions

Type of Contract: Commercial Goods-Technical Data

FAR

52.227-3 Authorization and Consent

52.227-11 Patent Rights—Ownership by the contractor

DFARS

252.227-7015 Technical Data—Commercial Items

252.227-7037 Validation of Restrictive Markings on Technical Data

Type of Contract: Noncommercial Goods-Technical Data

FAR

52.227-1 Authorization and Consent

52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement

52.227-11 Patent Rights—Ownership by the contractor

DFARS

252.227-7013 Rights in Technical Data—Noncommercial Items

252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation

252.227-7016 Rights in Bid or Proposal Information

252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions

252.227-7019 Validation of Asserted Restrictions—Computer Software

DFARS

252.227-7025 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends

252.227-7028 Technical Data or Computer Software Previously Delivered to Government

252.227-7030 Technical Data—Withholding of Payment

252.227-7037 Validation of Restrictive Markings on Technical Data

252.227-7038 Patent Rights—Ownership by the Contractor (Note: Large Business)

252.227-7039 Patents—Reporting of Subject Inventions

Type of Contract: Noncommercial Goods – No Technical Data Required

FAR

52.227-1 Authorization and Consent

52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement

DFARS

252.227-7025 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends

Type of Contract: Small Business Innovation Research (SBIR)

FAR

52.227-1 Authorization and Consent

52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement

52.227-11 Patent Rights—Ownership by the contractor

DFARS

252.227-7016 Rights in Bid or Proposal Information

252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions

252.227-7018 Rights in Noncommercial Technical Data and Computer Software – Small Business Innovation Research (SBIR) Program

252.227-7019 Validation of Asserted Restrictions—Computer Software

252.227-7025 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends

252.227-7028 Technical Data or Computer Software Previously Delivered to Government

252.227-7030 Technical Data—Withholding of Payment

DFARS

252.227-7037 Validation of Restrictive Markings on Technical Data

252.227-7039 Patents—Reporting of Subject Inventions

Type of Contract: Vessel Design

DFARS

252.227-7015 Technical Data—Commercial Items – Alternative 1.

The table that follows may be useful when reviewing a proposal to make sure that the appropriate clauses are included:

FAR/ DFARS PATENT, TECHNICAL DATA, AND COMPUTER SOFTWARE CLAUSES

TD = TECHNICAL DATA CS = COMPUTER SOFTWARE ICP = ITEM, COMPONENT, OR PROCESS
CSD = COMPUTER SOFTWARE DOCUMENTATION = TD

When to Incorporate Clauses/Provisions	252.227-	7013	7014	7015	7016	7017	7019	7028	7030	7037
Mandatory if TD for noncommercial ICP is to be delivered		X			X	X		X	X	X
Mandatory if noncommercial CS is to be delivered			X		X	X	X	X		
Mandatory if TD for commercial items is to be delivered			X							X
Strongly recommended in all solicitations		X	X	X	X	X	X	X	X	X
Strongly recommended in all contracts		X	X	X	X	X	X	X	X	X

SPECIFIC CLAUSES & THEIR USE (SEE DFARS FOR TITLES):

- 252.227-7018 - All SBIR contracts. (Do not use -7013 or -7014.)
- 252.227-7025 - All if access to less than unlimited rights TD/CS is anticipated. Strongly recommended in all contracts.
- 252.227-7026 - Voluntary clause used only to specifically identify at award TD & CS which may be ordered later.
- 252.227-7027 - Voluntary clause used to order additional deliverables for TD & CS "generated" during performance of the instant contract. Strongly recommended in all solicitations and contracts.
- 52.227-1 - All contracts and solicitations with limited exceptions.
- 52.227-2 - All contracts and solicitations with limited exceptions.
- 52.227-3 - Limited mandatory use in sealed bidding for "commercial" supplies/services & construction with many prohibitions on use.
- 52.227-10 - All which might result in a classified invention/patent.
- 52.227-11 - All R&D [DOD uses this clause with small business or nonprofit].
- 252.227-7038 - All R&D except when 52.227-11 used.
- 252.227-7039 - All if 52.227-11 is used.
- 252.246-7001 - Strongly urged whenever any technical data or software will be delivered under the contract. Using the clause avoids acceptance being "final" with respect to nonconforming markings. Review 246.708 and 246.710 for applicability. **As of 07 Sept 2011.**

Appendix 8: CLICKWRAP OR EMBEDDED LICENSE ISSUES

[Note to Preparers: *When citing regulations such as the DFARS and FAR, dates are included where possible to reflect the most recent version of this Guidebook. However, Contracting Officers and PMs need to check for current clause dates before using the language in this Guidebook.*]

The proposed contract language presented in this appendix relates to copyright, licenses, or other restrictions included in delivered software, whether imposed by a third party, the contractor itself, or the Open Source Software (OSS) community.

Frequently, Government contracts have all the usual clauses regarding contractor delivery of noncommercial software to the Government with the standard DFARS license rights (e.g., Government Purpose Rights). However, when delivery is required, the contractor does not deliver a compact disc or DVD, but instead posts the software on a website and provides the Government a password for access and download.

Often, if not always, attempting to access the site or software code activates a pop-up window that reads something like: "Accessing this website and downloading the code it contains indicates the User's consent to all the terms and conditions of the site, etc." In other cases, a license consent mechanism may be embedded into a program so that upon first use or every use, the program displays a similar pop-up window. The User then has the choice of trying to comprehend numerous pages of legalese or simply clicking "OK." In most cases, the User just clicks "OK."

This becomes a problem for the Government in cases where the Government User does not tell the Contracting Officer (CO) about the "clickwrap" license, or does not indicate whether that license appeared to provide terms and conditions that are different than the license specified in the contract, but instead simply confirms delivery. Upon confirmation of delivery, the CO authorizes payment to the contractor. Because these steps have been taken, there is now a risk of the appearance or argument that the CO has ratified the click-wrap license restrictions on behalf of the Government, which is probably not in the Government's best interests, and in any event violates the DFAR requirement for any non-standard licenses to be incorporated into the contract (which should allow for more detailed review to determine how the license relates to the previously established contract terms and conditions).

The following sample clause addresses this issue by requiring that any license, whether for commercial or noncommercial software, whether private or OSS, be approved by the CO and incorporated into the contract, or it does not apply. The clause should ideally be included in Section H or Section I of the contract, rather than the Section C Statement of Work (SOW). We make this recommendation because when interpreting a contract for a claim or protest, the SOW has a lower ranking of precedence⁵⁰.

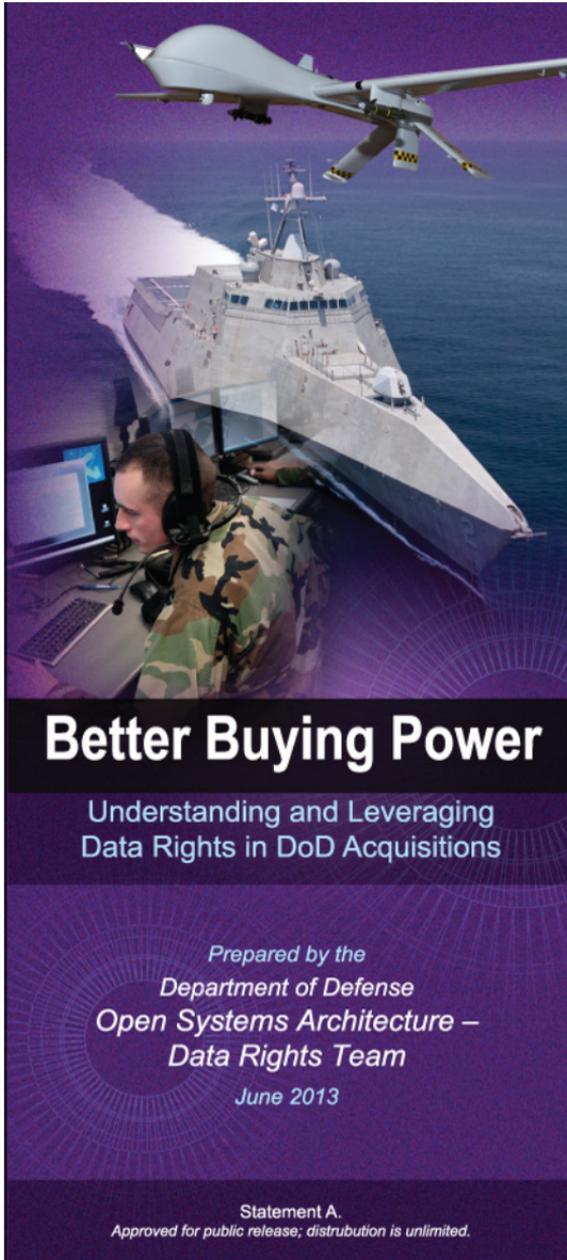
a. **LANGUAGE TO PREVENT CONTRACTOR USE OF “CLICKWRAP” LICENSES TO CIRCUMVENT GOVERNMENT PURPOSE RIGHTS**

- i. Except with respect to commercial computer software as defined in DFARS 252.227-7014(a)(1), no contractor, subcontractor, or third-party license or other restriction shall be included with or imposed on software delivered pursuant to this contract the terms of which differ from or conflict with the terms of this contract, including, but not limited to, terms relating to rights in technical data, rights in noncommercial computer software and noncommercial computer software documentation, indemnification, and liability; unless such license(s) or restriction(s) are approved by the Contracting Officer in writing and expressly incorporated into the contract prior to the delivery of software subject to such license(s) or restriction(s). Such licenses or restrictions include by way of illustration and not limitation so-called “clickwrap” licenses.
- ii. For any commercial computer software as defined in DFARS 252.227-7014(a)(1) that the contractor intends to incorporate into or deliver with any software to be delivered pursuant to this contract, the contractor shall identify such software or documentation to the Contracting Officer or the Contracting Officer’s designated representative prior to delivery thereof. The contractor shall also supply to the Contracting Officer or the Contracting Officer’s designated representative a copy of any licenses applicable to such software at the time the software is identified. The contractor, in accordance with the Contracting Officer’s instructions, shall negotiate any changes to the license that are required to make the license consistent with Federal procurement law and the Government’s needs

⁵⁰ See the applicable order of precedence clause, e.g., FAR 52.215-8, or 52.212-4(s).

