Air Force Data Rights Guidebook

SMART IP

2019

U.S. Air Force

Authored by: Intellectual Property Cross Functional Team chaired by SAF/AQ & SAF/GCQ

FOREWORD

This publication is intended to equip Air Force acquisition personnel to handle common issues encountered in the realm of intellectual property (IP) acquisition under the Defense Federal Acquisition Regulation Supplement (DFARS), particularly those issues surrounding rights in technical data and computer software. It is intended to complement rather than substitute for other Department of Defense (DoD) guidebooks on data rights. While those guidebooks may present basic information and considerations for planning and acquisition, this publication presents recurring issues that acquisition personnel can expect to face in the format of frequently asked questions. Each issue or question is followed by a suggested plan for dealing with that issue. Rather than being contemplative, the plans presented are intended to be actionable—not just a recitation of the rules. Unlike in other areas of defense acquisition, no one functional lead has the knowledge to resolve IP issues. The input and coordination of others are critical to understanding the scope of the issue, how it relates to a requirement or life-cycle objective, and what steps can and, more importantly, should be taken to resolve it.

That is the primary aim of this publication. Through action-oriented plans, acquisition personnel are equipped to make informed decisions with the aim of improving acquisition outcomes. Too often, approaches to resolving IP issues have limited the Air Force's ability to maintain and sustain its weapon systems. If as an Air Force we can avoid this undesirable outcome, we can better equip our fighting forces to defeat their adversaries in a superior fashion. That is a goal we all share, and one the suggested practices in this guide can make a reality.

UNDER SECRETARY OF THE AIR FORCE
WASHINGTON

21 Feb 2018

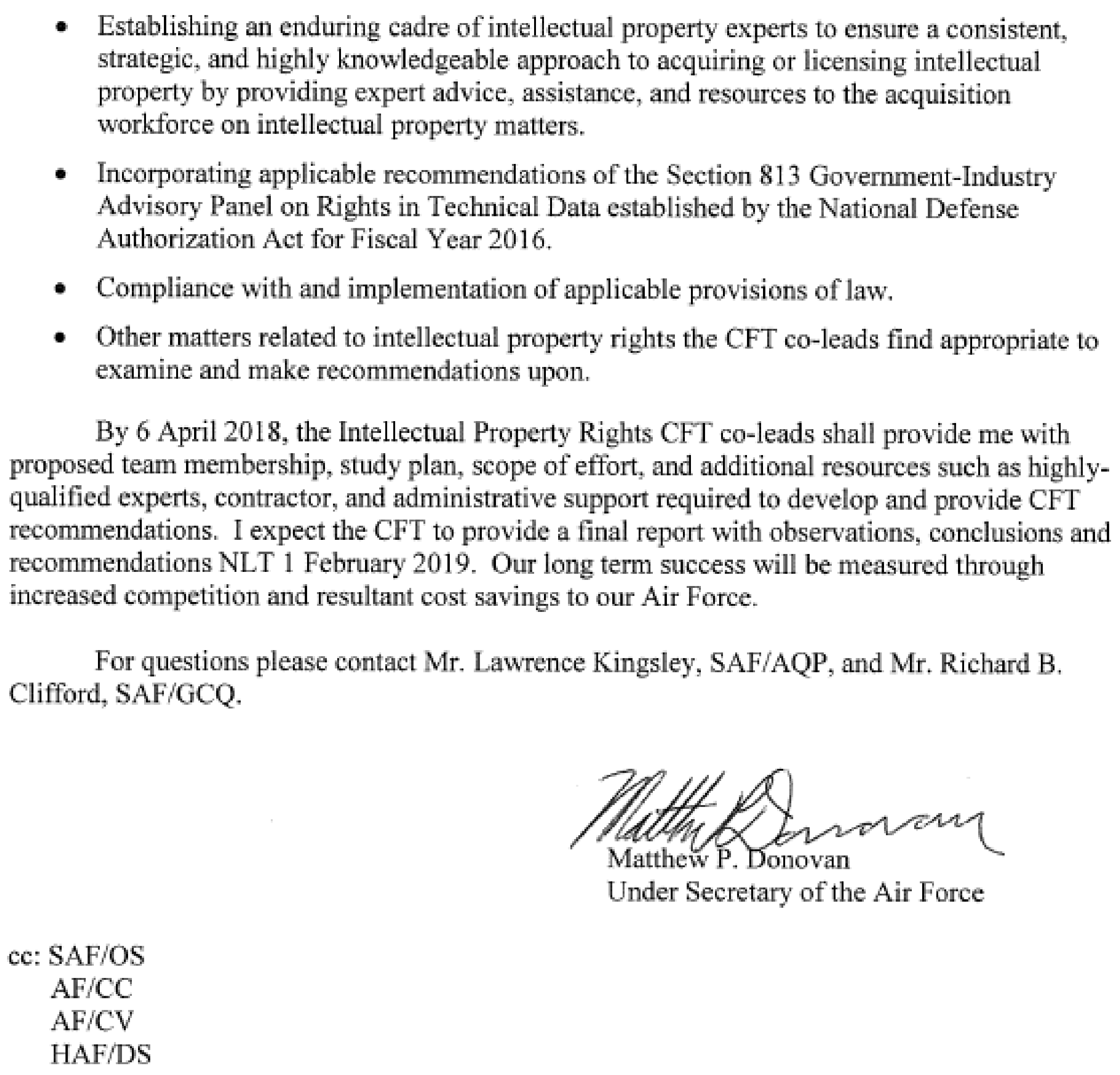
MEMORANDUM FOR SAF/AQ
SAF/GC
AF/JA
AFSPC/CC
AFMC/CC

SUBJECT: Intellectual Property Rights Cross Functional Team (CFT)

Obtaining adequate intellectual property license rights from our industry partners is critical to ensuring our major systems are affordable and adaptable to meet warfighter needs. Additionally, Congress is also concerned about these matters and recently wrote legislation encouraging customized intellectual property strategies. When we do not secure appropriate rights in technical data and computer software, we become dependent on incumbent contractors for the operation, maintenance, training, and sustainment of our major systems. Through these "vendor lock" actions, incumbent contractors can drive non-competitive prices for years or even decades after our major systems are deployed. We must prevent this by obtaining all appropriate intellectual property rights to which we are entitled and that Congress has deemed essential through legislative actions. By reducing extreme intellectual property licensing we can achieve significant cost savings by competing sustainment of our major programs throughout their life cycles.

I laud efforts to date to obtain intellectual property license rights necessary to develop, procure, and sustain our major systems. To further these efforts, I am establishing an Intellectual Property Rights Cross-Functional Team that will be co-led by SAF/AQ and SAF/GC, and composed of subject matter experts from SAF/AQ, SAF/GC, HAF/JA, Air Force Space Command, and Air Force Materiel Command. The CFT shall examine issues and make recommendations related to the following areas:

- Developing acquisition strategies and techniques for leveraging appropriate intellectual property rights to reduce "vendor lock" in program life cycles.
- Educating and training program managers, contracting officers, and source selection teams in identifying and negotiating intellectual property license rights needed to support future sustainment competitions, and capitalizing on the competitive environment to secure these rights at the lowest cost to the taxpayer.
- Assisting program managers in challenging improper vendor intellectual property assertions and proprietary markings on contract deliverable items.
- Ensuring Air Force regulations, instructions, and policies accurately and properly communicate to industry and our acquisition workforce our intellectual property needs for future sustainment and do not unreasonably hinder us from meeting those needs.



- Establishing an enduring cadre of intellectual property experts to ensure a consistent, strategic, and highly knowledgeable approach to acquiring or licensing intellectual property by providing expert advice, assistance, and resources to the acquisition workforce on intellectual property matters.
- Incorporating applicable recommendations of the Section 813 Government-Industry Advisory Panel on Rights in Technical Data established by the National Defense Authorization Act for Fiscal Year 2016.
- Compliance with and implementation of applicable provisions of law.
- Other matters related to intellectual property rights the CFT co-leads find appropriate to examine and make recommendations upon.

By 6 April 2018, the Intellectual Property Rights CFT co-leads shall provide me with proposed team membership, study plan, scope of effort, and additional resources such as highly-qualified experts, contractor, and administrative support required to develop and provide CFT recommendations. I expect the CFT to provide a final report with observations, conclusions and recommendations NLT 1 February 2019. Our long term success will be measured through increased competition and resultant cost savings to our Air Force.

For questions please contact Mr. Lawrence Kingsley, SAF/AQP, and Mr. Richard B. Clifford, SAF/GCQ.

Matthew P. Donovan
Under Secretary of the Air Force

cc: SAF/OS
AF/CC
AF/CV
HAF/DS

TABLE OF CONTENTS

Chapter 1 – Life-Cycle Planning for Intellectual Property (IP)

Background

In today's environment, interest in IP is high. Whether you find yourself in the Defense Department or industry, both seek IP with one aim in mind: to serve their interests. In industry, these interests may be framed in terms of profit and loss and long-term revenue. In the Defense Department, they are framed in terms of availability, cost, and long-term sustainability.

It is often said that contractors consider IP to be their "lifeblood." So much about a business enterprise could be described this way. Human capital and facilities capital are just as important as intellectual capital. But one form of intellectual capital is particularly important in the defense industry—namely the technical data and computer software for DoD's weapon systems. Obtaining delivery and appropriate rights in technical data and computer software are essential for DoD to operate, maintain, and sustain its systems, as well as to enable compliance with related statutory mandates. These activities go right to the heart of ensuring these systems are available, sustainable, and support a high level of readiness. Obtaining delivery and appropriate rights in technical data and computer software also allows DoD to compete certain life-cycle activities, and thus is key for realizing cost efficiencies throughout the life cycle.

Of course, if DoD is to attract contractors to meet defense requirements, then DoD must balance its interests with those of its contractors. Private capital will be brought to bear on defense problems only if offered an adequate return. The challenge has been to afford enough protections to technical data and computer software to offer such a return without sacrificing DoD's larger interests in furthering national security.

The DFARS seeks to address this challenge by providing guidance for determining the rights associated with technical data and software deliverables based on the nature of the data and its funding source. But rights in data and software are only part of a larger problem. That problem is how to meet the department's needs for life-cycle management. And solving it begins with careful planning—the subject of this chapter.

1.1. Incorporating IP into the Acquisition Strategy and Related Documents

A successful acquisition begins with planning, and acquisition planning culminates in an Acquisition Strategy. To meet DoD's needs for life-cycle support, an Acquisition Strategy should identify the needs for the product life cycle and chart a course for meeting them. It is vital that, in so doing, the Acquisition Strategy address needs for technical data and computer software.

Acquiring the right technical data and computer software is essential for ensuring Air Force systems will remain affordable and sustainable. Thus, these needs should be addressed in the Acquisition Strategy, or more specifically, the IP Strategy.

The IP Strategy covers almost every functional area within a Program Management Office (PMO), such as acquisition, financial, contracting, logistics, testing, and engineering, and it should contemplate the entire life cycle, not just the immediate requirements of the contract or PMO. As described in DoDI 5000.02, the IP Strategy should "identify and manage the full spectrum of IP and related issues (e.g., technical data and computer software deliverables, patented technologies, and appropriate license rights) from the inception of a program and throughout the life cycle. . . . [It] will be updated throughout the entire product life cycle, initially as part of the Acquisition Strategy, and during the Operations and Support Phase as part of the Life-Cycle Sustainment Plan." In other words, the IP Strategy is a living document that evolves throughout the life cycle. It contains all the critical thinking of the various subject matter experts (SMEs) within the PMO to ensure the system does not experience "vendor" lock, and can be properly sustained throughout its life cycle. While an IP strategy is a statutory requirement for all ACAT I and ACAT II programs as part of the Acquisition Strategy, all programs should analyze IP requirements as a part of their overall life-cycle plans.

1.1.1. I work in a PMO, and I am not sure how the IP Strategy should be integrated into the other acquisition, logistics, test, engineering, and contracting documents? How do these various documents fit together?

Response
All the various acquisition documents required by the PMO can fit together and relate to the IP Strategy in the following ways. For more information about these documents, refer to DoDI 5000.02.

- *Acquisition Strategy/Plan:* Within the Acquisition Strategy, the IP Strategy is represented as a summary section that is updated throughout the life cycle.

- *Life Cycle Sustainment Plan (LCSP):* Certain IP and rights will be necessary to execute the sustainment plan. Examine how the LCSP plans to satisfy each of the Integrated Product Support Elements and ensure that the IP Strategy seeks the rights and deliverables needed to execute these plans. Early in the acquisition process, specific support strategies may not have been decided. In this situation, it is critical to obtain the IP rights and deliverables that keep sustainment options open. When the system enters into the Operation and Support phase, the IP Strategy will become an annex to the LCSP.

- *Request for Proposals (RFP)/Contract:* The IP Strategy should map to contract requirements in the RFP. If it does not, offerors will be unable to meaningfully propose to these requirements, and the Air Force risks not being able to meet its life-cycle needs. For example, the Statement of Work (SOW) in a product development contract should require, along with the development activities, the creation and delivery of the associated technical data and computer software. Because these issues can dominate life-cycle decisions later, evaluation factors related to IP and life-cycle support, as well as associated agreements, should be included.

- *Contract:* Within the contract, technical data and computer software requirements found in the SOW must be delivered by inclusion of a Contract Data Requirement List (CDRL), DD Form 1423, in the contract attachments. CDRLs state, among other things, format and content of the deliverable. It is a best practice to ensure that the CDRLs are mapped to deliverable requirements in the SOW so that the contractor is required by the contract to deliver all required technical data and computer software.

In addition to the IP Strategy, other acquisition and program documents can be a requirement source and assist with identifying requirements to be included in the contract. A few relevant examples include:

- *Engineering Documents* such as the System Engineering Plan (which addresses topics like Modular Open System Architecture needs), test plans, technical baseline documentation (such as interface control documents, item specifications, and various performance requirements), software documentation, and other engineering documents.