- regarding such software. No such software shall be incorporated into or delivered with other software delivered pursuant to the terms of this contract without the Contracting Officer's express written permission.
- iii. For any open source software (as defined at Section 3.1 of the CENDI report at http://www.cendi.gov/publications/09-1FAQ_OpenSourceSoftware_FINAL_110109.pdf, that will be included in any deliverable item or part thereof under this contract or will be used to create any deliverable item or part thereof under this contract, the contractor shall:
- a) identify the open source software;
 - b) provide, for each of the software identified in a), copies of any and all licenses associated with such software;
 - c) ensure, for each of the licenses identified in b), that the Government's rights under such licenses permit the Government to use the deliverable(s) for its intended purpose; and
 - d) ensure that the contractor has complied with any and all requirements of the licenses identified in b).
- iv. Any licenses relating to open source software shall be subject to all the requirements of this clause.
- v. Notwithstanding the requirements of paragraphs i. and ii. hereof, no software shall be delivered pursuant to this contract if the software or any part thereof is subject to any copyright, license, or other reservation of rights (hereafter "reservation") that imposes any requirement of subsequent action by the Government, unless express written permission for such inclusion is obtained from the Contracting Officer prior to delivery of such software. Such requirement of subsequent action includes by way of illustration and not limitation: a requirement that upon distribution the Government must make such software available in any form to any entity; a requirement that prior to a distribution of the software by the Government the Government is obliged in any way to ensure that the entity to which it distributes the software abides by the terms of the reservation or acquires any license or other right; or any requirement that is inconsistent with Federal laws including but not limited to national security requirements, export control laws and regulations, or acquisition laws and regulations.
-

APPENDIX 9: BETTER BUYING POWER: UNDERSTANDING AND LEVERAGING DATA RIGHTS IN DOD ACQUISITIONS



BETTER BUYING POWER:

UNDERSTANDING AND LEVERAGING DATA RIGHTS IN DOD ACQUISITIONS (2 of 5)

“Data Rights” → Rights in Technical Data (TD) and Computer Software (CS)

“Data Rights” is a shorthand way to refer to the Government’s license rights in two major categories of valuable intellectual property:

- Technical Data (TD) includes any recorded information of a scientific or technical nature (e.g., product design or maintenance data, computer databases, and computer software documentation (CSD)).
- Computer software (CS) includes executable code, source code, code listings, design details, processes, flow charts, and related material.

Anticipating the Need for Data and Data Rights

A Program Manager must ensure that all TD and CS and related license rights required for procurement and sustainment of a system are available throughout the system’s life cycle.

- Sustainment activities include reprourement, maintenance, repair, modifications or interfacing/ interoperability activities, and upgrades or technology insertion.
- Consider a priced option for any data deliverables or data rights that you may need in the future, but do not order up front.

Identify and Resolve Data and Data Rights Issues Prior to Contract Award

Identify and resolve data delivery or data rights issues prior to contract award, by:

- Requiring Offerors to assert all restrictions on deliverable TD and CS—both commercial and noncommercial—up front, in their proposals;
- Evaluating the data and data rights packages being offered;
- Negotiating for mutually agreeable specialized license rights whenever the standard license categories do not meet both parties’ needs.

BETTER BUYING POWER: UNDERSTANDING AND LEVERAGING DATA RIGHTS IN DOD ACQUISITIONS (3 of 5)

Data Delivery Requirements

The DFARS clauses do not require delivery of TD or CS—the Government must include specific delivery requirements in each contract, mere access may not protect Government interests. Consider a priced option for contingency-based data delivery or data rights needs.

Data Rights Granted to the Government

The Government's license rights to a contractor's TD and CS generally depend upon the extent to which the Government funded the development of the technology, whether the technology is commercial or noncommercial, and any negotiations for mutually agreeable "special" license agreements. Some types of data qualify for Unlimited Rights regardless of development funding, such as "form, fit, and function data," (FFF) and data necessary for operation, maintenance, installation, and training (OMIT) purposes. (Excluding detailed manufacturing and process data).

Rights Category	Applies to These Types of TD or CS	Rights Criteria	Permitted Uses Within the Government	Permitted Uses by Third Parties Outside the Government ¹
Unlimited Rights (UR)	Noncommercial TD and CS	Developed exclusively at Government expense, and certain types of data (e.g., FFF, OMIT, CSD)	All uses; no restrictions	All uses; no restrictions
Government Purpose Rights (GPR)	Noncommercial TD and CS	Developed with mixed funding	All uses; no restrictions	For "Government Purposes" only; no commercial use ¹
Limited Rights (LR)	Noncommercial TD only	Developed exclusively at private expense	Unlimited; except may not be used for manufacture	Emergency repair or overhaul ¹
Restricted Rights (RR)	Noncommercial CS only	Developed exclusively at private expense	Only one computer at a time; minimum backup copies; modification ²	Emergency repair/overhaul; certain service/maintenance contracts ¹
Negotiated License Rights	Any/all TD and CS—including commercial TD and CS	Mutual agreement of the parties; use whenever the standard categories do not meet both parties' needs	As negotiated by the parties; however, must not be less than LR in non commercial TD and must not be less than RR in noncommercial CS (consult with legal counsel as other limits apply)	
SBIR Data Rights	Noncommercial TD and CS	All TD or CS generated under an SBIR contract	All uses; no restrictions	Cannot release or disclose except to Government support contractors ^{1,2}
Commercial TD License Rights	Commercial TD only	TD related to commercial items (developed at private expense)	Unlimited in FFF and OMIT; other rights as negotiated	
Commercial CS Licenses	Commercial CS only	Any commercial CS or CS documentation	As specified in the commercial license customarily offered to the public ⁴	

¹ All third party use under Government's license is subject to Government authorization. For rights categories other than UR, releases or disclosures to third parties must be accompanied by either the Non-Disclosure Agreement (NDA) from DFARS 227.7103-7 or must occur under a contract containing DFARS 252.227-7025. A notice requirement also applies to releases of LR data and RR software.

² In addition to the footnote 1 NDA and notice requirements, all authorized Covered Government Support Contractors of LR data or RR software must sign an NDA directly with the owner of the data/software, if required by the owner.

³ See DFARS 252.227-7014(a) for more information.

⁴ Such licenses must be consistent with Federal procurement law and satisfy user needs.

BETTER BUYING POWER: UNDERSTANDING AND LEVERAGING DATA RIGHTS IN DOD ACQUISITIONS (4 of 5)

Understanding and Leveraging Open Systems Architecture in DoD Acquisitions to Increase Competition

Effective Competition requires use of Competitive Strategies and an Open Business Model.

Open Business Model (OBM) = Use of Open Systems Architectures (OSA) and an Intellectual Property Strategy (IPS)

Open Systems Architectures (OSA)

Who?

- Program Managers and other Acquisition Corps professionals.

What?

- Plan for and leverage the use of Open Systems Architectures (OSA) and Open Business Model to increase access to innovation and reduce cost through competition.

Why?

- Use of OSA standards and approaches allows for multiple vendors to propose innovative and affordable design solutions that will meet performance and interface requirements. The multiplicity of solution alternatives creates opportunity for competition for the system components without being locked into a single vendor's proprietary design or technology. This sole source situations or costly acquisition of license rights to use proprietary solutions. This also facilitates fluid integration of new capability to meet warfighter demands.

When?

- OSA can be used anytime in the product life cycle. Maximum benefit is obtained if OSA is used from the beginning of system development, but later life cycle activities such as engineering changes, product improvements or modernization efforts can also be opportunities to bring in or enhance the use of OSA.

Where?

- OSA should be an integral part of the Acquisition Strategy development and the Systems Engineering process, both for initial product development and for later product improvements.

Intellectual Property Strategy (IPS)

The IPS addresses all of a program's Intellectual Property (IP) requirements (focusing on technical data and software and associated data rights) throughout the life cycle of the system.

BETTER BUYING POWER:
UNDERSTANDING AND LEVERAGING DATA RIGHTS IN DOD ACQUISITIONS
(5 of 5)

Data Rights Resources

Laws, Regulations, and Policies

- Title 10, U.S. Code, Sections 2320 and 2321
- Defense Federal Acquisition Regulation Supplement (DFARS):
 - 227.71 (*Rights in Technical Data*)
 - 227.72 (*Rights in Computer Software and Computer Software Documentation*)
 - 252.227-7013, -7014, -7015, -7018
- Better Buying Power 2.0
A Guide to Help You Think

Additional Guidance

- Army Guide for the Preparation of a Program Product Data Management Strategy (Under Revision)
- DoD Open Systems Architecture Contract Guidebook for Program Managers
- Acquiring and Enforcing the Government's Rights in Technical Data and Computer Software Under Department of Defense Contracts, Air Force Space and Missile Systems Center

Better Buying Power

Understanding and Leveraging
Data Rights in DoD Acquisitions

Please visit

<https://acc.dau.mil/oa>

for additional information and resources

Statement A.

Approved for public release; distribution is unlimited.

Appendix 10: BREAKING AND AVOIDING VENDOR LOCK

A. What is Vendor Lock?

Vendor lock⁵¹ creates a situation where acquisition choices are limited and an organization becomes dependent on a single manufacturer or supplier for product(s) and/or service(s). The organization cannot compete the associated work to another source (contractor or organic) without unacceptable costs and/or inconvenience. This dependency is typically a result of standards that are controlled by the vendor (i.e., manufacturer or supplier) or limited access to information as a result of a previous contractual relationship. These vendor lock situations are analogous to allowing the vendor to have some level of monopoly power in the marketplace, and may put the consumer at a significant disadvantage regarding competitive pricing.⁵² The downsides of vendor lock in any given acquisition may be offset by other associated factors, such as significant savings in upfront Government funded development costs by utilization of technologies that have been developed exclusively at private expense, including commercial technologies.⁵³ However, the monopoly power inherent in vendor lock situations provides the opportunity for vendors to offer noncompetitive pricing as the sole source of a relevant product or service. Government acquisition officials should be mindful of the short and long term savings and costs when conducting business analyses of actions that may create, or avoid, potential vendor lock. Avoiding and breaking vendor lock is consistent with ensuring maximum potential for competition as directed by the Under Secretary of Defense for Acquisition, Technology and Logistics' (USD AT&L) memo of

⁵¹ Vendor lock-in, or just lock-in, is the situation in which customers are dependent on a single manufacturer or supplier for some product (i.e., a good or service), or products, and cannot move to another vendor without substantial costs and/or inconvenience. This dependency is typically a result of standards that are controlled by the vendor (i.e., manufacturer or supplier). It can grant the vendor some extent of monopoly power and can thus be much more profitable than would be the absence of such dependency.

[http://www.lininfo.org/vendor_lockin.html] referenced in [\[nii.defense.gov/sites/oss/Open_Source_Software_%28OSS%29_FAQ.htm\]\(http://www.lininfo.org/sites/oss/Open_Source_Software_%28OSS%29_FAQ.htm\)\]](http://cio-</p></div><div data-bbox=)

⁵² http://www.lininfo.org/vendor_lockin.html

⁵³ Nondevelopmental technologies may also have advantages regarding technology maturity, thereby reducing technical risk.

September 14, 2010, known as “Better Buying Power”.⁵⁴ The patterns of behavior associated with breaking and avoiding vendor lock have many parallel facets. The remainder of this appendix explores a series of identified approaches associated with Breaking Vendor Lock for current programs, and, provide some additional guidance on avoiding Vendor Lock situations altogether.

B. Approaches to Breaking Vendor Lock:

Breaking vendor lock is a challenge that many development projects in the Department of Defense must overcome to maximize potential for capturing innovation and reducing life-cycle costs through the power of competition for the duration of the systems life-cycle. In situations where a vendor has cornered the marketplace for a technology or capability and cost reduction or improve capabilities and performance are needed, program offices must pursue a range of options to help them break out of these vendor lock situations which inhibit competition. The following preliminary set of approaches for addressing vendor lock are based on internal cases across the DoD Services and Agencies.

1. Establish an Environment for Change:

Recognition of the need for change in the marketplace, such as a new and serious National Security threat or downward budgetary pressures, will dramatically alter the competitive landscape of an acquisition environment and force Program Manager’s to seek-out new solutions in response. This environment for change must be translated into a shift in the business approach and technical requirements that are identified to develop identified warfighting solutions. Senior acquisition leadership as well as the Program Offices should announce that new methods to solve new problems are coming and that business as usual must change. This can be initiated at any level, but is most effective when it is initiated at the highest point in the acquisition hierarchy. It is especially important to be transparent with the warfighting customer and resource sponsor to ensure they are engaged stakeholders during the transformation process and are supportive of the new approach. There are a series of actions that the military Services can take to support breaking out of a current vendor locked program; these include:

⁵⁴ http://www.acq.osd.mil/docs/USD_ATL_Guidance_Memo_September_14_2010_FINAL.PDF

Elevate the issue

The first step to creating the necessary environment for change is to elevate the issue to the highest possible level and communicate the intended course of action which will be pursued for the purposes of providing additional acquisition flexibility and breaking out of a vendor locked situation. For example, in February 2009, the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) provided an Acquisition Decision Memorandum (ADM) which specifically outlined the need to adopt a common Ground Control Station (GCS) architecture for Unmanned Aerial Systems (UAS) that would permit additional capability to be easily integrated, enable competition, and encourage innovation in UAS GCS acquisitions. This approach was embraced by senior Navy and Army leadership in service-specific Acquisition Decision Memorandums which indicated support for the effort. The positive results of this effort are exemplified in the case below.

Case Study: Office of the Secretary for Defense, Unmanned Aircraft Systems Control Segment Working Group

The UCS-WG changed DoD's traditional approach to acquisition and used open architecture principles to develop a Service Oriented Architecture (SOA) Based Architecture for a common ground control station across the Services. The UCS WG funded a limited number of development pilots to demonstrate the UCS architecture and illustrate the potential for Joint development and integration of GCS capabilities by various companies proving to be a major breakthrough in improving acquisition flexibility and breaking out of vendor lock. The set of Initial Work Packages (IWP) demonstrated how the U.S. Air Force Weather service capability could be integrated into other Service's GCS, thus permitting acquisition flexibility and breaking vendor lock.

The AF Weather service interfaces with AF Weather Servers to provide tactical overlays of current and forecast weather conditions. Although the service was developed by the USAF it was successfully integrated into Navy and Army GCS'. The demonstration proved the service architecture was portable and hardware independent. The AF Weather exercise resulted in:

- 75% reduction in development and integration costs
- Integration time of one - three weeks

The typical cost for creating a GCS-specific weather service is in excess of \$2M, thus making the case for only one service development effort for use across multiple GCS'.

Source: "Open Architecture Efficiencies in the Development of DoD UAS Ground Control Stations (GCS)"

Publish the intent to compete

An additional step a program can take to break vendor lock is to publish the intent to compete any of the current work. Possibilities for competition for those vendor locked programs Post-Milestone C include system upgrades, technology insertion, operations and

maintenance support, training, any other sustainment activity. Secondary benefits to this evolving initiative include motivation of an incumbent to improve performance, reduce costs, or accelerate schedule; and motivation of competitors to maintain competitive capabilities and alternatives. To be effective, there must be a credible opportunity for the work to go to another vendor through competition. For new programs, a key consideration to prevent vendor lock is to openly communicate the intent to compete often as a part of the program's identified competition and acquisition strategies. Even if an incumbent remains as the contractor, the mere possibility of competition when clearly articulated should promote the secondary benefits.

Establish Government/Industry/Academia Forum

Establishing a government/industry/academia forum has been effective to undertake a coordinated approach to creating open architecture frameworks and to shift the development focus of a current program to one that is centered upon achieving greater performance and lower costs. This type of interactive forum would put the incumbent and its current business practices under scrutiny and permit outsiders to evaluate the current program for opportunities to improve upon the current "vendor locked" situation. These same principles can be applied to situations where new acquisitions are seeking ways to prevent vendor lock. In these cases, a similar review of an acquisition or competition strategy in a forum could take place in order to gauge feedback on precisely how "open" a suggested acquisition might be.

Establish a Flexible Contracting Approach

Many contracts have been structured in a monolithic and inflexible manner that often mirrors the type of systems they were intended to acquire. To support the concept of enabling "acquisition choice," Program Managers should be mindful to ensure their contracts and acquisition organizations are structured to permit modularity in acquisitions which will foster loosely coupled and highly cohesive business relationships among a wide variety of innovative and cost effective vendors. This approach to flexible contracting can be taken from program inception, pre-Milestone A throughout Milestone C to ensure and prevent a vendor locked relationship from occurring in the first place.

Case Study: Subs Acoustic Rapid COTS Insertion Program

In 1995, the U.S. Navy faced a serious crisis with the reduction in U.S. acoustic superiority impacting our ability to detect other submarines and vessels. At the same time, the former Soviet Union was improving on their acoustic capabilities. This technical challenge was compounded by a

significant reduction in program funding which required a radical change in the way the Navy built mission systems. The Program Executive Office for Submarines adopted an open architecture approach for the sonar systems and implemented many OA business and technical practices – modularized the sonar system, disclosed designs of the architecture, published interfaces, and increased competition to generate a wide range of possible solutions from many sources to address the mission challenge. This change led to the Acoustic Rapid COTS Insertion (ARCI) Program to upgrade capabilities quickly.

In addition to increasing competition and improving sonar system performance, ARCI generated significant large cost savings across all budget allocations in a comparison of the 1983-1993 budget allocations to 1996-2006 allocations (\$7.6 billion to \$3.6 billion). These savings reflect a reduction in Development and Production by a factor of six and a reduction in Operating and Support costs by a factor of eight. ARCI also realized over \$25 million in cost avoidance for logistics support, including over \$1 million in technical manuals, over \$2 million in direct vendor delivery, over \$19 million in interactive, multimedia instruction, and \$3 million in outfitting spares reduction.

Source: <http://acquisitionresearch.net/files/FY2009/NPS-AM-09-043.pdf>

2. Leverage and Exercise Data Rights:

Data rights are fundamental to breaking out of vendor locked relationships and are valuable for supporting increased transparency across the enterprise. When the government does not possess the data deliverables and associated data rights needed to re-compete an existing program, they typically become vendor locked.

There are a series of actions which a current vendor locked program can undertake with respect to data rights which may improve their current position, these include:

Assess what you have and what you need

As part of the newly required Technical Data Rights Strategy is a strategy worksheet designed to help program managers assess their current data and data rights and evaluate what (if any) additional data and/or rights they may need in the future to ensure they maintain the potential for competition throughout the acquisition life-cycle. A slightly modified version of this worksheet is also included in the Appendix of this Guidebook. Both new and existing Programs should undertake a rigorous assessment of their data and data rights to help inform their future activities to prevent and/or break out of vendor lock situations.

Require delivery of non-delivered CDRLs and assert data rights

As noted in the *Contract Guidebook for Program Mangers*, contracts should contain the appropriate language to require delivery of any previously non-delivered CDRLs. After delivery, Program offices should ensure they are also fully asserting their data rights for these

non-delivered CDRLs. For example, the Government, regardless of the source of funding, is entitled to Unlimited Rights in Form, Fit and Function (FFF) data. In some cases, however, programs have failed to take delivery of this data – which is the necessary first step to being able to exercise the Government’s rights as a means to break a vendor lock relationship. By requiring delivery of this information and data, program offices may be able to break out of vendor lock situations and compete for some goods/services. For those programs that may be trying to prevent vendor lock, ensuring that contracts contain the appropriate language for delivery of these items up front is vitally important.⁵⁵

Case Study: ONR SEWIP Program

Intended to serve as a replacement for the AN/SLQ-32 shipboard electronic warfare suite, the Surface Electronic Warfare Improvement Program (SEWIP) was born out of the Multi-Function Electronic Warfare (MFEW) program from the Office of Naval Research (ONR). Under the ONR MFEW effort, several critical electronic warfare technology elements were matured to a technical readiness level (TRL) of 6. Through the course of maturing this technology in the program, ONR was also able to capture Government Purpose Rights (GPR) on most of the hardware and software. This technology was then transitioned to the SEWIP program for integration into a larger development effort. In the competition for SEWIP, the Navy provided the actual MFEW GPR data as GFI with the RFP. Inclusion of this information ultimately resulted in a more robust competition.

In addition, data rights options were included as part of the Block 2 RFP. The program leveraged the Open Architecture Contract Guidebook for Program Managers to identify specific contracting language that would support acquiring data rights options in the RFP. The RFP thus provided the option for Offerors to price data rights and included evaluation criteria on that option in the RFP. As a result, this resulted in all Offerors addressing the data rights option directly in the RFP as well as an ultimate contract award with Unlimited Data Rights at no cost for all SEWIP Block 2 hardware and software technical data developed under the contract.

3. Change approach to Systems Engineering:

Systems engineering is a fundamental component of breaking vendor lock. This especially holds true for legacy programs with similar functionality across a product line. Program Manager’s should understand the impact that an inflexible, proprietary system architecture will have on their program throughout the acquisition life-cycle.

⁵⁵ Section 815 of the 2012 National Defense Authorization Act adds a new category of technical data “data necessary for segregation and reintegration.” When implemented into the DFARS, this new category should assist with breaking of vendor lock.