- *Logistics Planning Documents* such as the LCSP (which documents the entire product support strategy) can be particularly useful for identifying product support needs and options for meeting them. If depot maintenance may be required, more technical data and computer software requirements may exist than for other maintenance concepts. Also, development of logistics plans can make apparent what technical data and software will be required for effective life-cycle support.

- Other documents like the *Program Protection Plan* and *Financial Documents* (e.g., Program Objective Memorandum and budget requests) can include information relevant to the IP Strategy, including references to critical program information, costs for data and storage, and additional information regarding development, production, and sustainment.

1.1.2. What should the Acquisition Strategy address regarding IP?

Response
DoDI 5000.02 identifies the content required in the IP Strategy. The instruction requires a holistic consideration of life-cycle needs and their distillation into an actionable plan, the what, how, and why of life-cycle support.

- What: Analyze the data required to design, manufacture, and sustain the system as well as to support re-competition for production, sustainment, or upgrade. Consider baseline documentation data, analysis data, cost data, test data, results of reviews, engineering data, drawings, models, and bills of materials.

- How: Address how the program will provide for delivery of technical data with the appropriate level of rights the government requires for the system's total life-cycle sustainment. Include analysis of data needs to implement the product support life-cycle strategy including such areas as materiel management, training, information assurance protection, cataloging, open architecture, configuration management, engineering, technology refreshment, maintenance/repair within the technical order (TO) limits and specifically engineered outside of TO limits, and reliability management.

- Why: The business case analysis calculation, conducted in concert with the engineering tradeoff analysis, outlines the approach for using open systems architectures and acquiring IP rights. The cost benefit analysis explains whether to include a priced contract option for the future delivery of technical data and IP rights not acquired upon initial contract award. An analysis of the risk that the contractor may assert limitations on the government's use and release of technical data or computer software (e.g., technical data and computer software developed exclusively at the contractor's expense) factors into the strategy.

Once these aspects of the life cycle are analyzed, the results are included in the IP Strategy, producing a strategy that addresses what data is required to support acquisition and sustainment strategies, how data quality will be managed, data format, how the program will verify markings, and how the data will be stored. As the program matures, the IP Strategy will be updated in the Acquisition Strategy and LCSP to reflect the changes.

1.1.3. If a program has been approved as a Rapid Acquisition Program (Section 804), how does that affect the IP Strategy?

Response
Rapid Acquisition authorities typically give PMOs leeway to select requirements and procedures deemed most appropriate to the acquisition. For example, AFGM2018-63-146-01, *Air Force Guidance Memorandum for Rapid Acquisition Activities*, section 1.2., dated 13 June 2018, states that, "[m]any encouraged steps or practices may not apply to specific rapid acquisition activities. The PM and [Milestone Decision Authority] should tailor rapid acquisition activities to the strategies, reviews, metrics and operating thresholds that make sense for the program in question."

With the focus on speed in rapid acquisition environments, it is even more critical that the program consider long-term support requirements. PMOs should develop IP Strategies that reflect a careful consideration of the necessary technical data and computer software for the new weapon system or program to be sustained throughout its life cycle. The PMO must acquire technical data and computer software that are needed to ensure the program can meet all its goals—both short term and long term.

1.1.4. How does the IP Strategy promote competition and prevent "vendor lock" for purposes of life-cycle support?

Response

While this is a straightforward question, the response unfortunately is not. IP considerations are often complex, and every Air Force procurement is unique. The IP Strategy lays out how the Air Force will acquire, sustain, and maintain the system and promote competition where practical.

For example, consider that a new system is being procured by the Air Force, but the system depends heavily on software (i.e., it contains a large amount of computer software source code and object code). The PMO via the IP Strategy Integrated Product Team (IPT) conducts a cost analysis and determines that it would be much more cost effective to have various vendors or government activities maintain, upgrade, and manage the computer software source code and object code over the life cycle of that system.

The IPT develops a comprehensive IP Strategy document/plan to promote competition by:

- Including specific language in the RFP that states the requirement that the PMO deliver computer source code and object code to other companies/vendors or government activities for purpose of maintenance, upgrade, and management, and
- Including an evaluation factor addressing software deliverables and rights (e.g., that evaluated whether the offeror would deliver the necessary computer source code and object code and how well the rights the offeror agrees to grant to the Government meet this requirement.

The best solution addressing this requirement in the RFP would require the contractor to design the weapon system consistent with Modular Open System Approach principles and then obtain the appropriate CDRL deliverables (and government purpose rights (GPR) or unlimited rights (UR) to those deliverables).

For this to occur, the IP Strategy document/plan requires the proper CDRLs to be developed for the computer software source code, object code, and documentation, and requires the mapping of each CDRL to rights the Air Force would receive in the deliverables under that CDRL. Both the CDRLs and data rights mapping are requirements of the RFP. Finally, the Air Force's PMO reviews all data rights markings on the computer source code, object code, and computer software documentation at time of delivery to confirm there are no nonconforming or unjustified markings. If any nonconforming or unjustified markings are included on the deliverables, the PMO pursues the contractual remedies to address the contractor's contractual failure so that the Air Force can provide properly marked deliverables to another contractor to use, maintain, or upgrade the computer software source code and object code.

The Strategy

To prevent "vendor lock" and promote competition/organic sustainment, the PMO should:

Step 1: Establish an IPT, consisting of a cross-functional team of SMEs and led by a data manager with a strong background in IP and IP rights. IPT members should be knowledgeable in technical data and computer software, IP rights, the system's architecture (both hardware and software), and why the data are needed.

Step 2: Issue a data call to identify what data are necessary for sustainment and future competition of the system or subsystems. Consider whether specially negotiated licenses could be used effectively to support the product support strategy. Figures 1 and 2 present flow charts that the IPT could use to determine the deliverables and required rights.

Step 3: Conduct a Data Requirements Review Board in accordance with DoD 5010.12-M to ensure the data and software requirements in the IP Strategy are authenticated. Questions to be presented include: "What data are needed? Why the data are needed? For what purpose will the data be used?"

Step 4: Conduct a cost analysis and determine the most cost effective means for maintaining, upgrading, and managing the system over its life cycle. Consider options including the original equipment manufacturer (OEM), other sources, or government activities.

Step 5: Include the IPT's plan to promote competition in the Acquisition Strategy and the LCSP, addressing all functional areas (i.e., logistics, engineering, cost, program management, risks, testing, and contracting documents (SOW/RFP/Contract/CDRLs)).

Step 6: Develop the proper CDRLs for technical data and computer software (e.g., source code, object code, executable code, and documentation).

Step 7: Prior to entry into Milestone A or B, integrate the IP Strategy into the RFP and any applicable programmatic documents. Within the Source Selection Plan, consider requiring delivery of technical data, computer software, contract and management data the IPT has identified as necessary, and evaluation factor(s) assessing the associated rights the offeror proposes to provide.

Step 8: When drafting the SOW, RFP, and contract:

- Include specific language in the RFP explaining the technical data and computer software requirements, including whether the PMO will need to provide data or source code to other companies or government activities;
- Require offerors to implement a Modular Open Systems Approach to acquire a system with severable modules that the program can compete separately and interfaces developed to open standards (see sections 1.1.5. and 1.1.6. discussing Modular Open Systems Approaches);
- Require, via CDRLs, delivery of all mandatory technical data and computer software. For example, include CDRLs with data item descriptions requiring delivery of interface control documents and application programming interfaces (e.g., for computer software IEEE STD 12207);
- Require offerors to include in their proposals a list/table mapping CDRLs to rights the Air Force would receive in the deliverables;
- Include the Deferred Delivery clause (DFARS 252.227-7026), which allows the Air Force to defer delivery of identified technical data or computer software deliverables, as well as the Deferred Ordering clause (DFARS 252.227-7027) in the model contract if appropriate;
- Include in the RFP the mandatory Data Rights Assertions clause (DFARS 252.227-7017), which requires offerors to identify all noncommercial technical data and computer software that will be delivered to the Air Force with less than UR;
- Consider modifying the data rights assertions requirements (e.g., via special H clause, to mandate that offerors provide assertions for commercial technical data and commercial computer software in the same format as for noncommercial deliverables and submit any licenses for commercial software with their proposal); and
- Ensure a CDRL requiring delivery of a data accession list is included in the model contract.

Step 9: Prior to releasing the RFP, conduct an Industry Day to clearly articulate requirements for technical data and computer software delivery and the associated rights desired. Provide industry with opportunities to offer feedback on all IP issues.

Step 10: Use industry feedback to revise the RFP.

Step 11: Thoroughly train all members of your technical evaluation team to ensure understanding of the requirements and evaluation factors related to technical data, computer software, and associated rights.

Step 12: Engage in meaningful discussions during the evaluation to ensure the evaluation team understands the offerors' proposed delivery of technical data, computer software, and associated rights.

Step 13: After award, create a spreadsheet (see Figure 3 as an example) to list the Work Breakdown Structure (WBS) elements of the new system. Each element will map to:

- The data or software needed (depot, intermediate, organizational maintenance)
- The specific drawing number or computer software source code version
- The specific IP rights license to that drawing or computer software source code version

Step 14: Before acceptance of deliverables, the PMO reviews all data rights markings on the technical data or computer software to identify any nonconforming or unjustified markings. If the deliverables contain any nonconforming or unjustified markings, the PMO should pursue contractual remedies to address the contractor's failure to meet contract requirements and require the contractor to provide properly marked (or unmarked) documents.

Figure 1. Determining IP Needs

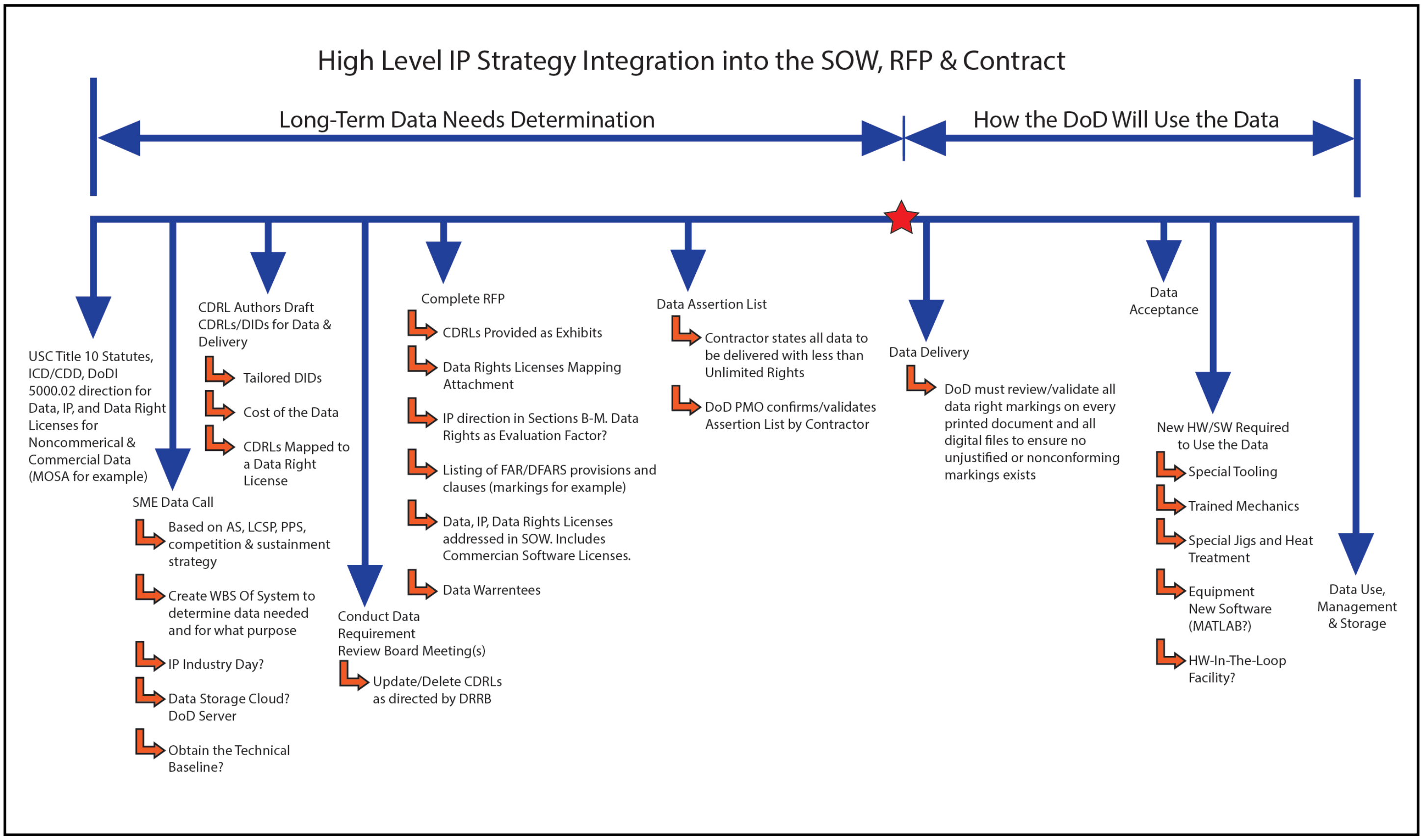
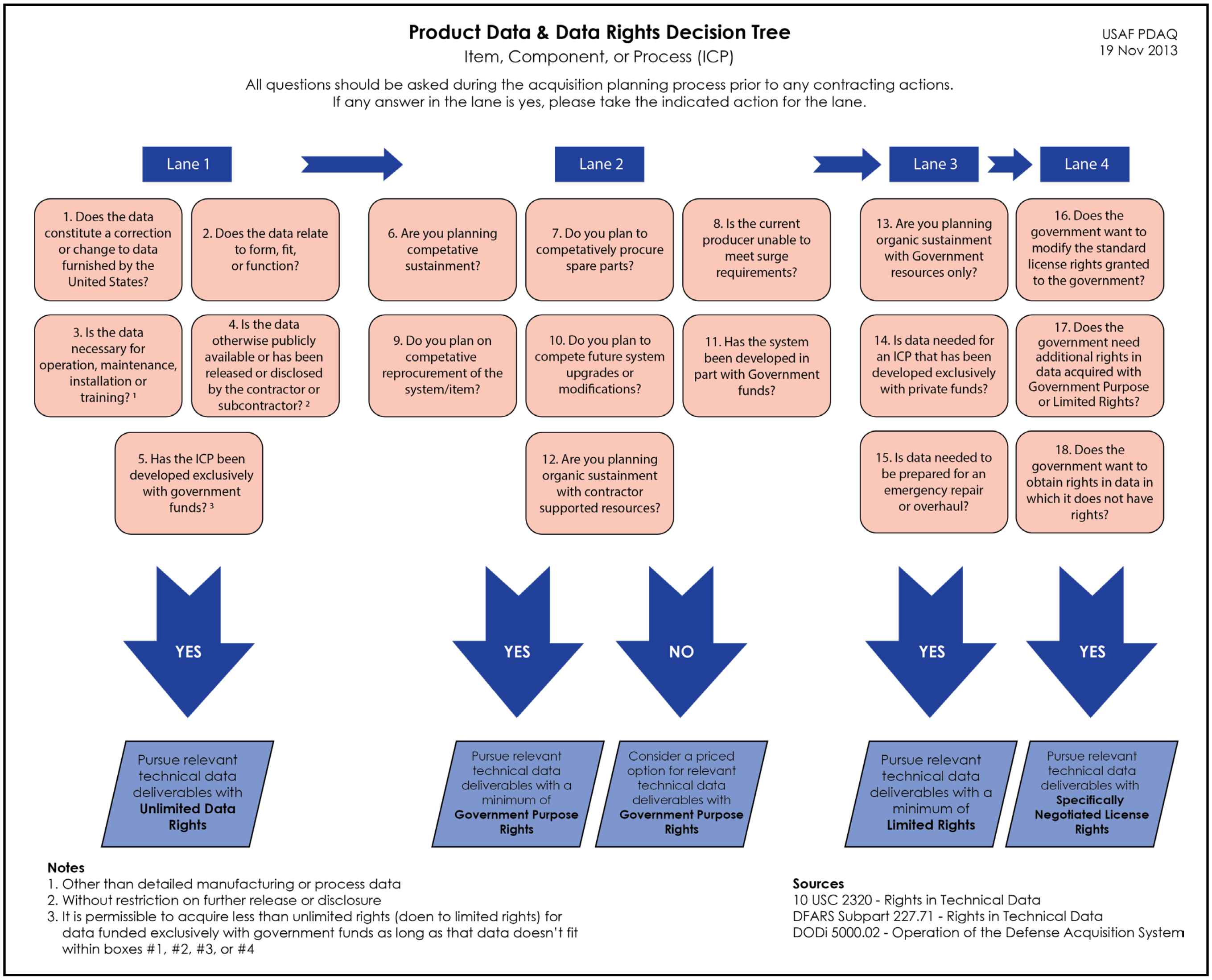