Typically these types of architectures prohibit or significantly restrict the option for technology insertion from third-party vendors; lead to the potential for systems to become obsolete; and in some cases can be highly expensive to maintain. To overcome these challenges PMs can:

Develop a common architecture across a product line or similar Programs of Record

Development of a common architecture is an approach to preventing vendor lock and should typically be completed early on in the course of the acquisition life-cycle. By developing a common architecture design across a range of products or similar Programs of Record, a Program Manager can expand the potential for competition as there will be more opportunities to compete with a standardized, well defined, common architecture. This approach will permit economies of scale and improved learning to enhance prospects for innovation and reduced costs.

In cases where a program may be already vendor locked, a common architecture can be developed from existing program artifacts if they are supported by a comprehensive approach to migration. Part of this migration strategy must include a plan that addresses how the funding for such an effort may be structured to support commonality across a line of products that may have several different owners. In legacy programs, particular attention must also be paid to “backfit” and “forward fit” of systems.

Functionally decompose legacy Programs to determine where competition will reap the most benefits

Program Managers can more optimally break vendor lock by specifically identifying which parts of the system architecture would benefit most from being competed and focusing their efforts on these components and/or sub-systems. Such an approach helps programs better understand the potential return on investment for where it might be most beneficial for a program to break up a vendor locked portion of the system. PMs can also leverage areas in the system architecture where they may hold Government Purpose Rights or Unlimited Rights (or a specially negotiated license that supports competitive actions) to better define interfaces for those system components which have been identified as being the most beneficial to “open up”.

When trying to prevent vendor lock the same approach can be taken on early in system design to help identify which parts of the system it would be most beneficial to “open” up. PMs should be mindful of cases in these situations to help guide decision-making to ensure their programs have integrated the lessons learned in the past. Accordingly

these system modules can and should be competed accordingly throughout the system life cycle.

4. Hold Competition:

Competition is widely believed to be the best way to break up a vendor lock situation. The threat of competition can be used as an incentive for the incumbent to improve performance and reduce costs. The following approaches support encouraging more competition in vendor locked programs and may assist in preventing vendor lock all together:

Create an alternative, and then compete it

Another approach to breaking a current vendor lock cycle is to generate an alternative or competing product using another vendor. This approach also enables non-traditional vendors, such as academia or government labs, to be considered. By competing in this manner, additional competitive pressure is then placed on the incumbent vendor to improve performance, lower costs, and/or offer data rights options to the client.

Limit Integrator role

One possible approach to maximizing prospects for competition and breaking vendor lock is to limit the role of the integrator when technology insertion is being undertaken. In these cases an existing integrator may be forbidden from building components that will be provided as part of technology insertion and upgrades in future competitions related to the system. In these cases the integrator may be then incentivized solely on their ability to successfully integrate a third-party component. In considering this approach, the PM and acquisition officials must be mindful of the Competition in Contracting Act and properly justify any exclusion of sources in accordance with FAR Subpart 6.3.

Share GPR for next competition

For those data where the Government enjoys GPR rights (or any special license that permits competitive activities), it may exercise these rights in support of a follow-on competition. In these cases, GPR data may be shared as part of the RFP package as noted in the SEWIP case study. This approach can support a more robust competitive environment.

Inject Open System Architecture (OSA) through technical insertions

While ideally an OSA should be designed at the forefront of the systems development process, most legacy programs do not have open technical features included in their systems design. By injecting various

OSA features into existing programs during technology insertion or upgrades it may permit a vendor locked program to open itself up.

Inject and/or release components as Open Source Software (OSS)

Replacing certain components with Open Source Software (OSS) components, or releasing certain components as OSS to the public, can also reduce lock. This is because OSS components can be supported by multiple suppliers. Software components can be released as OSS to the public by the Government if the Government has Unlimited Rights (for more information, see “Open Technology Development (OTD): Lessons Learned & Best Practices for Military Software” Appendix B) See Appendix 5 for more information on OSS.

Use Government Labs for Integration

Government labs have also been successfully used for integration in the past depending on the size and scope of the program. Utilizing these labs as integration hubs for existing programs may be another mechanism to break up vendor lock. Care should be taken to ensure that enough relevant technical data, including computer software, can be secured to compete again, if necessary.

5. Incentivize Good Behavior and Reward Subsequent Outcomes:

Provided the proper business case can be made, incentivizing good behavior can be another tool for breaking vendor lock. The following approach may be used to incentivize good behavior:

Vendor-to-vendor cooperation as part of past performance evaluations

In these cases, programs may choose to include cooperation with third-parties in system acquisitions as part of the proposal evaluation process. These evaluations might require a bidder to demonstrate how they have historically included other businesses in their previous contracts and generate a plan of action that ensures good vendor-to-vendor cooperation during contract execution.

6. Change Contracts:

Competition is executed through contracts. The *Program Managers Contract Guidebook* provides a detailed overview of contractual language that should be included to maximize prospects for open systems and minimize vendor lock.

Incentive fees for delivery, collaboration, and life cycle savings

Contracts can be structured to include a wide array of incentives to help mitigate the impacts of being in a vendor locked relationship. Incentive fees and award terms for a vendor locked program can be made as a means to encourage collaboration with third-party vendors, improve

performance, lower life-cycle costs and quicken development schedules. As with any incentive, having the program office hold the contractor accountability for achievement is key for its effectiveness.

Include OSA as part of evaluation criteria

As noted extensively in the *OSA Contract Guidebook*, key OSA technical requirements can be included in source selection evaluation criteria for follow-on contracts as a means to break down a vendor-locked system and convert it into a more open one as technology insertion and upgrades take place. If Offerors fail to respond to these OSA specific technical requirements, which are designed to break vendor lock, they will lose points on the follow-on evaluation and subsequently run the risk of losing the work.

Reward reuse of existing products in Evaluation Criteria

Rewarding reuse is also another mechanism for breaking a vendor lock relationship. For a new contract evaluation, a program office can reward reuse of existing products in a vendor's proposal by requiring a certain amount of reuse or a certain component (or set of components) be reused as part of its requirements to be evaluated during the source selection process.

Appendix 11: SAMPLE CONTRACT DATA REQUIREMENTS LISTS (CDRLs)

The following pages include sample CDRLs that can be used in conjunction with Appendix 1 and other parts of this *Guidebook* to define the project's deliverables and other information products. These are only a sample.

CONTRACT DATA REQUIREMENTS LIST (CDRL) DD FORM 1423

TABLE 1. DATA INSPECTION AND ACCEPTANCE CODES

<u>CODE</u>	<u>DEFINITION</u>	
<u>DD 250 CODE</u>	<u>INSPECTION</u> <u>ACCEPTANCE</u>	
SS	Source*	Source*
DD	Destination	Destination
SD	Source*	Destination
DS	Destination	Source*
LT**	Letter of transmittal only.	
NO**	No inspection, acceptance or letter of transmittal required.	
XX	Inspection and acceptance requirements specified elsewhere in the contract.	

* Source indicates contractor facility

** These codes are not authorized for data comprising final delivery of Technical Data Packages or for final delivery of Technical Manuals. (LT may, however, be used for delivery of preliminary TDPs or TMs.)

LT is not authorized for use when inspection is required. LT is used when the contracting agency does not desire to have a DD Form 250 for each and every piece of data developed by the contractor. The only other authorized use of LT is the special case where the contracting agency does not desire to have separate DD Forms 250, but desires to have a Government Quality

Assurance (QA) representative perform inspection. The Government QA representative shall be listed on the distribution in Block 14 and requested, via the QA letter of instruction, to provide comments.

Block 10. FREQUENCY

The frequency of data submittal. Entries in this block are explained in Table 2. If the data is of a recurring type, it is to be submitted at the end of the reporting period established in this block unless otherwise indicated in Block 16.

TABLE 2. DATA SUBMITTAL FREQUENCY CODES

<u>CODE</u>	<u>FREQUENCY</u>
ANPLY	Annually
ASGEN*	As generated
ASREQ*	As required
BI-MO	Every two months
BI-WE	Every two weeks
CP/RQ*	Change pages as required
DAILY	Daily
DFDEL	Deferred delivery (See DFARS 252.227-7026)
MTHLY	Monthly
ONE/R	One time with revisions
OTIME	One time (Does not include draft submissions)
QRTLY	Quarterly
R/ASR*	Revisions as required
SEMIA	Every six months
WEKLY	Weekly
XTIME	Multiple separate submittals (2TIME, 3TIME, etc.) (Does not include draft submissions)
See Block 16*	Requirement is fully described in Block 16. Used in lieu of other codes where such as inadequate to define requirement, or used in addition to other codes requiring amplification in Block 16.

NOTE: The codes are limited to five (d) digits for automation purposes.

*The ELINs citing these codes will have an additional explanation in Block 16 to provide the contractor with guidance necessary to accurately price the deliverable data item.

Block 12. DATE OF FIRST SUBMISSION

The due date for initial data submission. This is normally the postage date or date the data is delivered to the ACO, entered as year/month/day (e.g., 03/MAY/02) or keyed to a specific event or milestone, using a code from Table 3.

NOTE: No classified dates are cited in the CDRL.

TABLE 3. DATA SUBMISSION CODES

<u>CODE</u>	<u>FREQUENCY</u>
ASGEN*	As generated
ASREQ*	As required
DFDEL*	Deferred delivery
XDAC**	Days after contract award
XDACM**	Days after contract modification
XDARC**	Days after receipt of comments
XDARP**	Days after reporting period
XDATC**	Days after test completion
XDPTT**	Days prior to testing
EOC	End of contract
EOQ	End of quarter
NLT	No later than
See Block 16*	Used to indicate requirement is fully described in Block 16.
	Used in lieu of other codes where such as inadequate to define requirement, or used in addition to other codes requiring amplification in Block 16.

* The ELINs citing these codes will have in Block 16 additional specific instructions relative to data submissions.