High Level IP Strategy Integration into the SOW, RFP & Contract
Long-Term Data Needs Determination
How the DoD Will Use the Data
USC Title 10 Statutes, ICD/CDD, DoDI 5000.02 direction for Data, IP, and Data Right Licenses for Noncommercial & Commercial Data (MOSA for example)
SME Data Call
Based on AS, LCSP, PPS, competition & sustainment strategy
Create WBS Of System to determine data needed and for what purpose
IP Industry Day?
Data Storage Cloud? DoD Server
Obtain the Technical Baseline?
CDRL Authors Draft CDRLs/DIDs for Data & Delivery
Tailored DIDs
Cost of the Data
CDRLs Mapped to a Data Right License
Conduct Data Requirement Review Board Meeting(s)
Update/Delete CDRLs as directed by DRRB
Complete RFP
CDRLs Provided as Exhibits
Data Rights Licenses Mapping Attachment
IP direction in Sections B-M. Data Rights as Evaluation Factor?
Listing of FAR/DFARS provisions and clauses (markings for example)
Data, IP, Data Rights Licenses addressed in SOW. Includes Commercian Software Licenses.
Data Warrentees
Data Assertion List
Contractor states all data to be delivered with less than Unlimited Rights
DoD PMO confirms/validates Assertion List by Contractor
Data Delivery
DoD must review/validate all data right markings on every printed document and all digital files to ensure no unjustified or nonconforming markings exists
Data Acceptance
New HW/SW Required to Use the Data
Special Tooling
Trained Mechanics
Special Jigs and Heat Treatment
Equipment New Software (MATLAB?)
HW-In-The-Loop Facility?
Data Use, Management & Storage

Figure 2. Product Data and Data Rights Decision Tree



Product Data & Data Rights Decision Tree

Item, Component, or Process (ICP)

USAF PDAQ
19 Nov 2013

All questions should be asked during the acquisition planning process prior to any contracting actions.
If any answer in the lane is yes, please take the indicated action for the lane.

Lane 1

1. Does the data constitute a correction or change to data furnished by the United States?

2. Does the data relate to form, fit, or function?

3. Is the data necessary for operation, maintenance, installation or training? [1]

4. Is the data otherwise publicly available or has been released or disclosed by the contractor or subcontractor? [2]

5. Has the ICP been developed exclusively with government funds? [3]

YES → Pursue relevant technical data deliverables with **Unlimited Data Rights**

Lane 2

6. Are you planning competative sustainment?

7. Do you plan to competatively procure spare parts?

8. Is the current producer unable to meet surge requirements?

9. Do you plan on competative reprocurement of the system/item?

10. Do you plan to compete future system upgrades or modifications?

11. Has the system been developed in part with Government funds?

12. Are you planning organic sustainment with contractor supported resources?

YES → Pursue relevant technical data deliverables with a minimum of **Government Purpose Rights**

NO → Consider a priced option for relevant technical data deliverables with **Government Purpose Rights**

Lane 3

13. Are you planning organic sustainment with Government resources only?

14. Is data needed for an ICP that has been developed exclusively with private funds?

15. Is data needed to be prepared for an emergency repair or overhaul?

YES → Pursue relevant technical data deliverables with a minimum of **Limited Rights**

Lane 4

16. Does the government want to modify the standard license rights granted to the government?

17. Does the government need additional rights in data acquired with Government Purpose or Limited Rights?

18. Does the government want to obtain rights in data in which it does not have rights?

YES → Pursue relevant technical data deliverables with **Specifically Negotiated License Rights**

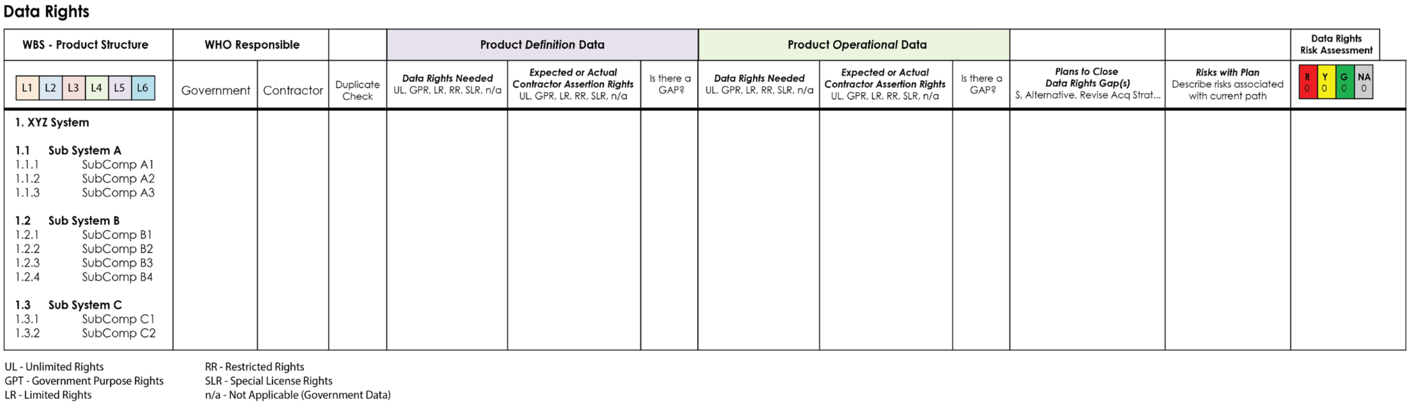
Notes

1. Other than detailed manufacturing or process data
2. Without restriction on further release or disclosure
3. It is permissible to acquire less than unlimited rights (doen to limited rights) for data funded exclusively with government funds as long as that data doesn't fit within boxes #1, #2, #3, or #4

Sources

10 USC 2320 - Rights in Technical Data
DFARS Subpart 227.71 - Rights in Technical Data
DODi 5000.02 - Operation of the Defense Acquisition System

Figure 3. Work Breakdown Structure and Data Rights (source: NAVAIR's "DR SAVE" program)



Data Rights

WBS - Product Structure	WHO Responsible			Product *Definition* Data			Product *Operational* Data					Data Rights Risk Assessment
L1 L2 L3 L4 L5 L6	Government	Contractor	Duplicate Check	***Data Rights Needed*** UL, GPR, LR, RR, SLR, n/a	***Expected or Actual Contractor Assertion Rights*** UL, GPR, LR, RR, SLR, n/a	Is there a GAP?	***Data Rights Needed*** UL, GPR, LR, RR, SLR, n/a	***Expected or Actual Contractor Assertion Rights*** UL, GPR, LR, RR, SLR, n/a	Is there a GAP?	***Plans to Close Data Rights Gap(s)*** S, Alternative, Revise Acq Strat...	***Risks with Plan*** Describe risks associated with current path	R 0 · Y 0 · G 0 · NA 0
1. XYZ System **1.1 Sub System A** 1.1.1 SubComp A1 1.1.2 SubComp A2 1.1.3 SubComp A3 **1.2 Sub System B** 1.2.1 SubComp B1 1.2.2 SubComp B2 1.2.3 SubComp B3 1.2.4 SubComp B4 **1.3 Sub System C** 1.3.1 SubComp C1 1.3.2 SubComp C2												

UL - Unlimited Rights
GPT - Government Purpose Rights
LR - Limited Rights

RR - Restricted Rights
SLR - Special License Rights
n/a - Not Applicable (Government Data)

1.1.5. How do I implement a Modular Open System Approach (MOSA) within the Program Office?

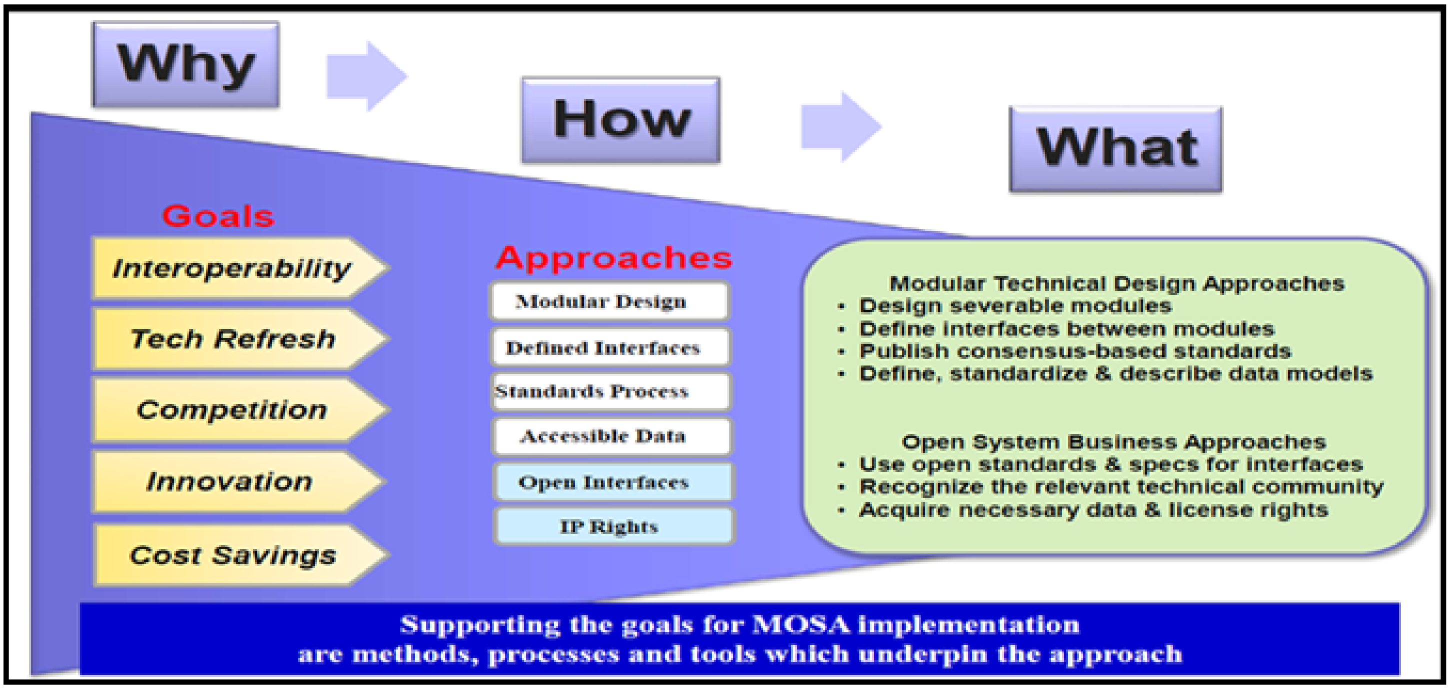
Response

The purpose of MOSA is to increase competition among system developers through the use of open standards and published interfaces. "Open standards" are widely accepted and supported standards set by recognized standards organizations or the marketplace. These standards support interoperability, portability, and scalability and are available to the general public at no cost or with a moderate license fee.

The goal of MOSA is to prevent vendor lock, or vendor lock-in. This is the situation in which a PMO depends on a single manufacturer or supplier. The organization cannot compete the associated work or obtain substitute supplies from another source (contractor or organic) without unacceptable costs or administrative burden. This dependency is typically a result of standards that are controlled by the vendor (i.e., manufacturer or supplier) or limited access to information due to 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 PMO at a significant disadvantage in obtaining competitive pricing.

Figure 4 provides a high-level flow depicting the goals, approaches, and business approaches in implementation of MOSA.

Figure 4. Implementing MOSA


Why
How
What
Goals
Interoperability
Tech Refresh
Competition
Innovation
Cost Savings
Approaches
Modular Design
Defined Interfaces
Standards Process
Accessible Data
Open Interfaces
IP Rights
Modular Technical Design Approaches
• Design severable modules
• Define interfaces between modules
• Publish consensus-based standards
• Define, standardize & describe data models
Open System Business Approaches
• Use open standards & specs for interfaces
• Recognize the relevant technical community
• Acquire necessary data & license rights
Supporting the goals for MOSA implementation
are methods, processes and tools which underpin the approach

Over the past two decades, the DoD has become aware that a weapon system's architecture can be designed to significantly enhance the DoD's ability to achieve agility, rapid capability enhancement, interoperability, increased competition, and lower costs over the life cycle of the program. As a result, DoDI 5000.02 Change 3 now requires, to the maximum extent feasible and cost effective, program managers to apply an "open" systems approach to design development that results in modular, interoperable systems that allow components to be added, modified, replaced, removed, and supported by different vendors throughout each system's life cycle, thereby reducing dependency on the original developer's data.

In recent years, Congress has enacted several provisions affecting DoD's rights in technical data and imposing related requirements. These have included provisions setting forth directions and requirements for DoD to implement MOSA in major defense acquisition programs, as well as establishing rights in certain major system interfaces used in a MOSA (e.g., FY17 NDAA Section 805 (10 USC 2446a and 2446b); FY17 NDAA Section 809 (10 USC 2320(a)(2)(F) and (a)(2)(G)). As of the date of publication of this Guide, these changes have not been implemented in the DFARS. Due to the complexity of this area and ongoing statutory and regulatory changes, it is strongly recommended that any program that may be subject to these requirements consult legal counsel as soon in the planning process as possible to determine any program impacts that may result from these changes.

The Acquisition Strategy document of the weapon system should identify where, why, and how a MOSA will or will not be used in the program.

If the PMO pursues a MOSA, the RFP and resulting contract must also contain the appropriate MOSA language. Although somewhat dated, one reference that may assist the PMO and Contracting Officer in implementing MOSA is the Open Systems Architecture Contract Guidebook for Program Managers, Version 1.1, May 2013. This Guidebook should be used by the acquisition community to incorporate MOSA principles and practices into the acquisition of systems and services. The Guidebook 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.

The Strategy

The Acquisition Strategy document of the weapon system should identify where, why, and how a MOSA will or will not be used in the program. If the PMO pursues a MOSA, the RFP and resulting contract must also contain the appropriate MOSA language. Specific considerations include:

Step 1: Maximize Competition. The program should compete any of the current work that can be done by other contractors. Possibilities for competition for post-Milestone C vendor-locked programs include system upgrades, technology insertion, operations and maintenance support, training, and other sustainment activity. Secondary benefits to maximizing competition 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, however, there must be a credible opportunity for the work to go to another vendor through competition.

For new programs, a key strategy to prevent vendor lock includes openly communicating PMO's intent to maximize competition throughout the program's life cycle. At a minimum, this should be included in the Acquisition Strategy. Even if an incumbent remains as the prime contractor, the mere possibility of competition when clearly articulated should lead to secondary benefits.

Step 2: Establish a Flexible Contracting Approach. Use a performance-based contracting approach to acquire open interface standards. The Open Systems Architecture Contract Guidebook for Program Managers provides some useful recommendations. For more general information on performance-based contracting, see DoD Standardization Document (SD) 15, Guide for Performance Specifications, Defense Standardization Program August 24, 2009. This approach calls for offerors to propose a plan describing how they will produce open-architecture-compliant software. Additionally, refer to MIL-STD-961E and MIL-HDBK-520A for more guidance.

Use a detailed specification contracting approach to acquire open-interface-standard-compliant software based on a specified standard such as the Air Force Open Mission Standard (OMS), Future Airborne Capability Environment (FACE), or Sensor Open Systems Architecture (SOSA).

Step 3: Require Delivery of Data with Appropriate Rights. Contracts that require delivery of technical data or computer software should include specific delivery requirements for all data or software, with the appropriate level of rights, necessary to meet the program's requirements for the life cycle of the program. For hardware, the Air Force, regardless of the source of funding, is entitled to UR to technical data that is form, fit, and function (FFF) data (e.g., interface data) or technical data necessary for operation, maintenance, installation, and training (OMIT) that is not detailed manufacturing or process data.

In some cases, however, programs have failed to complete the necessary first step to being able to exercise the Air Force's rights as a means to break a vendor lock relationship: to order or include delivery requirements for technical data or computer software, including data or software produced by Government-funded development tasks, FFF data, OMIT data, etc. By requiring delivery of this data and software, the PMO may be able to break out of vendor lock situations and compete for some supplies/services. For those programs that may be trying to prevent vendor lock, ensuring that contracts contain the appropriate language for delivery of necessary technical data and computer software up front is vitally important.

Step 4: Develop a Common Architecture. A common architecture can be developed across a product line or similar Programs of Record. In order to get the most benefit, preventing vendor lock, a common architecture should typically be completed early in the course of acquisition planning. 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, with more opportunities to compete across a standardized, well defined, common architecture. This approach will permit economies of scale and improved learning to enhance prospects for innovation and reduced costs.

1.1.6. My Program Office is planning to use a Modular Open System Approach (MOSA) for our next acquisition. I know that interface data is critical in effectively implementing a MOSA. How can my Program Office acquire and manage the necessary interface data?

Response

Reviewing a few definitions may be useful. 10 USC 2446a, *Requirement for modular open system approach in major defense acquisition programs; definitions*, provides definitions for a Major System Component, Major System Interface, and a Major System Platform.

Major System Component

A high-level subsystem or assembly, including hardware, software, or an integrated assembly of both, that can be mounted or installed on a major system platform through well-defined major system interfaces.

Major System Interface

A shared boundary between a major system platform and a major system component, between major system components, or between major system platforms, defined by various physical, logical, and functional characteristics, such as electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software elements, that is characterized clearly in terms of form, function, and the content that flows across the interface in order to enable technological innovation, incremental improvements, integration, and interoperability.

Major System Platform

The highest level structure of a major weapon system that is not physically mounted or installed onto a higher level structure and on which a major system component can be physically mounted or installed.

The term "interface" is often used when discussing MOSA, although the precise meaning given to the term may vary.

Interface

The functional and physical characteristics required to exist at a common boundary or connection between persons, between systems, or between persons and systems; or,

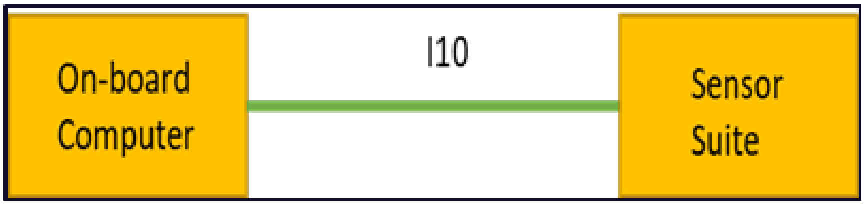
A system external to the system being analyzed that provides a common boundary or service necessary for the other system to perform its mission in an un-degraded mode (e.g., a system that supplies power, cooling, heating, air service, or signal inputs). (Source: *International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) Standard 24765:2010: Systems and Software Engineering – Vocabulary*)

Another definition of an interface:

An interface is a place at which independent systems or components thereof meet and act or communicate with each other. An interface is characterized by two terminals, each touching one element in the system architecture or environment, and a media of communication. The interface is completed between these terminals via an interface media such as physical contact, electrical signals in wiring, fluid flow in plumbing, or a radio signal in space. The interface is not the media itself, rather the functionality facilitated by the media. Every interface in a system can be said to have a source, a destination, and a media. (See, *System Requirements Analysis*, Jeff O. Grady, 2006)

Figure 5 is a graphical representation of an interface: two terminals (on-board computer and sensor suite) with the media between the two terminals (28-volt direct current).

Figure 5. Top Level – Schematic

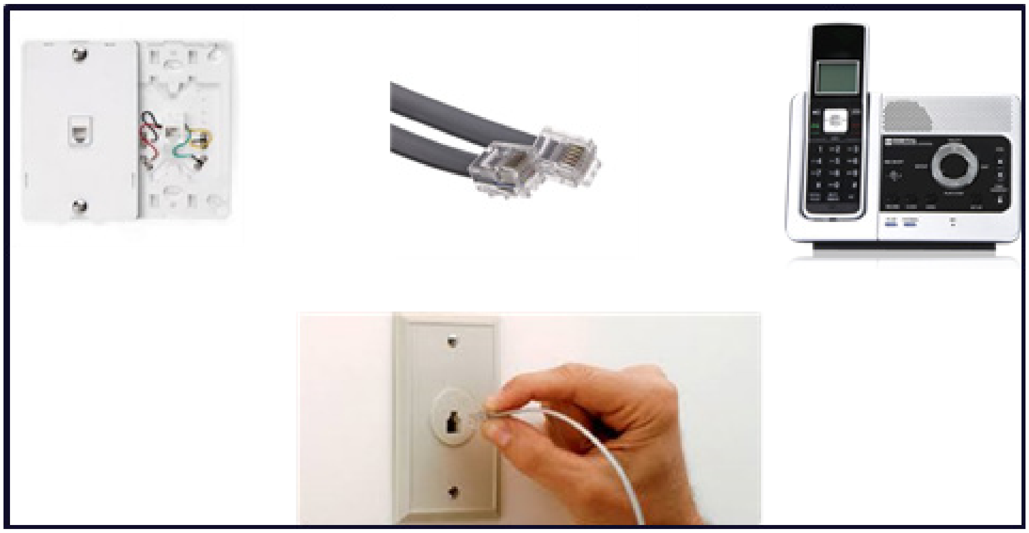


Form, Fit, and Function (FFF) Data

The DFARS defines FFF data as technical data that describes the required overall physical, functional and performance characteristics (along with the qualification requirements, if applicable) of an item, component, or process to the extent necessary to permit identification of physically and functionally interchangeable items.

An example of an everyday system that uses open standards for interfaces to allow maximum use of a commercial system (your home phone) is shown in Figure 6. The phone is wired into a wall plate via a phone connector (RJ-11) and wire. Since all the interfaces that connect the phone to the wall plate are designed to comply with commercial standards, numerous manufactures can supply a phone that a customer can buy and plug into the wall plate and voila it works! Customers do not need to worry about whether their phone will be compatible with the wall plate because the interfaces are standard. This allows consumers to buy any number of phones produced by different manufacturers at various costs and with various functions to meet their specific needs. The open standards allow manufacturers to compete for customers for their phones, leading to decreased prices and/or improved designs and upgrades.

Figure 6. Phone Interface



Pursuant to DFARS clauses current as of the publication of this Guide, FFF data is delivered to the government with UR regardless of the funding source for development of the data. (Note: This automatic grant of rights applies only to data, not computer software.) Since all interface technical data fall within the definition of FFF data, the Air Force receives UR in all delivered interface data. Examples of such interface data include interface control documents, interface requirement specifications, and control drawings (as defined in the American Society of Mechanical Engineers (ASME) Standard Y14.24-2012, *Types and Applications of Engineering Drawings*).

The Strategy

The contractor's design approach should result in modules with minimal dependencies on other modules (loose coupling), as evidenced by simple, well defined interfaces. This approach should ensure that changes to one module will not necessitate extensive changes to other modules, facilitating module replacement and system enhancement. The program should require delivery of documentation describing the approach used to determine the level of coupling and the design trade-off approach:

Step 1: Require delivery of all interface technical data.

Step 2: Review deliverables to ensure that no noncommercial interface technical data is delivered with restrictive markings (it should not contain any restrictive data rights markings as it is FFF data subject to UR).

Step 3: Evaluate interface design and management during a source selection. For example, include an evaluation factor requiring the offeror to describe how it will clearly define component and system interfaces, and, at a minimum, requiring the offeror to address the following:

- Describe how it will define and document all subsystem and configuration item-level interfaces to provide fully functional, physical, and electrical 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, vendor unique standards, as well as the impact of those standards on the proposed modularity and logistics approach.
- Describe interfaces including, but not limited to, mechanical and electrical (power and signal wiring).
- Address the interface and data exchange standards between the component, module or system, and the interconnecting or underlying information exchange medium.

1.2. Identifying Intellectual Property Requirements

To say identifying IP requirements is a challenge would be an understatement. If ever there was a Goldilocks exercise in defense acquisition, identifying IP requirements is it. The DFARS disallows requiring “all the data.” But experience shows that while having too many requirements may be costly and useless, having insufficient data negatively impacts life-cycle support. The goal is to establish requirements that are not too much, not too little, but just right.