** The "X" is assigned a value indicating the number of days, e.g., 30DAC.

INSTRUCTIONS FOR COMPLETING DD FORM 1423 <i>(See DoD 5010.12-M for detailed instructions.)</i>	
<u>FOR GOVERNMENT PERSONNEL</u>	<u>FOR THE CONTRACTOR</u>
<p>Item A. Self-explanatory.</p> <p>Item B. Self-explanatory.</p> <p>Item C. Mark (X) appropriate category: TDP - Technical Data Package; TM - Technical Manual; Other - other category of data, such as "Provisioning," "Configuration Management," etc.</p> <p>Item D. Enter name of system/item being acquired that data will support.</p> <p>Item E. Self-explanatory (to be filled in after contract award).</p> <p>Item F. Self-explanatory (to be filled in after contract award).</p> <p>Item G. Signature of preparer of CDRL.</p> <p>Item H. Date CDRL was prepared.</p> <p>Item I. Signature of CDRL approval authority.</p> <p>Item J. Date CDRL was approved.</p> <p>Item 1. See DoD FAR Supplement Subpart 4.71 for proper numbering.</p> <p>Item 2. Enter title as it appears on data acquisition document cited in Item 4.</p> <p>Item 3. Enter subtitle of data item for further definition of data item (optional entry).</p> <p>Item 4. Enter Data Item Description (DID) number, military specification number, or military standard number listed in DoD 5010.12-L (AMSDL), or one-time DID number, that defines data content and format requirements.</p> <p>Item 5. Enter reference to tasking in contract that generates requirement for the data item (e.g., Statement of Work paragraph number).</p> <p>Item 6. Enter technical office responsible for ensuring adequacy of the data item.</p> <p>Item 7. Specify requirement for inspection/acceptance of the data item by the Government.</p> <p>Item 8. Specify requirement for approval of a draft before preparation of the final data item.</p> <p>Item 9. For technical data, specify requirement for contractor to mark the appropriate distribution statement on the data (ref. DoDD 5230.24).</p> <p>Item 10. Specify number of times data items are to be delivered.</p> <p>Item 11. Specify as-of date of data item, when applicable.</p> <p>Item 12. Specify when first submittal is required.</p> <p>Item 13. Specify when subsequent submittals are required, when applicable.</p> <p>Item 14. Enter addressees and number of draft/final copies to be delivered to each addressee. Explain reproducible copies in Item 16.</p> <p>Item 15. Enter total number of draft/final copies to be delivered.</p> <p>Item 16. Use for additional/clarifying information for Items 1 through 15. Examples are: Tailoring of documents cited in Item 4; Clarification of submittal dates in Items 12 and 13; Explanation of reproducible copies in Item 14.; Desired medium for delivery of the data item.</p>	<p>Item 17. Specify appropriate price group from one of the following groups of effort in developing estimated prices for each data item listed on the DD Form 1423.</p> <p style="margin-left: 20px;">a. Group I. Definition - Data which is not otherwise essential to the contractor's performance of the primary contracted effort (production, development, testing, and administration) but which is required by DD Form 1423.</p> <p style="margin-left: 20px;">Estimated Price - Costs to be included under Group I are those applicable to preparing and assembling the data item in conformance with Government requirements, and the administration and other expenses related to reproducing and delivering such data items to the Government.</p> <p style="margin-left: 20px;">b. Group II. Definition - Data which is essential to the performance of the primary contracted effort but the contractor is required to perform additional work to conform to Government requirements with regard to depth of content, format, frequency of submittal, preparation, control, or quality of the data item.</p> <p style="margin-left: 20px;">Estimated Price - Costs to be included under Group II are those incurred over and above the cost of the essential data item without conforming to Government requirements, and the administrative and other expenses related to reproducing and delivering such data item to the Government.</p> <p style="margin-left: 20px;">c. Group III. Definition - Data which the contractor must develop for his internal use in performance of the primary contracted effort and does not require any substantial change to conform to Government requirements with regard to depth of content, format, frequency of submittal, preparation, control, and quality of the data item.</p> <p style="margin-left: 20px;">Estimated Price - Costs to be included under Group III are the administrative and other expenses related to reproducing and delivering such data item to the Government.</p> <p style="margin-left: 20px;">d. Group IV. Definition - Data which is developed by the contractor as part of his normal operating procedures and his effort in supplying these data to the Government is minimal.</p> <p style="margin-left: 20px;">Estimated Price - Group IV items should normally be shown on the DD Form 1423 at no cost.</p> <p>Item 18. For each data item, enter an amount equal to that portion of the total price which is estimated to be attributable to the production or development for the Government of that item of data. These estimated data prices shall be developed only from those costs which will be incurred as a direct result of the requirement to supply the data, over and above those costs which would otherwise be incurred in performance of the contract if no data were required. The estimated data prices shall not include any amount for rights in data. The Government's right to use the data shall be governed by the pertinent provisions of the contract.</p>

DD FORM 1423-1 (BACK), FEB 2001

Contract Data Requirement List

The following pages provide the reader with Contract Data Requirement List (CDRL) examples. Some examples contain 2 CDRL examples in a single sheet; the title of those pages notes that there are two examples (e.g., Examples 1&2). Pages with a single example (e.g., Example 3) in the title only contain one such example.

Contract Data Requirements List - Example 1 & 2

CONTRACT DATA REQUIREMENTS LIST <i>(2 Data Items)</i>										Form Approved OMB No. 0704-0188		
The public reporting burden for this collection of information is estimated to average 220 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government heading Contracting Officer for the Contract/PR No. listed in Block E.												
A. CONTRACT LINE ITEM NO. 0001 and 0002			B. EXHIBIT A		C. CATEGORY: TDP _____ TM _____ OTHER <u>MISC</u>							
D. SYSTEM/ITEM Highly Accurate Targeting System				E. CONTRACT/PR NO. N00024-12-D-12345			F. CONTRACTOR TBD					
1. DATA ITEM NO. A001	2. TITLE OF DATA ITEM SCIENTIFIC AND TECHNICAL REPORTS					3. SUBTITLE SOFTWARE AND FIRMWARE DATA						
4. AUTHORITY (Data Acquisition Document No.) DI-MISC-80711				5. CONTRACT REFERENCE SOW para 3.4.4.5.5			6. REQUIRING OFFICE NAVSEA 054					
7. DD 250 REQ. LT		9. DIST STATEMENT REQUIRED B *		10. FREQUENCY MTHLY		12. DATE OF FIRST SUBMISSION 45 DAC		14. DISTRIBUTION				
8. APP CODE A				11. AS OF DATE 0		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE		b. COPIES		
16. REMARKS Blk 8: Approval will be for technical content. The Government requires 10 days to review and the Contractor will have 10 days to incorporate any changes and return to the Government. Blk 9: Distribution Statement B: Distribution authorized to U.S. Government agencies only (administrative or Operational Use as of 6-28-2011). Other requests for this document shall be referred to SEA 054, WNY, Washington, DC. 20376 Blks: 10, 11, 12 and 13: The first submission shall be 45 days after the contract start and monthly thereafter. The report shall be delivered at the end of the month, NLT 5 workings beyond the end of the month. Blk 14: Media Requirements: The report shall be electronically delivered in MS Word version 2003-2007, e-mail notification to addressees.								NAVSEA 054		Draft	Reg	Final
								NAVSEA 054I		1	1	0
15. TOTAL								2		0		
17. PRICE GROUP												
18. ESTIMATED TOTAL PRICE												
1. DATA ITEM NO. A002	2. TITLE OF DATA ITEM INTERFACE CONTROL DOCUMENT (ICD)					3. SUBTITLE						
4. AUTHORITY (Data Acquisition Document No.) DI-CMAN-81248				5. CONTRACT REFERENCE SOW Para.3.3.2.1			6. REQUIRING OFFICE NAVSEA 054					
7. DD 250 REQ. LT		9. DIST STATEMENT REQUIRED D *		10. FREQUENCY ASREQ *		12. DATE OF FIRST SUBMISSION See Blk 16		14. DISTRIBUTION				
8. APP CODE A				11. AS OF DATE N/A		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE		b. COPIES		
16. REMARKS Block 8: Approval will be for technical content. The Government requires 20 working days to review. Contractor has 20 working days to incorporate any changes and return to the Government. Block 9: Distribution Statement D: Distribution authorized the Department of Defense and U.S. DOD Contractors (administrative or Operational Use) (as of 6-28-2011). Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC. 20376 Blks 10, 12 and 13: Initial delivery of the ICD shall be delivered 10 days prior to CDR and final submission shall be at CDR. Blk 14: The report shall be electronically delivered to EDMS, version 3.3 to 1.4) with, email notification to addressees.								NAVSEA 054		Draft	Reg	Final
								NAVSEA 054I		1	1	0
15. TOTAL								2		0		
17. PRICE GROUP												
18. ESTIMATED TOTAL PRICE												
G. PREPARED BY Cynthia Strande, SEA 04512			H. DATE		I. APPROVED BY WILLIAMS.DONNA.S.122980962				J. DATE			