For these reasons, data acquisition planning is critically important. Not only does this process involve a range of people representing different functional disciplines, but it also requires answering such questions as: What does the program need to accomplish for life-cycle support? Who should be involved when making these determinations? In view of these needs, what technical data and computer software should be acquired to meet them? How is this best done? Once these requirements are specified, how will the Government measure and assure contractor performance? Beyond that, how will these materials be used, updated, and maintained throughout the life cycle?

None of these questions are easily answered, especially in the pre-acquisition phase. The questions that follow should provide a useful start to PMOs as they begin their acquisition planning, which is only really a start. Just as planning never ends in the acquisition life cycle, so will needs for technical data and computer software change over time. Plans should be updated accordingly.

1.2.1. How do I assess my program’s short- and long-term IP requirements? Is there a best practice for ensuring that the necessary and proper data and software for life-cycle support are identified and received?

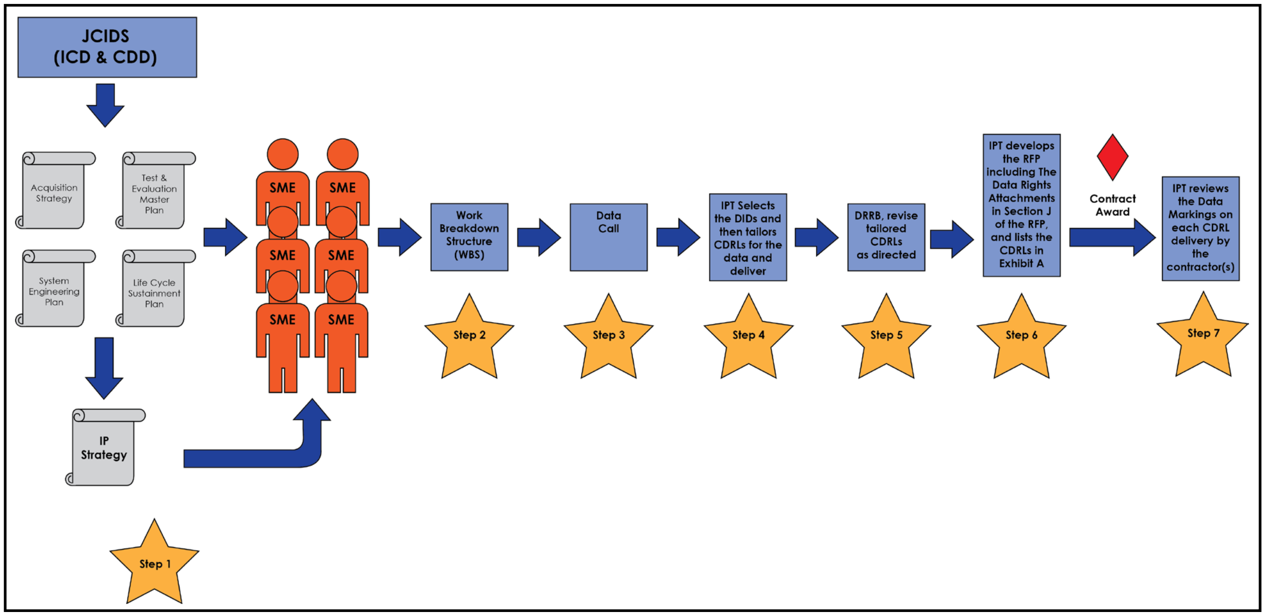
Response

Establishing and conducting a Data Call (see DoD 5010.12-M, Chapter 2) is a best practice for ensuring that necessary and proper data and software are obtained. The results from the Data Call will determine the data needs and requirements for the design, testing, production, operations, maintenance, and logistics support over the life cycle. The results of the Data Call will also enable the PMO to prepare CDRLs with the appropriate Data Item Descriptions (DIDs) for inclusion in the RFP and resulting contract.

The Strategy

Step 1: Develop a Standard Operating Procedure (SOP) within the PMO to describe the process to conduct a formal Data Call. Figure 7 provides a graphical representation of a high-level data process that includes a Data Call.

Figure 7. High-Level Data Process


JCIDS (ICD & CDD)
Acquisition Strategy
Test & Evaluation Master Plan
System Engineering Plan
Life Cycle Sustainment Plan
IP Strategy
Step 1
SME
SME
SME
SME
SME
SME
Work Breakdown Structure (WBS)
Step 2
Data Call
Step 3
IPT Selects the DIDs and then tailors CDRLs for the data and deliver
Step 4
DRRB, revise tailored CDRLs as directed
Step 5
IPT develops the RFP including The Data Rights Attachments in Section J of the RFP, and lists the CDRLs in Exhibit A
Step 6
Contract Award
IPT reviews the Data Markings on each CDRL delivery by the contractor(s)
Step 7

Step 2: Involve all SMEs from all functional areas that support the weapon system. A partial list of SMEs includes logistics, systems engineering, software engineering, test and evaluation, and management.

Step 3: Ensure the SMEs are thoroughly trained in the procedures for conducting a Data Call.

Step 4: Select a data manager to facilitate the identification of technical and computer software to order and to lead all efforts during the Data Call, with specific points of contact for each functional area. For example,

- Depot/item managers for a given part, system, or subsystem
- The Product Support Manager for all logistics data required
- A Lead System Engineer for all technical and computer software data requirements.
- If the PMO does not know what to order and a depot has not yet been tasked with pre-depot planning support, identify SMEs who have experise in determining delivery and rights in technical and computer software needed for sustainment and to enable a follow-on competitive procurement.

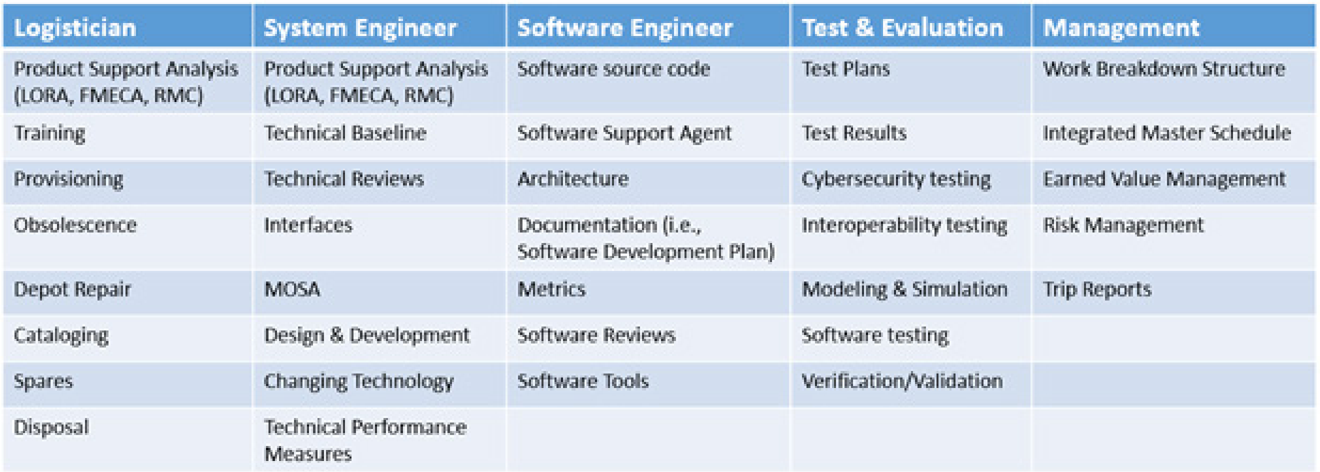
Step 5: SMEs should review the following primary documents for the inputs on the Data Call: Acquisition Strategy, Life Cycle Sustainment Plan, Systems Engineering Plan, Test Evaluation and Master Plan and the IP Strategy.

Step 6: Each SME should identify and justify specific, minimum essential technical data and computer software delivery and rights requirements based on the intended use of each deliverable for each future task.

Step 7: The Data Manager will use the responses to the Data Call to establish technical data and computer software deliverables and rights that must be implemented as contractual requirements. Look at the current contract developmental and production tasks and see whether future task data needs overlap with current task data outputs. For software-intensive programs, the IEEE STD12207 is an excellent reference that lists all developmental tasks and outputs of such tasks. Consolidated requirements are reviewed at several management levels, any one of which may challenge the need for technical data or computer software or question their absence.

Step 8: Request anyone challenging the technical data or computer software deliverables or rights to do so in writing to the Data Manager. Table 1 shows a notional "functional swim-lane" for each SME to analyze to determine what data is necessary and proper for design, testing, production, operations, maintenance and logistics support.

Table 1. SME Notional "Swim-Lane" Data Analyses
(not all SMEs are listed nor are all data analyses shown)



Logistician	System Engineer	Software Engineer	Test & Evaluation	Management
Product Support Analysis (LORA, FMECA, RMC)	Product Support Analysis (LORA, FMECA, RMC)	Software source code	Test Plans	Work Breakdown Structure
Training	Technical Baseline	Software Support Agent	Test Results	Integrated Master Schedule
Provisioning	Technical Reviews	Architecture	Cybersecurity testing	Earned Value Management
Obsolescence	Interfaces	Documentation (i.e., Software Development Plan)	Interoperability testing	Risk Management
Depot Repair	MOSA	Metrics	Modeling & Simulation	Trip Reports
Cataloging	Design & Development	Software Reviews	Software testing	
Spares	Changing Technology	Software Tools	Verification/Validation	
Disposal	Technical Performance Measures			

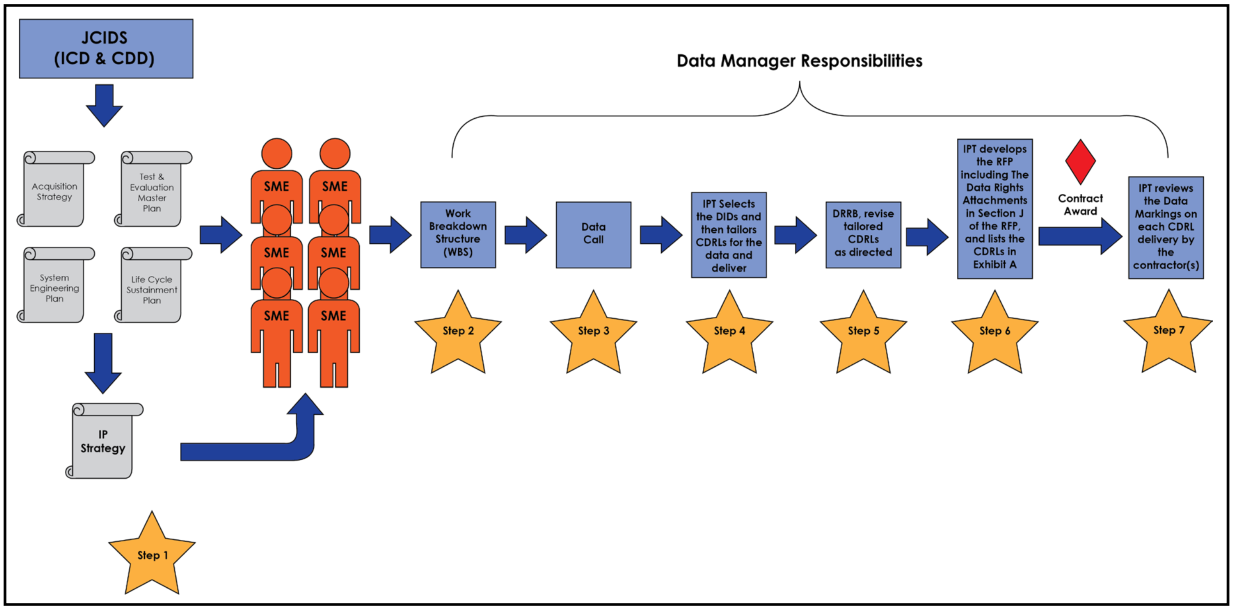
Step 9: Develop the proper and necessary CDRLs based on the data needs and requirements for sustainment as derived from the Data Call. Note, many DIDs are out-of-date, so tailor existing DIDs or create new DIDs as required.

1.2.2. What is the role of a Data Manager within the PMO, and how does the Data Manager support technical data and computer software acquisition?

Response

A Data Manager is trained and designated as the principal focal point within a program and is responsible for ensuring compliance with the policies and procedures outlined in DoD and Air Force policy and guidance. Figure 8 identifies the responsibilities of a Data Manager to ensure that the proper and necessary data is acceptable, acquired, and stored.

Figure 8. Data Manager Responsibilities

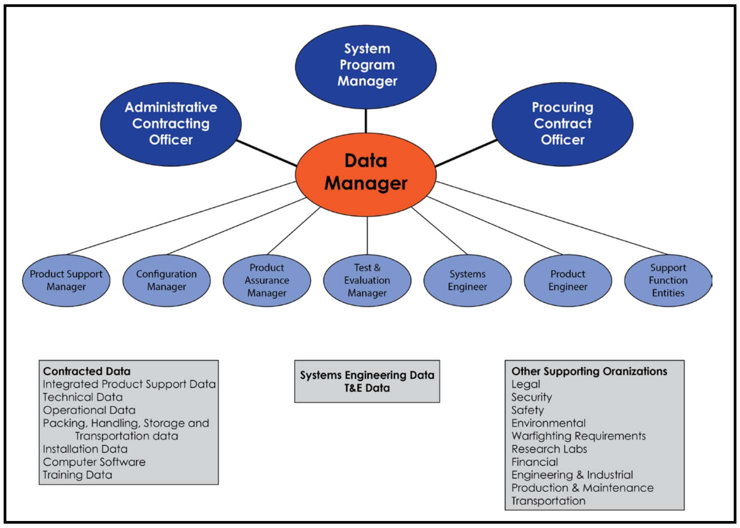

JCIDS
(ICD & CDD)
Acquisition Strategy
Test & Evaluation Master Plan
System Engineering Plan
Life Cycle Sustainment Plan
IP Strategy
Step 1
SME
SME
SME
SME
SME
SME
Data Manager Responsibilities
Work Breakdown Structure (WBS)
Step 2
Data Call
Step 3
IPT Selects the DIDs and then tailors CDRLs for the data and deliver
Step 4
DRRB, revise tailored CDRLs as directed
Step 5
IPT develops the RFP including The Data Rights Attachments in Section J of the RFP, and lists the CDRLs in Exhibit A
Step 6
Contract Award
IPT reviews the Data Markings on each CDRL delivery by the contractor(s)
Step 7

In general, the Data Manager should be the PMO's lead for all data tasks. If a Data Manager is not available, the PMO should reach out to the Program Executive Officer to request a Data Manager be "matrixed-in" to support the program. The Data Manager should reach out to all functional areas regarding technical data and computer software requirements, and provide or obtain necessary training for team members. Team members should know, for example, how to complete the DD Form 1423 to specify a pre-formatted contract data requirement. A Data Manager should lead the cross-functional teams for Steps 1 through 7 as shown in Figure 9. The Data Manager must be involved in developing the IP Strategy, Acquisition Strategy, and the LCSP. The Data Manager should work with the Product Support Manager to conduct the necessary Product Support Analysis, the results of which will support the data requirements for the PMO.