Contract Data Requirements List - Example 3

CONTRACT DATA REQUIREMENTS LIST (CDRL) (1 Data Item)												Form Approved OMB No. 0704-0188		
<p>The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.</p>														
A. CONTRACT LINE ITEM NO. CLN - 0009			B. EXHIBIT A			C. CATEGORY: TDP _____ TM _____ OTHER _____ IPSC _____								
D. SYSTEM/ITEM HIGHLY ACCURATE TARGETING SYSTEM				E. CONTRACT/PR NO. A1263C-11-D-0001				F. CONTRACTOR						
1. DATA ITEM NO. A030		2. TITLE OF DATA ITEM COMPUTER PROGRAM END ITEM DOCUMENTATION					3. SUBTITLE SOFTWARE AND FIRMWARE CODE				17. PRICE GROUP			
4. AUTHORITY (Data Acquisition Document No.) DI-IPSC-80590				5. CONTRACT REFERENCE SEE 16				6. REQUIRING OFFICE ABCD-EFGH-IJKL-M-N				18. ESTIMATED TOTAL PRICE		
7. DD 250 REQ LT		9. DIST STATEMENT REQUIRED		10. FREQUENCY SEE 16		12. DATE OF FIRST SUBMISSION 180 DAC		14. DISTRIBUTION						
8. APP CODE A		11. AS OF DATE N/A		13. DATE IF SUBSEQUENT SUBM. SEE 16		a. ADDRESSEE			b. COPIES					
						Draft			Final					
16. REMARKS BLK 5:3.3.1.2.7[SOW-3342], 3.3.4.2.7.1 [SOW-1794], 3.3.10.5 [SOW-1879], 3.3.3.4.1 [SOW-3743] BLK 8: GOVERNMENT APPROVAL OR DISAPPROVAL WITHIN 30 WORKING DAYS AFTER RECEIPT. SUBMIT REVISIONS AND COMMENT RESPONSES WITHIN 15 WORKING DAYS AFTER RECEIPT OF GOVERNMENT COMMENTS. BLK 9: FOR DIST ST AND EXP WARN SEE END OF EXHIBIT A. BLKS 10, 13: SUBMIT 90 DAYS PRIOR TO SYSTEM CDR AND AT THE END OF THE PERIOD OF PERFORMANCE. SUBMIT FOR EVERY SOFTWARE UPDATE. BLK 14: CLASSIFIED DATA SUBMITTED VIA COMPACT DISC (CD-ROM) IN NATIVE FILE FORMAT TO ABCD-EFGH-IJKL-M-N. DELIVERY REQUIREMENTS: SYSTEM RESIDENT SOFTWARE/FIRMWARE AND BINARY IMAGES: - SOURCE CODE FOR ALL TACTICAL SOFTWARE - SOURCE CODE FOR ALL FIRMWARE (VHDL OR EQUIVALENT) - SOURCE CODE FOR ALL CONTRACTOR/SUBCONTRACTOR DEVELOPED FRAMEWORKS/TOOLS/KITS/ LIBRARIES/ETC UTILIZED IN DEVELOPMENT - SOURCE CODE FOR ALL GOVERNMENT PROVIDED SOFTWARE AND TOOLS UTILIZED IN DEVELOPMENT - SOURCE CODE OR OBJECT CODE, LIBRARIES, AND DOCUMENTATION THAT HAS BEEN CUSTOMIZED OR MODIFIED FROM A COMMERCIAL PRODUCT. - SOURCE CODE FOR ALL CONTRACTOR TOOLS REQUIRED TO BUILD, LOAD, DEBUG, EXECUTE, AND PROCESS DATA FROM THE TEST HARDWARE. - SOURCE CODE FOR ALL COMPONENTS AND TOOLS THAT ARE NOT LISTED EXPLICITLY BUT ARE REQUIRED TO BUILD ALL SYSTEM RESIDENT SOFTWARE AND FIRMWARE. - DETAIL LIST OF ALL COMMERCIAL HARDWARE AND SOFTWARE REQUIRED TO BUILD, TEST, AND LOAD SYSTEM RESIDENT SOFTWARE AND FIRMWARE INCLUDING COMPILERS, DEBUGGERS, PROFILERS, OPERATING SYSTEMS, BOARD SUPPORT PACKAGES, LIBRARIES, FIRMWARE SYNTHESIS AND TEST TOOLS, AND HARDWARE INTERFACES TO TACTICAL HARDWARE. - BUILD SUPPORT INFRASTRUCTURE SUCH AS MAKEFILES, FOR ALL COMPONENTS AND TOOLS SUCH THAT EVERY COMPONENT MAY BE BUILT AT THE GOVERNMENT SITE. - UNIT TEST SCRIPTS AND VERIFICATION SOURCE CODE - DOWNLOADABLE BINARY IMAGES FOR ALL SOFTWARE AND FIRMWARE - TACTICAL ALGORITHM, SOFTWARE AND FIRMWARE DESIGN DOCUMENTS ALL DOCUMENTATION SHALL REFLECT ALGORITHMS, SOFTWARE AND FIRMWARE INCLUDED IN THE SOFTWARE/FIRMWARE VERSION DELIVERED OR INCLUDE SEPARATE DOCUMENTATION IDENTIFYING DIFFERENCES						ABCD-EFGH-IJKL-M-N LETTER ONLY F CLASS SEE 16						I		
						15. TOTAL			0 0 1					
G. PREPARED BY BETTY PATEL				H. DATE 1 Jul 2011		I. APPROVED BY SIMON SAYS				J. DATE 1 Jul 2011				
DD FORM 1423-1, FEB 2001						PREVIOUS EDITION MAY BE USED						Page 1 of 1 Pages		

Contract Data Requirements List - Example 5 & 6

CONTRACT DATA REQUIREMENTS LIST <i>(2 Data Items)</i>										Form Approved OMB No. 0704-0188			
<p>The public reporting burden for this collection of information is estimated to average 220 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government Printing Contracting Office for the Contract/PR No. listed in Block C.</p>													
A. CONTRACT LINE ITEM NO. 0001 and 0002			B. EXHIBIT A		C. CATEGORY: TOP _____ TM _____ OTHER _____ IPSC _____								
D. SYSTEM/ITEM Highly Accurate Targeting System				E. CONTRACT/PR NO. N00024-12-D-12345				F. CONTRACTOR TBD					
1. DATA ITEM NO. A003		2. TITLE OF DATA ITEM SOFTWARE DEVELOPMENT PLAN						3. SUBTITLE					
4. AUTHORITY (Data Acquisition Document No.) DI-IPSC81427A			5. CONTRACT REFERENCE SOW Para. 3.4.6.1.			6. REQUIRING OFFICE NAVSEA 054							
7. DD 250 REQ LT		9. DIST STATEMENT REQUIRED		10. FREQUENCY ONE/R		12. DATE OF FIRST SUBMISSION 45DAC		14. DISTRIBUTION					
8. APP CODE A *		B *		11. AS OF DATE N/A		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE					
16. REMARKS Blk 8: Approval will be for technical content. The Government requires 10 days to review and Contractor has 10 days to incorporate changes and return to the Government. Blk 9: Distribution Statement B: Distribution authorized to U.S. Government agencies only (administrative or Operational Use as of 6-28-2012. Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC., 20376. Blks 10, 11 and 12: The plan shall be delivered on the 45th work day after contract award. Subsequent submittals shall be delivered 10 working days after receipt of comments. Blk 14: Media Requirements: The plan shall be electronically delivered up to the EDMS 3.4 to 10.4 with e:mail notification to addressees.								Draft		Final			
								NAVSEA 054		1		1	
NAVSEA 0541		1		1		0							
15. TOTAL								2		0			
17. PRICE GROUP													
18. ESTIMATED TOTAL PRICE													
1. DATA ITEM NO. A004		2. TITLE OF DATA ITEM SOFTWARE DEVELOPMENT PLAN						3. SUBTITLE SOFTWARE TRAINING PLAN					
4. AUTHORITY (Data Acquisition Document No.) DI-IPSC 81427A			5. CONTRACT REFERENCE SOW Para.			6. REQUIRING OFFICE NAVSEA 054							
7. DD 250 REQ LT		9. DIST STATEMENT REQUIRED		10. FREQUENCY ONE/R		12. DATE OF FIRST SUBMISSION 90 DAC		14. DISTRIBUTION					
8. APP CODE *A		B *		11. AS OF DATE N/A		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE					
16. REMARKS Block 8: Approval will be for technical content. The Government requires 15 working days to review. Contractor has 15 working days to incorporate any changes and return to the Government. Block 9: Distribution Statement B: Distribution authorized to U.S. Government agencies only (administrative or Operational Use as of 6-28-2012. Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC 20376. Blks 10, 12 and 13: The Software Training Plan shall be delivered 90 working days after contract start. Subsequent submittals shall be 15 working days after receipt of comments. Blk 14: Media Requirements: The plan shall be electronically delivered up to the EDMS 3.4 to 10.4) with e:mail notification to addressees.								Draft		Final			
								NAVSEA 054		1		1	
NAVSEA 0541		1		1		0							
15. TOTAL								2		0			
17. PRICE GROUP													
18. ESTIMATED TOTAL PRICE													
G. PREPARED BY Cynthia Strande, SEA 04512			H. DATE		I. APPROVED BY WILLIAMS.DONNA.S 12208962				J. DATE				

DD FORM 1423-2, AUG 96

PREVIOUS EDITION MAY BE USED.

Page _____ of _____ Pages
Adobe Professional 8.0

Contract Data Requirements List - Example 9 & 10

CONTRACT DATA REQUIREMENTS LIST <i>(2 Data Items)</i>										Form Approved OMB No. 0704-0188			
The public reporting burden for this collection of information is estimated to average 220 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate at 0704-0188. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed forms to the Government Issuing Contracting Office for the Contract/PR No. listed in Block 7.													
A. CONTRACT LINE ITEM NO. 0001, 0002			B. EXHIBIT A		C. CATEGORY: TDP _____ TM _____ OTHER _____ IPSC _____								
D. SYSTEM ITEM Highly Accurate Targeting System				E. CONTRACT/PR NO. N00024-12-D-12345				F. CONTRACTOR TBD					
1. DATA ITEM NO. A007	2. TITLE OF DATA ITEM SOFTWARE DESIGN DESCRIPTION					3. SUBTITLE							
4. AUTHORITY (Data Acquisition Document No.) DI-IPSC-81435A				5. CONTRACT REFERENCE SOW para. 4.3.2.1				6. REQUIRING OFFICE NAVSEA 054					
7. DD 250 REQ LT		8. DIST STATEMENT REQUIRED C *		10. FREQUENCY ASREQ		12. DATE OF FIRST SUBMISSION 30 DAC		14. DISTRIBUTION					
8. APP CODE A*				11. AS OF DATE See Blk 16		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE		b. COPIES			
16. REMARKS Blk 8: Approval will be for technical content. Government requires 30 days to review and Contractor has 30 days to incorporate changes and return to the Government. Blk 9: Distribution Statement C: Distribution authorized to Department of Defense and their Contractors (administrative or Operational Use as of 6-28-201). Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC 20376. Blks 10, 11, 12 and 13: The specification first initial submission shall be 90 working days after contract start. All subsequent submission shall be 10 days after a changed is made to the baseline specification. Blk 14: Media Requirements: The specification shall be electronically delivered in MS Word version 2007-2010, e-mail notification to addressees.								NAVSEA 054		Draft	Reg	Final	Reqs
								NAVSEA 0541		1	1	0	0
15. TOTAL										2 2 0			
17. PRICE GROUP													
18. ESTIMATED TOTAL PRICE													
1. DATA ITEM NO. A008	2. TITLE OF DATA ITEM SOFTWARE TEST PLAN					3. SUBTITLE							
4. AUTHORITY (Data Acquisition Document No.) DI-IPSC 81438A				5. CONTRACT REFERENCE SOW Para.3.5.4.1				6. REQUIRING OFFICE NAVSEA 054					
7. DD 250 REQ LT		8. DIST STATEMENT REQUIRED C *		10. FREQUENCY ASREQ		12. DATE OF FIRST SUBMISSION SEE BLK 16		14. DISTRIBUTION					
8. APP CODE A				11. AS OF DATE N/A		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE		b. COPIES			
16. REMARKS Block 8: Approval will be for technical content. The Government requires 15 working days to review. Contractor has 15 working days to incorporate any changes and return to the Government. Block 9: Distribution Statement C: Distribution authorized to the Department of Defense and their Contractors (Administrative or Operational Use) (as of 6-28-2012). Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC 20376. Blks 10, 12 and 13: The Software Test Plan shall be delivered 10 working days prior to each planned test. Blk 14: Media Requirement: The shall be electronically delivered in MS Word Powerpoint, version 2007-2010, with e-mail notification to addressees.								NAVSEA 054		1	1	0	0
								NAVSEA 0541		1	1	0	0
15. TOTAL										2 2 0			
17. PRICE GROUP													
18. ESTIMATED TOTAL PRICE													
G. PREPARED BY Cynthia Strande, SEA 04512			H. DATE		I. APPROVED BY WILLIAM DONNA S 12208962			J. DATE					
DD FORM 1423-2, AUG 96 PREVIOUS EDITION MAY BE USED. Page ___ of ___ Pages Adobe Professional 8.0													

Contract Data Requirements List - Example 11 & 12

CONTRACT DATA REQUIREMENTS LIST <i>(2 Data Items)</i>										Form Approved OMB No. 0704-0188					
The public reporting burden for this collection of information is estimated to average 220 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government Printing Contracting Office for the Contract/PR No. listed in Block 4.															
A. CONTRACT LINE ITEM NO. 0001, 0002			B. EXHIBIT A		C. CATEGORY: TDP _____ TM _____ OTHER _____ IPSC _____										
D. SYSTEM/ITEM Highly Accurate Targeting System				E. CONTRACT/PR NO. N00024-12-D-12345				F. CONTRACTOR TBD							
1. DATA ITEM NO. A009	2. TITLE OF DATA ITEM SOFTWARE PRODUCT SPECIFICATION					3. SUBTITLE									
4. AUTHORITY (Data Acquisition Document No.) DI-IPSC-81441A				5. CONTRACT REFERENCE SOW para. 4.3.2.1				6. REQUIRING OFFICE NAVSEA 054							
7. DD 250 REQ LT		8. DIST STATEMENT REQUIRED C *		10. FREQUENCY ASREQ		12. DATE OF FIRST SUBMISSION 90 DAC		14. DISTRIBUTION							
8. APP CODE A *				11. AS OF DATE See Blk 16		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE							
16. REMARKS Blk 8: Approval will be for technical content. Government requires 30 days to review and Contractor has 30 days to incorporate changes and return to the Government. Blk 9: Distribution Statement C: Distribution authorized to Department of Defense and their Contractors (administrative or Operational Use as of 6-28-2012). Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC 20376. Blks 10, 11, 12 and 13: The specification first initial submission shall be 90 working days after contract start. All subsequent submission shall be 10 days after a changed is made to the baseline specification. Blk 14: Media Requirements: The specification shall be electronically delivered in MS Word version 2007-2010, e-mail notification to addressees.								Draft		Reg		Final			
								NAVSEA 054		1		1		0	
NAVSEA 0541		1		1		0									
15. TOTAL								2		2		0			
17. PRICE GROUP															
18. ESTIMATED TOTAL PRICE															
1. DATA ITEM NO. A010	2. TITLE OF DATA ITEM COMPUTER SOFTWARE PRODUCT END ITEM					3. SUBTITLE									
4. AUTHORITY (Data Acquisition Document No.) DI-MCCR-80700				5. CONTRACT REFERENCE SOW Para.3.5.4.1				6. REQUIRING OFFICE NAVSEA 054							
7. DD 250 REQ LT		8. DIST STATEMENT REQUIRED C *		10. FREQUENCY ASREQ		12. DATE OF FIRST SUBMISSION 120 DAC		14. DISTRIBUTION							
8. APP CODE A *				11. AS OF DATE N/A		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE							
16. REMARKS Block 8: Approval will be for technical content. The Government requires 15 working days to review. Contractor has 15 working days to incorporate any changes and return to the Government. Block 9: Distribution Statement C: Distribution authorized to the Department of Defense and their Contractors (Administrative or Operational Use) (as of 6-28-2012). Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC 20376. Blks 10, 12 and 13: The Product End Item, initial delivery shall be 120 days after contract start and 10 after a change is made to the baseline of the end item . Blk 14: Media Requirement: The Product End item shall be electronically delivered in MS Word Suite, version 2007-2010, with e-mail notification to addressees.								Draft		Reg		Final			
								NAVSEA 054		1		1		0	
NAVSEA 0541		1		1		0									
15. TOTAL								2		2		0			
17. PRICE GROUP															
18. ESTIMATED TOTAL PRICE															
G. PREPARED BY Cynthia Strande, SEA 04512			H. DATE		I. APPROVED BY WILLIAM.DORNAL.S.12208962 4				J. DATE						
DD FORM 1423-2, AUG 96			PREVIOUS EDITION MAY BE USED.				Page _____ of _____ Pages Advice Professional 8.0								

Contract Data Requirements List - Example 13 & 14

CONTRACT DATA REQUIREMENTS LIST <i>(2 Data Items)</i>										Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 220 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government Printing Office for the Contract/PR No. listed in Block E.</p>											
A. CONTRACT LINE ITEM NO. 0001, 0002		B. EXHIBIT A		C. CATEGORY: TDP _____ TM _____ OTHER _____ IPSC _____							
D. SYSTEM/ITEM Highly Accurate Targeting System			E. CONTRACT/PR NO. N00024-12-D-12345			F. CONTRACTOR TBD					
1. DATA ITEM NO. A013	2. TITLE OF DATA ITEM SOFTWARE RESOURCES DATA REPORTING INITIAL DEVELOPER REPORT AND DATA DICTIONARY				3. SUBTITLE						
4. AUTHORITY (Data Acquisition Document No.) DI-IPSC-81739B			5. CONTRACT REFERENCE SOW Para. 4.3.2.1			6. REQUIRING OFFICE NAVSEA 054					
7. DD 290 REQ LT		8. DDT STATEMENT REQUIRED		10. FREQUENCY MTHLY		12. DATE OF FIRST SUBMISSION 45 DAC		14. DISTRIBUTION			
8. APP CODE A*		C*		11. AS OF DATE 0*		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE		b. COPIES	
								Draft		Final	
								Reg		Repro	
16. REMARKS											
Blk 8: Approval will be for technical content. Government requires 15 days to review and Contractor has 15 days to incorporate changes and return to the Government.										NAVSEA 054 1 1 0	
Blk 9: Distribution Statement C: Distribution authorized to Department of Defense and their Contractors (Administrative or Operational Use as of 6-28-2012). Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC 20376.										NAVSEA 054I 1 1 0	
Blks 10, 11, 12 and 13: The report and data dictionary first initial submission shall be 45 working days after contract start and monthly thereafter. The report shall be delivered NLT than the end of the month.											
Blk 14: Media Requirements: The report shall be electronically delivered in MS Word version 2007-2010, e-mail notification to addressees.											
15. TOTAL										2 2 0	
1. DATA ITEM NO. A014	2. TITLE OF DATA ITEM CONTRACT FUNDS STATUS AND MANAGEMENT REPORT (CFSR)				3. SUBTITLE						
4. AUTHORITY (Data Acquisition Document No.) DI-MGMT-81468			5. CONTRACT REFERENCE SOW Para.3.5.4.1			6. REQUIRING OFFICE NAVSEA 054					
7. DD 290 REQ LT		8. DDT STATEMENT REQUIRED		10. FREQUENCY MTHLY		12. DATE OF FIRST SUBMISSION 45DAC		14. DISTRIBUTION			
8. APP CODE N/A		C*		11. AS OF DATE 0		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE		b. COPIES	
								Draft		Final	
								Reg		Repro	
16. REMARKS											
Block 9: Distribution Statement C: Distribution authorized to the Department of Defense and their Contractors (Administrative or Operational Use) (as of 6-28-2012). Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC 20376.										NAVSEA 054 1 1 0	
Blks 10, 12 and 13: The Status report initial delivery shall be 45 days after contract start and monthly thereafter. The report shall be delivered at the end of the month.										NAVSEA 054I 1 1 0	
Blk 14: Media Requirement: The report shall be electronically delivered in MS Word Suite, version 2007-2010, with e-mail notification to addressees.											
15. TOTAL										2 2 0	
G. PREPARED BY Cynthia Strande , SEA 04512			H. DATE		I. APPROVED BY WILLIAMS DONNA S (2208080)				J. DATE		

17. PRICE GROUP

18. ESTIMATED TOTAL PRICE

17. PRICE GROUP

18. ESTIMATED TOTAL PRICE

Contract Data Requirements List – Example 16 & 17

CONTRACT DATA REQUIREMENTS LIST <i>(2 Data Items)</i>										Form Approved OMB No. 0704-0188					
<p>The public reporting burden for this collection of information is estimated to average 220 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government Contracting Officer for the Contract/PR No. listed in Block 4.</p>															
A. CONTRACT LINE ITEM NO. 0001, 0002			B. EXHIBIT A		C. CATEGORY: TDP _____ TM _____ OTHER _____ MGMT _____			D. SYSTEM/ITEM Highly Accurate Targeting System				E. CONTRACT/PR NO. N00024-12-D-12345		F. CONTRACTOR TBD	
1. DATA ITEM NO. A011		2. TITLE OF DATA ITEM DATA ACCESSIONS LIST			3. SUBTITLE							17. PRICE GROUP			
4. AUTHORITY (Data Acquisition Document No.) DI-MGMT-81453A				5. CONTRACT REFERENCE SOW para. 4.3.2.1				6. REQUIRING OFFICE NAVSEA 054				18. ESTIMATED TOTAL PRICE			
7. DD 250 REQ LT		9. DIST STATEMENT REQUIRED C *		10. FREQUENCY ASREQ		12. DATE OF FIRST SUBMISSION 60 DAC		14. DISTRIBUTION				18. ESTIMATED TOTAL PRICE			
8. APP CODE N/A		11. AS OF DATE See Blk 16		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE		b. COPIES		18. ESTIMATED TOTAL PRICE					
16. REMARKS						NAVSEA 054		Draft		Final					
Blk 9: Distribution Statement C: Distribution authorized to Department of Defense and their Contractors (administrative or Operational Use as of 6-28-2012). Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC 20376.						NAVSEA 0541		0		1					
Blks 10, 11, 12 and 13: The Data Accession list first initial submission shall be 60 working days after contract start. All subsequent submission shall be 10 days after an additional piece of data is added to the list.								0		0					
Blk 14: Media Requirements: The list shall be electronically delivered in MS Word version 2007-2010, e-mail notification to addressees.															
15. TOTAL						2		2		0					
1. DATA ITEM NO. A012		2. TITLE OF DATA ITEM SOFTWARE TEST DESCRIPTION			3. SUBTITLE							17. PRICE GROUP			
4. AUTHORITY (Data Acquisition Document No.) DI-IPSC-81439A				5. CONTRACT REFERENCE SOW Para.3.5.4.1				6. REQUIRING OFFICE NAVSEA 054				18. ESTIMATED TOTAL PRICE			
7. DD 250 REQ LT		9. DIST STATEMENT REQUIRED C *		10. FREQUENCY ASREQ *		12. DATE OF FIRST SUBMISSION See Blk 16		14. DISTRIBUTION				18. ESTIMATED TOTAL PRICE			
8. APP CODE A*		11. AS OF DATE N/A		13. DATE OF SUBSEQUENT SUBMISSION See Blk 16		a. ADDRESSEE		b. COPIES		18. ESTIMATED TOTAL PRICE					
16. REMARKS						NAVSEA 054		Draft		Final					
Block 8: Approval will be for technical content. The Government requires 15 working days to review. Contractor has 15 working days to incorporate any changes and return to the Government.						NAVSEA 0541		1		1					
Block 9: Distribution Statement C: Distribution authorized to the Department of Defense and their Contractors (Administrative or Operational Use) (as of 6-28-2012). Other requests for this document shall be referred to NAVSEA 054, WNY, Washington, DC 20376.								0		0					
Blks 10, 12 and 13: The Software Test Description shall be delivered 10 days prior to the each test.															
Blk 14: Media Requirement: The shall be electronically delivered in MS Word Suite, version 2007-2010, with e-mail notification to addressees.															
15. TOTAL						2		2		0					
G. PREPARED BY Cynthia Strande, SEA 04512			H. DATE		I. APPROVED BY WILLIAM DORNIA S. (220906)			J. DATE							