The Data Manager has the following specific responsibilities:

- Facilitates the timely and economical acquisition and availability of technical data and computer software, including delivery and rights.
- Ensures that only essential requirements for supporting the program are included on the contract.
- Ensures that technical data and computer software delivered conforms to the contract's requirements.
- Identifies and catalogs all valid requirements for technical data and computer software and associated rights for inclusion in the contract.
- Identifies and provides a repository for all contractor-delivered technical data and computer software.

Figure 9. Data Manager Interaction within the PMO



1.2.3. Is there any current process that the Air Force PMO can perform to assist in receiving the necessary technical data and computer software with the required level of rights?

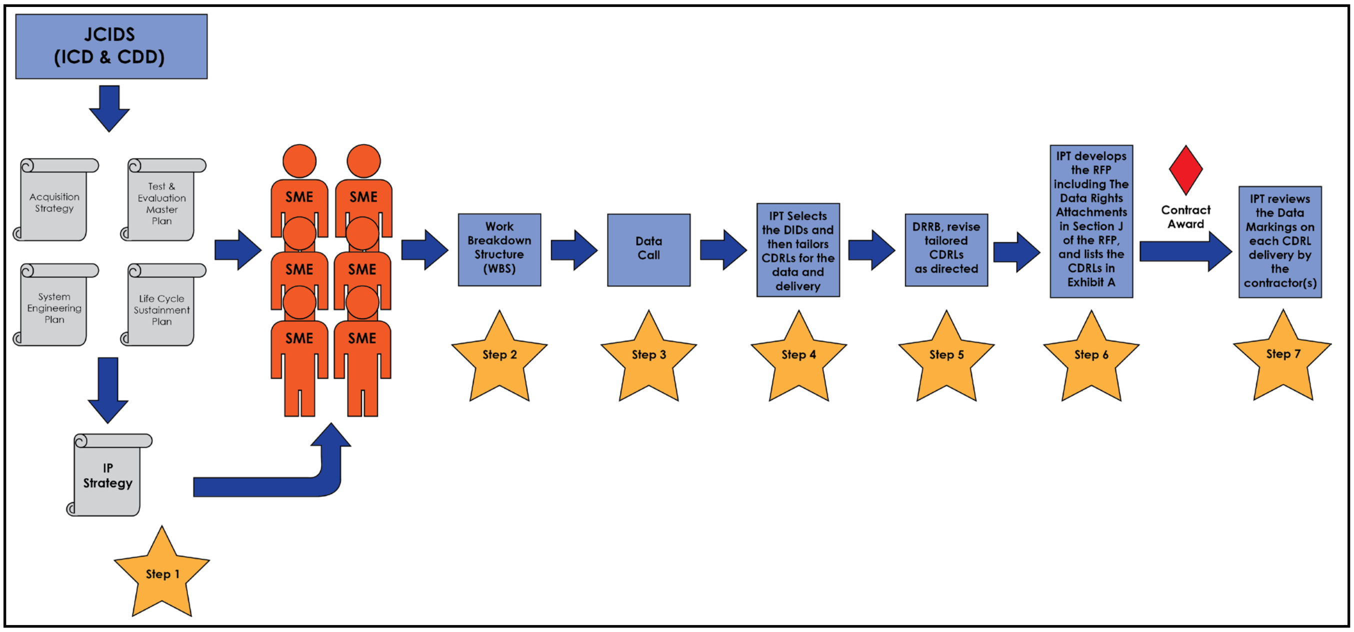
Response

One way to meet this requirement is to mandate that the contractor deliver technical data or computer software by inclusion of a CDRL in the contract. The CDRL provides a contractual method to require the contractor to prepare and/or deliver technical data or computer software that meets specific approval and acceptance criteria. The Data Requirements Review Board (DRRB) reviews the acquisition to ensure all requirements for technical data and computer software are properly captured and documented in appropriate DIDs in a CDRL attached to the contract.

The Strategy

Step 1: The PMO should develop an SOP describing the required CDRLs and the process to determine technical data and computer software and associated rights requirements for the acquisition, as well as establishing a DRRB. Refer to Figure 10, a high-level process for the acquisition and review of technical data and computer software. (This Issue Paper addresses Steps 4 and 5.)

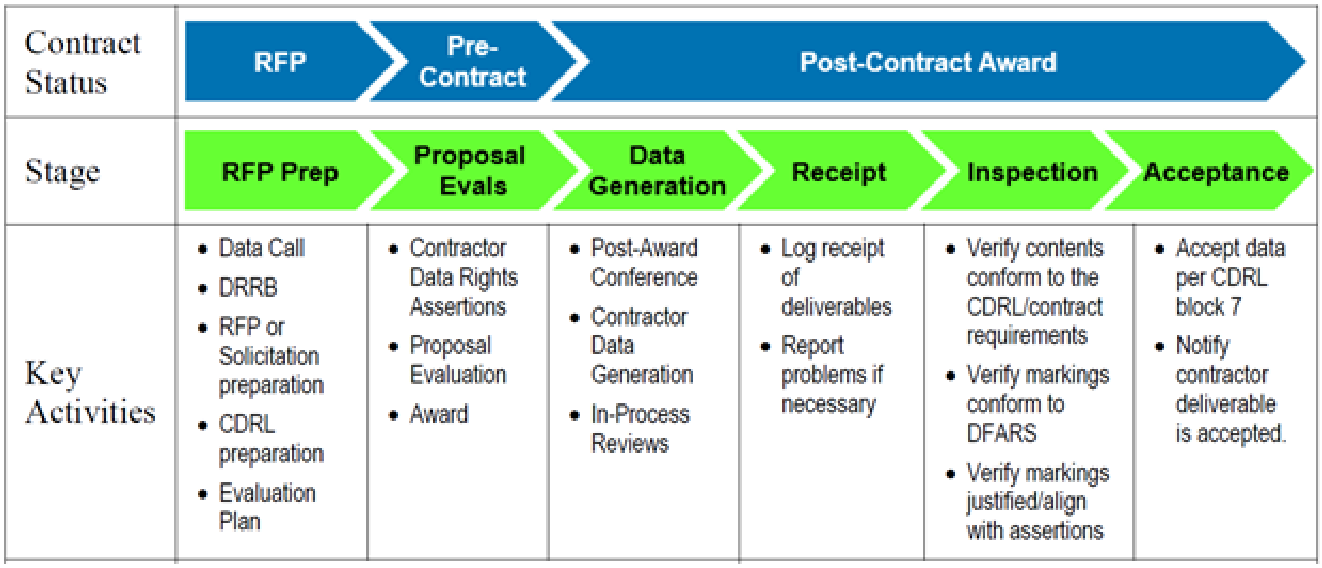
Figure 10. High-Level Data Process


JCIDS
(ICD & CDD)
Acquisition Strategy
Test & Evaluation Master Plan
System Engineering Plan
Life Cycle Sustainment Plan
IP Strategy
Step 1
SME
SME
SME
SME
SME
SME
Work Breakdown Structure (WBS)
Step 2
Data Call
Step 3
IPT Selects the DIDs and then tailors CDRLs for the data and delivery
Step 4
DRRB, revise tailored CDRLs as directed
Step 5
IPT develops the RFP including The Data Rights Attachments in Section J of the RFP, and lists the CDRLs in Exhibit A
Step 6
Contract Award
IPT reviews the Data Markings on each CDRL delivery by the contractor(s)
Step 7

Step 2: The SOP should include procedures to ensure all SMEs are trained in preparing tailored CDRLs. This training should be accomplished before development of CDRLs and should include training in determining technical data and computer software deliverables and rights requirements (Step 4 in Figure 10).

Step 3: The results from the Data Call (Step 3 in Figure 10) will determine the technical data and computer software needs and requirements for the sustainment of the weapon system. These results guide development of the CDRLs. Figure 11 (sourced from DoD 5010.12-M) identifies the timing of CDRL preparation within the acquisition process.

Figure 11. Data Acquisition Process



Contract Status	RFP	Pre-Contract	Post-Contract Award			
Stage	RFP Prep	Proposal Evals	Data Generation	Receipt	Inspection	Acceptance
Key Activities	• Data Call • DRRB • RFP or Solicitation preparation • CDRL preparation • Evaluation Plan	• Contractor Data Rights Assertions • Proposal Evaluation • Award	• Post-Award Conference • Contractor Data Generation • In-Process Reviews	• Log receipt of deliverables • Report problems if necessary	• Verify contents conform to the CDRL/contract requirements • Verify markings conform to DFARS • Verify markings justified/align with assertions	• Accept data per CDRL block 7 • Notify contractor deliverable is accepted.

Step 4: After all CDRLs are drafted, the DRRB should meet to review CDRLs and the SOW/Performance Work Statement (PWS) (Step 5 in Figure 10). The DRRB reviews all data and functional requirements to ensure that requirements are appropriate to the contract's objectives, and in accordance with the life-cycle needs established by the Acquisition Strategy, LCSP, and the IP Strategy. The DRRB verifies the following:

- The CDRL is required for acquisition and sustainment of the weapon system so that only the necessary and proper technical data and computer software is being procured.
- The CDRL (DD Form 1423, Contract Reference – block 5) aligns to the applicable SOW/PWS paragraphs so that all technical data and computer software requirements are traceable to the contract.
- The CDRL is properly completed per DoD 5010.12-M.
- The DID been tailored in block 16 of the CDRL or a one-time DID has been prepared and approved in accordance with MIL-STD 963C and DoD Manual 4120.4 if necessary.
- The approval requirements, delivery dates, and deferred ordering or delivery of technical data and computer software are reasonable, consistent with program schedule, and have been properly specified on the CDRL.
- CDRL authors make all the necessary corrections and updates directed by the DRRB.

Step 5: Draft minutes for each DRRB meeting, document the approval or reasons for disapproval of all CDRLs submitted for review, and list all action items assigned at the meetings.

1.3. Other Data Acquisition Topics

1.3.1. What is the Data Accession List (DAL) and how should I use it? How does the PMO know which technical data and computer software items to order after initial contract award, and how is this done?

Response
The DAL refers to a CDRL deliverable in which a contractor is required to identify all technical data and computer software a contractor or subcontractor has generated in performance of the contract. With this information, the PMO can identify technical data and computer software items for future ordering, such as via the Deferred Ordering Clause at DFARS 252.227-7027 or under existing terms in the contract or an appropriate contract modification.

Whereas CDRLs generally identify the technical data and computer software deliverables the contractor must provide to the Government, the DAL identifies internal contractor data generated over the course of contract performance that the Government may request the contractor to make available, may have delivered pursuant to a term of the contract, or may require as a deliverable by negotiating an appropriate contract modification.

Another way to gain insight is to use contract performance data such as the Integrated Master Schedule and Contract Work Breakdown Structure to link the SOW to hardware and software items being developed on the contract. When government funding can be associated with the development of these items, then ordering the technical data and computer software pertaining to them that has been generated during performance of the contract can be helpful for life-cycle management.

Also, the details found in contract performance information and the DAL can be used to develop a compelling narrative about Government funding for development of the ultimate end item. This can be particularly helpful in providing the Government's rights in technical data or computer software in future negotiations or disputes.

The Strategy

Step 1: Include the DAL (DI-MGMT-81453B) as a CDRL on the contract and as a requirement in the SOW. Include this CDRL among the other requirements for contract performance information (such as the IMS or WBS).

Step 2: When including the DAL in the SOW, include language requiring that preliminary data, work-in-progress information products, and final information products be identified on the DAL when generated. This requirement should be specified in Blocks 10-13 of the CDRL Form 1423.

Step 3: Consider including language in the SOW requiring the contractor to deliver data or computer software included on the DAL within a reasonable time after receiving a written request from the Government identifying the items to be delivered. Include language limiting compensation for delivery to the cost of converting the data or computer software into the prescribed form, for reproduction and delivery.

Step 4: Review the DAL when it is delivered to identify technical data, computer software, and other information being generated as part of the contract in view of your life-cycle objectives. Verify that the DAL includes the required identification of Government rights for each item included.

Step 5: Use the information gained in Steps 1 and 2 to evaluate the contractor's original assertions and initiate a challenge through the Contracting Officer if the reported information indicates that the asserted restriction may not be justified.

Step 6: When the PMO has a requirement for any technical data or computer software being generated under the contract or otherwise being reported as created with government funds, initiate an appropriate contract action or contract change through the Contracting Officer to have those items delivered.

1.3.2. How can the PMO use other contract deliverables, such as the Work Breakdown Structure (WBS), to obtain technical data and computer software needed for life-cycle support?

Response

The WBS (see MIL-STD-881D) is a tool that displays and defines the product, or products, to be developed or produced under a contract and relates the elements of work to be accomplished to one another and to the end product. In other words, the WBS is a product-oriented representation of the contract. When a combination of hardware and software items are being assembled and delivered as an end item, the WBS will display that information in a hierarchical manner. As shown in Figures 12 and 13, the WBS focuses on system components and their configuration, and may include subsystems, items or modules, components, configuration items, and computer software configuration items and the interfaces between them.

Figure 12. WBS Graphical Representation

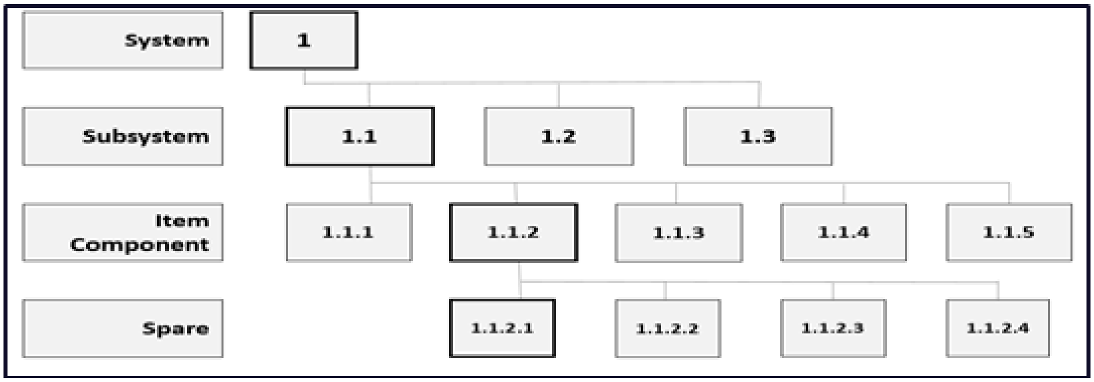
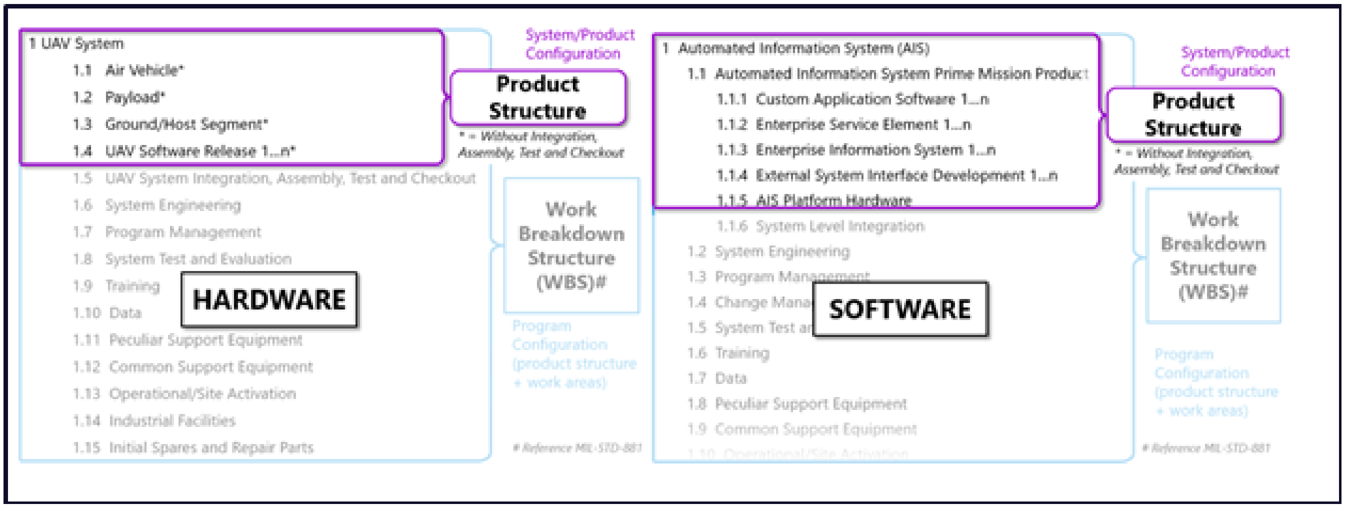


Figure 13. Unmanned Aerial Vehicle Work Breakdown Structures


1 UAV System
1.1 Air Vehicle*
1.2 Payload*
1.3 Ground/Host Segment*
1.4 UAV Software Release 1...n*
1.5 UAV System Integration, Assembly, Test and Checkout
1.6 System Engineering
1.7 Program Management
1.8 System Test and Evaluation
1.9 Training
1.10 Data
1.11 Peculiar Support Equipment
1.12 Common Support Equipment
1.13 Operational/Site Activation
1.14 Industrial Facilities
1.15 Initial Spares and Repair Parts
HARDWARE
System/Product Configuration
Product Structure
* = Without Integration, Assembly, Test and Checkout
Work Breakdown Structure (WBS)#
Program Configuration (product structure + work areas)
# Reference MIL-STD-881
1 Automated Information System (AIS)
1.1 Automated Information System Prime Mission Product
1.1.1 Custom Application Software 1...n
1.1.2 Enterprise Service Element 1...n
1.1.3 Enterprise Information System 1...n
1.1.4 External System Interface Development 1...n
1.1.5 AIS Platform Hardware
1.1.6 System Level Integration
1.2 System Engineering
1.3 Program Management
1.4 Change Mana
1.5 System Test ar
1.6 Training
1.7 Data
1.8 Peculiar Support Equipment
1.9 Common Support Equipment
1.10 Operational/Site Activation
SOFTWARE
System/Product Configuration
Product Structure
* = Without Integration, Assembly, Test and Checkout
Work Breakdown Structure (WBS)#
Program Configuration (product structure + work areas)
# Reference MIL-STD-881

By adding levels of indenture to the end product as represented in the WBS, one can perform a more detailed assessment of how the end item, its subsystems and components, and interfaces were developed. In this way, components and interfaces an offeror asserts were developed exclusively at private expense can be isolated from components and interfaces that were not developed exclusively at private expense. This will make it easier for the Government to determine what rights it should receive to the technical data and computer software associated with the end item.

The WBS is a powerful tool for visualizing the end item to be developed and its subsystems, components, and interfaces, in order to provide more information when acquiring technical data and computer software acquisition. What follows is one way a PMO can use the WBS to shape the portions of an RFP related to data and software, and to identify the level of rights the Government is entitled to receive. By beginning with the WBS, the PMO can construct a table for managing data rights assertions and for pricing. Similar tables can be created for production (spares) and product support (maintenance).

Table 2. Notional Table of Noncommercial Technical Data for System-Only IP Rights

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9
CDRL Number	Data Item Description	CDRL Title	CDRL Subtitle	SOW Reference	CLIN	WBS Element	Govern-ment Needed Rights	Offeror Assterted Rights

The Strategy
Step 1: The PMO creates the end item's WBS using MIL-STD-881D.

Step 2: The PMO issues a Data Call and completes a DRRB in order to finalize CDRL content. The PMO then populates Columns 1-7 of Table 2.

Step 3: The PMO develops the product support strategy for each component (e.g., competition, sole-source) identified in the WBS and includes that information in the Acquisition Strategy and LCSP.

Step 4: The PMO populates Column 8 of Table 2 based on the results of the DRRB and Acquisition Strategy, identifying the CDRLs to be included in the contract and what IP rights must be obtained in those CDRLs. With respect to those components for which the PMO intends to compete maintenance/sustainment, the PMO performs market research to determine whether that item was developed exclusively at private expense, documents the results of that analysis and market research in the Acquisition Strategy, and then compares the results of that analysis to the information contained in Column 8 of Table 2 to determine the probability that the PMO will be able to compete maintenance/sustainment of that component identified within the WBS.

Step 5: The Contracting Officer includes the following information in the RFP:

- CDRLs validated during the DRRB.
- IP Rights Section J attachment that identifies the particular level of rights the Government requires to specific content to be delivered in each CDRL.
- Section L instructions stating that, if an offeror intends to assert any restrictions on the DoD's ability to use, release, or disclose a CDRL to non-Government employees, that offeror must (1) identify the lowest level of indenture in its proposed Contractor WBS wherein that item will reside; (2) identify what text in that CDRL requires delivery of the item of technical data or computer software that describes its technical baseline to which the asserted restriction pertains; and (3) for technical data, explain why that item does not fit within any of the statutory or regulatory provisions that entitle the DoD to acquire unlimited/unrestricted rights in that technical data irrespective of whether that technical data was developed exclusively at private expense.
- Section M evaluation criteria stating that the Government will evaluate the extent to which (1) the information provided by the offeror supports its position and (2) the offeror's proposed IP licenses will satisfy the Government's minimum needs.

Step 6: The PMO evaluates the information provided by the offeror in response to the Section L instructions in accordance with Section M. Specifically, the PMO should populate Column 9 of Table 2 and compare those results to the information contained in Column 8 of Table 2. If essential for the successful completion of the procurement, the Contracting Officer can request during discussions that records be provided substantiating that the item, component, or process was developed exclusively at private expense. Upon receipt of those substantiating records, the PMO determines the validity of that asserted restriction.

Chapter 2 – Intellectual Property in Source Selection

In a source selection, offerors are required to include an attachment to their offers that identifies noncommercial technical data or computer software that will be furnished to the Government with restrictions on use, release, or disclosure. It is critical, prior to issuing the solicitation, that the PMO identify all data and software deliverables that may be required to execute the program, including meeting future life-cycle needs, to put offerors on notice to make these assertions. When the PMO does these things, the program's technical data and computer software requirements will be evident in the source selection documentation.

A program's source selection documents should reflect the PMO's analysis of the program's plans for maintenance and sustainment of the systems, subsystems, and components making up the product baseline. Ultimately, these plans will be translated into contract requirements that include CDRLs for delivering specific data and software items and making other items available for life-cycle support. Unless the PMO has fully analyzed its life-cycle needs, communicated those needs in the solicitation, and translated them into contract requirements, the program is at high risk of being subject to "vendor lock" for the life cycle. And, as experience has taught, vendor lock makes it more likely the Air Force will be unable to operate, maintain, and sustain the system in a cost effective manner, to meet the statutory and regulatory requirements associated with depot maintenance (e.g., competition, Core depot maintenance, 50/50), and to satisfy the warfighter's readiness requirements. This chapter aims to help PMOs pull their varied efforts together into a successful Acquisition Strategy and source selection, which begins by deciding how IP will fit into the effort.

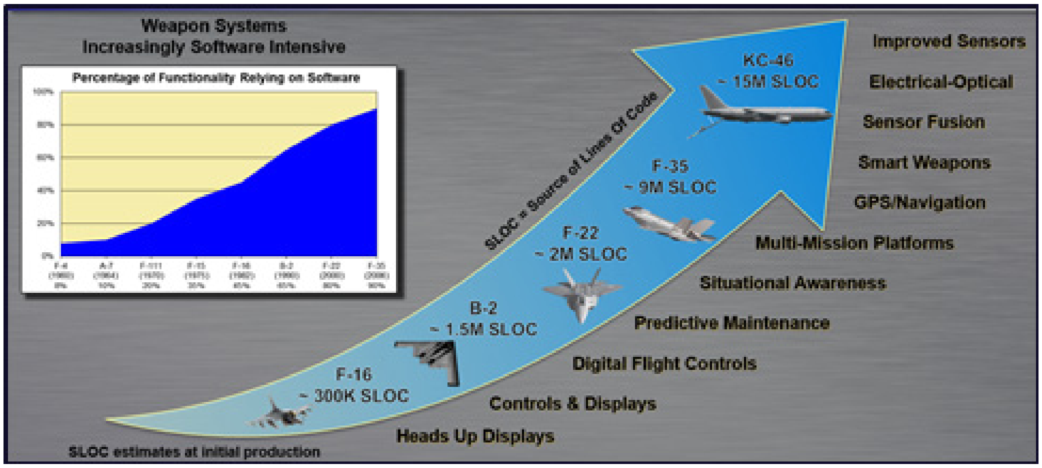
2.1. Why should a PMO evaluate the IP rights an offeror proposes or otherwise asserts as part of a source selection?

Response

Evaluating the IP rights an offeror proposes, either in the form of a license or on the basis of restrictive assertions, will enable the PMO to make informed decisions about how the substance of the proposal is likely to impact the life cycle. This includes assessing the likelihood of "vendor lock" for its duration.

A case in point can be made with software. Air Force weapon systems are increasingly software intensive. As shown on Figure 14, the F-35 aircraft has about 9 million software source lines of code and nearly 90% of its functionality relies on computer software. Likewise, the KC-46 aircraft has even more software—approximately 15 million software source lines of code. Yet, the value in computer software is not only in its functionality, but in the ability to adapt it readily in response to future needs. The license rights available in the software will determine whether making these changes can be done only by the original source, by an organic software team, by a third party, of even via DevOps methodology, where the coding team is a blend of contract and government talent.

Figure 14. Flight Software Growth



As data and software increase in importance, it is becoming critical to obtain appropriate rights in IP to ensure life-cycle objectives remain viable. Evaluating this part of a proposal is an enabler to this end.

2.2. What benefits can the PMO expect by evaluating IP rights in source selection, and how is that best done?

Response
Some benefits of evaluating IP rights during source selection include:

1. Leveraging competition between offerors so the PMO can obtain the optimal solution for IP rights necessary to meet life-cycle objectives, at a fair and reasonable price, and in a way that promotes determinations of best value. Notwithstanding industry arguments that evaluating offerors' IP rights in their proposals is a violation of the 10 U.S.C. 2320(a)(2)(H) prohibition on requiring a contractor to relinquish rights in or refrain from offering technical data in which the Government's rights are restricted because an item was exclusively developed at private expense, the Government is entitled to evaluate proposed solutions and select the one that best meets its requirements. Further, not doing such an evaluation risks entering into a contract that does not fulfill the agency's requirements and ultimately failing to meet the mission.