DD FORM 1423-2, AUG 96

PREVIOUS EDITION MAY BE USED.

Page ___ of ___ Pages
Adobe Professional 8.0

Contract Data Requirements List - Example 18

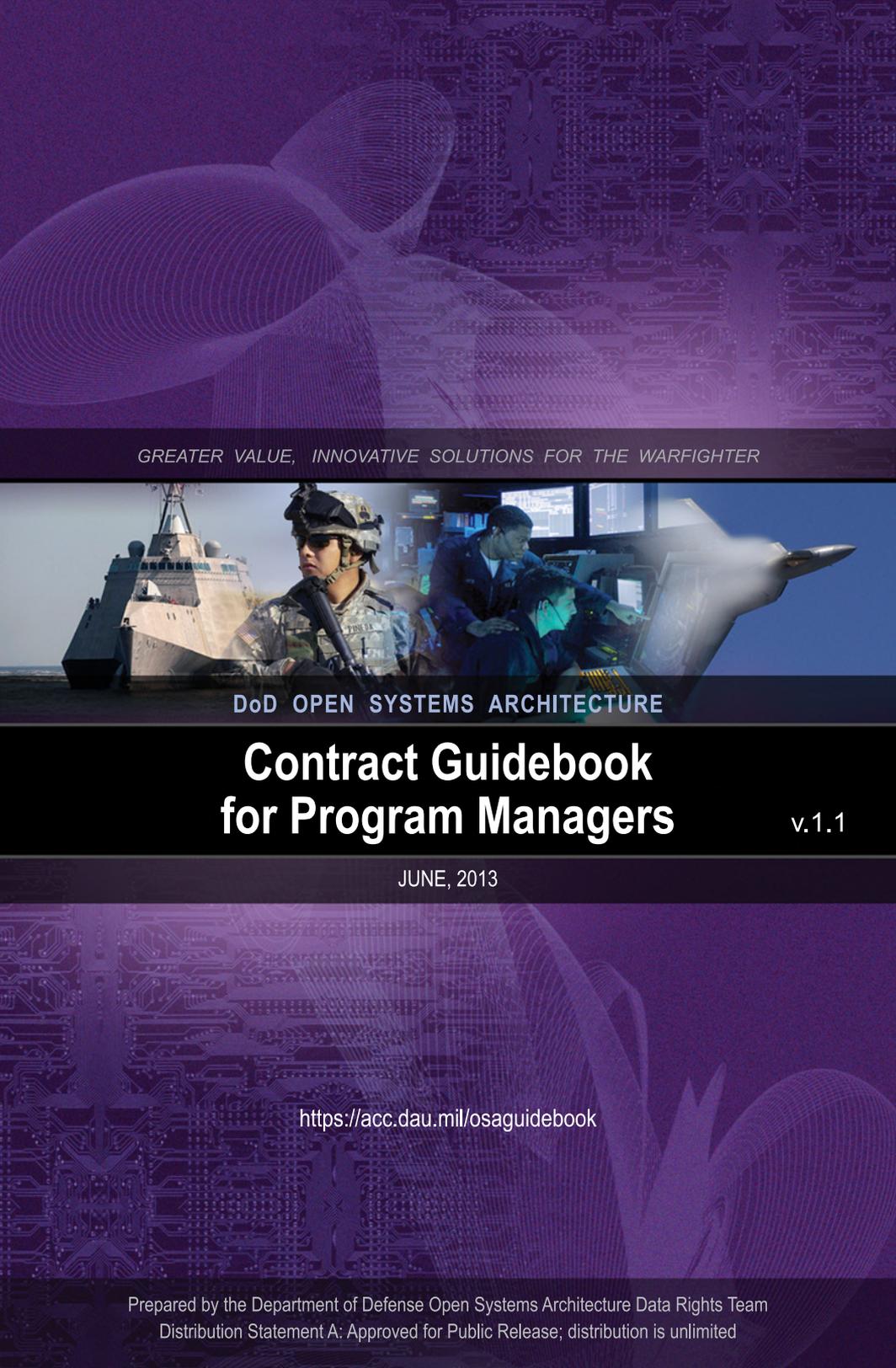
CONTRACT DATA REQUIREMENTS LIST (CDRL) (1 Data Item)										Form Approved OMB No. 0704-0188				
<p>The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed forms to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.</p>														
A. CONTRACT LINE ITEM NO. CLN - 0009			B. EXHIBIT A		C. CATEGORY: TDP ___ TM ___ OTHER ___ MGMT ___									
D. SYSTEM ITEM HIGHLY ACCURATE TARGETING SYSTEM				E. CONTRACT/PR NO. A1283C-11-D-0001			F. CONTRACTOR							
1. DATA ITEM NO. A061		2. TITLE OF DATA ITEM DATA ACCESSION LIST (DAL)				3. SUBTITLE								
4. AUTHORITY (Cite Acquisition Document No.) DI-MGMT-01453				5. CONTRACT REFERENCE 3.3.10.4 (SOW-010)			6. REQUIRING OFFICE ABCD-EFGH-IJKL-M-N							
7. DD 250 REQ LT		9. DIST STATEMENT REQUIRED D		10. FREQUENCY SEE 16 N/A		12. DATE OF FIRST SUBMISSION 180 DAC N/A		14. DISTRIBUTION						
8. APP CODE N/A				11. AS OF DATE N/A		13. DATE IF SUBSEQUENT SUBM. N/A		a. ADDRESSEE		b. COPIES				
<p>16. REMARKS Blk 9. For Dat St and Exp Wam see end of Exhibit A. Blks 10. Subsequent submissions shall be semi-annually. Blk 14. Submission via EDMS (3.3.10.4).</p>								Drat		Final		Reps		
								ABCD-EFGH-IJKL-M-N						1
								SEE 16						
15. TOTAL								0	0	1				
G. PREPARED BY ROBERT PALMER				H. DATE 15 Jun 2011		I. APPROVED BY BARBARA JENSON			J. DATE 25 Jun 2011					

17. PRICE GROUP

18. ESTIMATED TOTAL PRICE

Contract Data Requirements List - Example 19

CONTRACT DATA REQUIREMENTS LIST (CDRL) (1 Data Item)												Form Approved OMB No. 0704-0188					
The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government issuing Contracting Officer for the Contract/PR No. listed in Block E.																	
A. CONTRACT LINE ITEM NO. CLIN - 0116, 0212, 0312			B. EXHIBIT A			C. CATEGORY: TDP _____ TM _____ OTHER _____ JPSC _____											
D. SYSTEM/ITEM HIGHLY ACCURATE TARGETING SYSTEM				E. CONTRACT/PR NO. A12B3C-11-D-0001				F. CONTRACTOR									
1. DATA ITEM NO. 8019		2. TITLE OF DATA ITEM SOFTWARE TEST DESCRIPTION (STD)						3. SUBTITLE SOFTWARE QUALIFICATION TESTING						17. PRICE GROUP			
4. AUTHORITY (Cite Acquisition Document for.) DI-IPSC-81439					5. CONTRACT REFERENCE 3.4.8.2 [SOW-4953]					6. REQUIRING OFFICE ABCD-EFGH-IJKL-M-N					18. ESTIMATED TOTAL PRICE		
7. DD 250 REQ LT		9. DIST STATEMENT REQUIRED		10. FREQUENCY SEMA		12. DATE OF FIRST SUBMISSION SEE 10		14. DISTRIBUTION									
8. APP CODE A		D		11. AS OF DATE N/A		13. DATE IF SUBSEQUENT SUBM. N/A		a. ADDRESSEE			b. COPIES						
16. REMARKS BLK 8: GOVERNMENT APPROVAL OR DISAPPROVAL WITHIN 20 WORKING DAYS OF RECEIPT. SUBMIT REVISIONS AND COMMENT RESPONSES WITHIN 15 WORKING DAYS AFTER RECEIPT OF GOVERNMENT COMMENTS. BLK 9: FOR DIST ST AND EXP WARN SEE END OF EXHIBIT A. BLK 12: SUBMIT 90 DAYS AFTER LRIP OPTION EXERCISE. BLK 14: SUBMISSION VIA EDMS (3.3.10.4)								ABCD-EFGH-IJKL-M-N			Draft	Reg	Repro	Final			
								SEE 10						I			
								15. TOTAL			0	0	0	1			
G. PREPARED BY KEVIN TILLMAN				H. DATE 21 Jun 2011		I. APPROVED BY RYAN GOLDSTEIN				J. DATE 5 Jul 2011							
DD FORM 1423-1, FEB 2001				PREVIOUS EDITION MAY BE USED				Page ___ of ___ Pages									



GREATER VALUE, INNOVATIVE SOLUTIONS FOR THE WARFIGHTER

DoD OPEN SYSTEMS ARCHITECTURE

Contract Guidebook for Program Managers

v.1.1

JUNE, 2013

<https://acc.dau.mil/osaguidebook>

Prepared by the Department of Defense Open Systems Architecture Data Rights Team
Distribution Statement A: Approved for Public Release; distribution is unlimited