2. Effectively communicating the need for technical data and computer software deliverables and the required rights and the Air Force's intention to pay for them. It also allows offerors to determine what they consider to be a fair price for the Air Force to acquire those IP rights, but communicates that a price that is too great might make the offeror's total evaluated price too high to win the contract. This approach fosters competition during all phases of the life cycle of the weapon system.

3. Easing the administrative burden of managing assertions, especially after contract award. While contractors are allowed to change their assertions under limited circumstances after contract award, when the PMO evaluates the assertions during the source selection, it is better positioned to limit changes to those assertions that would have impacted the source selection decision. This can be extremely helpful for ensuring the "deal" does not change after contract award based on new terms.

Consider this example of how using IP rights as an evaluation factor can preserve the PMO's bargain during program execution: as part of the proposal, Offeror A proposed to exceed the program's minimum needs for IP rights to a greater extent than did Offeror B, with both receiving an Outstanding Technical Rating as a result. Offeror C proposed the bare minimum for IP rights for the proposal to be acceptable and responsive and received an Acceptable Technical Rating. Offeror A's total evaluated price was slightly higher than Offeror B's total evaluated price, and Offeror C's total evaluated price was significantly lower than both. After performing a tradeoff analysis, the Source Selection Authority selected Offeror A's proposal for award, as its technical superiority was worth the price premium. The Source Selection Authority documented that Offeror A's superior IP rights offer was the most significant factor in the results of the tradeoff analysis. Two years later, the awardee (Offeror A) attempted to update its assertions based on inadvertent omissions, but in so doing, proposed to deliver critical technical data deliverables subject to a lower level of rights than previously proposed in response to the RFP. Given the evaluation criteria in the RFP, if the awardee had made those additional assertions in its proposal, its Technical Rating would have been Acceptable (at best), and therefore the tradeoff analysis would have resulted in its technical solution not being worth the price premium. Since the source selection record indicated that the most significant factor in the awardee winning the contract was its proposal for IP, the Contracting Officer can reject the new assertions as the Government can use the record to show that the inadvertent omissions would have materially affected the source selection decision.

2.3. Are there basic steps a PMO can take to implement IP considerations in a source selection?

The Strategy
Here is a simple two-step process for implementing IP considerations in a source selection:

Step 1: Review the program's Acquisition Strategy, LCSP, System Engineering Plan, IP Strategy, and any additional useful documentation to identify with particularity the PMO's minimum needs for IP and the source of those needs (e.g., competition for the maintenance or sustainment of the weapon system, subsystem, and components).

Step 2: Include the following factors in the evaluation criteria in Section M of the RFP: (a) a Technical Factor evaluating the extent to which the offeror proposes to provide IP rights in deliverables necessary to meet the Government's requirements; and (b) a description of how the offeror's proposed prices for IP rights will become a part of the offeror's total evaluated cost/price in the Cost/Price Factor.

2.4. How should an RFP be structured in order to acquire the necessary deliverables and associated IP rights to develop, produce, maintain, sustain, and dispose of the weapon system in an enforceable contract?

Response
Once life-cycle objectives are known, requirements are identified, and the SOW/PWS properly scoped, the PMO should begin specifying the CDRLs via DD Form 1423. Each CDRL will reference a DID specifying content and format for the deliverable while also cross-referencing the tasking statements in the SOW/PWS. A contractor's assertions should be based on these deliverables.

One of the keys to managing these assertions successfully, in addition to evaluating their life-cycle impacts, is to ensure that assertions map only to the CDRLs that are required. Each assertion should map to a CDRL and not be "parentless" in this regard. Also, to be better informed about the potential life-cycle impacts of these assertions, the PMO can use the WBS methodology described in Chapter 1 to further map the assertions to individual elements of the product baseline. By doing these things, the PMO will be better positioned to reduce unnecessary assertions, will ensure rights in individual CDRLs are clearly delineated, and will be prepared to evaluate how those assertions could affect life-cycle objectives based on where they correspond to the product baseline.

The Strategy

Step 1: Identify deliverable content via DD Form 1423s and relate them to tasking statements in the SOW/PWS.

Step 2: Include assertions requirements in Section L of the solicitation by referencing DFARS 252.227-7017. Also reference DFARS 252.227-7028 to ensure technical data or computer software previously delivered to the Government can be clearly identified.

Step 3: Require the offeror to map any assertions to specific deliverables (refer to Section 5.1.4.). This will reduce the effort necessary after award to determine what license rights the Government acquired to a specific deliverable, and it will make it easier to challenge markings that do not comply with DFARS requirements

Step 4: Require the offeror to map assertions associated with technical data or computer software to the WBS element for the component described by that product baseline.

Step 5: Baseline the contents of a specific CDRL to a single level of license rights and specify them in Section J. This will make it easier to determine what rights were acquired for specific deliverables.

Step 6: Assertions should be clear, definite, and associated with private development. If not all of these things are present, use appropriate evaluation notices to ensure assertions are properly understood.

Step 7: If assertions are to be evaluated, include evaluation criteria in Section M. Include evaluation criteria in the RFP that allow the Government to evaluate the extent to which technical data and computer software subject to restrictions will satisfy the minimum needs of the program.

2.5. When should a PMO consider obtaining a specially negotiated license?

Response

There are numerous circumstances under which a PMO should consider obtaining a specially negotiated license. These include where the standard license for technical data for a commercial item does not meet the program's needs, when an offeror's assertions of private expense development will not allow the program to meet life-cycle objectives, when the program believes it can trade rights for some items that may be unnecessary to meet life-cycle needs to get greater rights in other items that may be needed, or where the program believes that the potential contractor(s) will not agree to deliver technical data or computer software to the Government with the standard rights granted by the DFARS but may be willing to deliver technical data or computer software subject to a lesser level of rights that will still meet the Government's requirements. The Air Force has a great deal of flexibility in negotiating IP rights in deliverables, but the DFARS does not allow the Government to accept less than limited rights (LR) in technical data or restricted rights in commercial software. The Government should also not agree to a position that unduly restricts competition.

2.6. What should the PMO consider when deciding whether to evaluate IP as part of a source selection? How can the PMO evaluate IP if it decides that is appropriate?

Response

One factor contributing to the Air Force's difficulty in acquiring adequate technical data rights is the lack of emphasis on evaluating technical data rights during source selection. AFI 63-101/20-101 requires source selection to consider Government rights in data. The Government evaluates IP rights and other IP considerations as part of the source selection by ensuring the RFP contains evaluation criteria that make it clear that IP rights are a material requirement of the solicitation. The following questions and best practices are provided to assist future source selection teams in procurement of appropriate technical data rights for the AF.

The Strategy

Step 1: In determining whether to include IP rights as an evaluation factor, the PMO should consider the nature of the contract, including:

- Does the contract involve development of a new system?
- Does the contract involve modifications to an existing system or major components/subcomponents? If so, are they minor modifications?
- Do we plan to compete follow-on work, sustainment, or upgrades for the system, components, or subcomponents?
- Was the development of an existing system, components, or subcomponents funded by the Government, a contractor, or both?
- Is the system a commercial item?
- How would IP rights be evaluated?
- Does evaluating IP rights give one competitor an advantage or unduly restrict competition?
- If separately evaluating IP rights is not appropriate or practical, can IP rights be considered as part of another factor?

Step 2: Some questions to ask to determine whether Data Rights is a discriminator:

- How would you evaluate?
- Would there be a clear winner (i.e., does someone have an advantage going into the process)?

Step 3: Some basics to consider on creating a discriminator:

- For an item that was developed exclusively at private expense (and the concomitant assertions of limited/restricted rights), the Government can evaluate the impact on (a) other evaluation factors, (b) the effects on competition for the item if it is to be procured in substantial quantities in the future, and (c) its effect on the total value of the proposal, including potential life-cycle costs (10 USC 2305; 41 USC 253b; DFARS 227.7103-10; DFARS 227.7203-10).
- Although assertions can be challenged as part of the evaluation process, it is probably better to evaluate the impact of those assertions on the Government's requirements as opposed to challenging the assertions themselves in the pre-award stage, unless resolution of the assertion is essential for completion of the procurement (DFARS 227.7103-13; DFARS 227.7203-13).

Data rights can be used as a discriminator in a variety of ways:

1. Technical Factor

- IP rights can be evaluated as part of the Government's evaluation of technical proposals during either tradeoff analysis or lowest price technically acceptable source selections. In the case of the former, the Government will evaluate the extent to which offeror's proposed IP rights satisfy the Government's minimum needs. In the case of the latter, the Government would evaluate whether the offeror's proposed IP rights satisfy the Government's minimum needs. In either case, those minimum needs and their pedigree must be clearly stated in the RFP so as to demonstrate that those minimum needs are not unduly restrictive of competition.
- If an offeror proposes to deliver IP rights associated with a commercial item, the Government should first validate that the item satisfies the definition of a commercial item. If so, then the Government should evaluate the IP rights proposed to determine whether it meets the agency's needs and does not violate Federal procurement law.

2. Past Performance Factor

- The questionnaires associated with past performance references should ask about the offeror's past performance with respect to issues such as affixing nonconforming/unjustified markings to deliverables and refusing to deliver content along with the IP rights it proposed to provide to that reference prior to award.
- The Government should review all relevant information in the Contractor Performance Assessment Reporting System for any instances where the offeror affixed nonconforming/unjustified markings to deliverables, or refused to deliver content along with the IP rights it proposed to provide to that reference prior to award.

3. Price-Based Evaluation Factor

- Price must be evaluated in every source selection. If the offeror fails to propose a fixed price for IP rights where the RFP required a price be proposed, that failure to conform to material terms and conditions of the RFP means the proposal is unacceptable and may not form the basis for award.
- If the proposed IP rights will be furnished under a cost-reimbursable Contract Line Item Number (CLIN), the Government must perform a cost realism analysis of those proposed costs and adjust the proposed costs upward as appropriate. If the proposed IP rights will be furnished under a fixed price CLIN and the Government stated it would perform a price realism analysis of that CLIN, then it must do so. In either case, the Government must demonstrate its evaluation of the offeror's proposed technical approach was consistent with the offeror's proposed costs or prices.
- Offerors can be given a price credit for proposing to deliver greater IP rights and/or greater IP than the Government's minimum needs. But such a credit must be expressly identified in the RFP. Upon demand, the Government must be able to explain how it calculated the amount of that credit.

2.7. Are there any best practices the PMO can adopt in evaluating IP as part of a source selection?

Response

A variety of best practices can be leveraged by the PMO to help improve IP evaluation.

Pre-RFP

- Determine requirements for technical data and computer software deliverables and associated IP rights for all phases of the life of the program.
- Use a data decision tree (Figure 2) to identify required technical data and computer software deliverables and IP rights and document in a tool. Consider the system baseline, the rationale for rights in deliverables. This will determine the language to be included in the RFP and inform the evaluation process.

RFP – Source Selection Considerations

- Include IP Rights as a Technical Factor. Although the PMO cannot require a contractor to provide a higher level of rights than provided by the regulations in technical data or computer software developed exclusively at private expense, the PMO can evaluate whether and how well an offeror's proposed IP rights meet the PMO's requirements. A pass/fail evaluation scheme could be construed to improperly penalize an offeror for failing to offer a higher level of rights than provided by the regulations. Instead use a tradeoff with ratings or consider a Value Adjusted Total Evaluated Price source selection approach, which provides a monetized adjustment for an enhanced aspect of a proposal (i.e., identifying a specific value beforehand that represents the better performance offered by a proposal and adjusting the offeror's total evaluated price downward by that amount if that element of performance is offered). For example, an offeror's total evaluated price could be adjusted downward by $1 million (the value of the identified level of rights to the PMO) if a certain computer software deliverable were delivered subject to GPR or UR.
- Consider including a special clause that further defines what constitutes OMIT. The DFARS provide that DoD automatically receives UR in technical data necessary for OMIT (that is not detailed manufacturing or processing data (DMPD)), but does not define those terms. Including clear definitions of the terms in the contract may limit future disputes over deliverables and rights. When identifying technical data deliverables that are necessary for OMIT, consider the impact of DMPD. For example, could the contractor be required to deliver those deliverables without DMPD or a separate version that does not include DMPD.
- Consider including a special clause addressing commercial computer software licenses (see Figure 15).
- The RFP should include an assertion table tailored to reflect any added RFP requirements (e.g., requirements to provide assertions for commercial technical data and commercial computer software, requirements to map assertions to CDRLs or statement of work/performance work statement paragraphs).
- Consider requiring in the RFP that offerors use drop downs and prepopulation of Excel spreadsheets in provided tables to ensure offerors properly complete assertions tables and for ease in reviewing and evaluating those assertions.
- Consider using specially negotiated license rights (SNLR) to incentivize agreements to deliver technical data or computer software with the required level of rights. For example, extending the time period from 5 years to 10 years, during which the PMO will have GPR in certain deliverables. Any SNLRs and how they will be evaluated must be identified in the RFP.
- Describe the PMO's sustainment strategy for the life cycle of the program (i.e., organic, competition for the system or subsystems). .
- Include a priced option for delivery of specified technical data or computer software if appropriate.

For source selection evaluation ease:

- If a source selection has a large number of technical data and computer software deliverables, consider use of a tool to organize the evaluation of technical data and computer software deliverables and rights. For example, an Access Database system could be used as follows:
    - Allow multiple evaluators and reviewers to evaluate assertions simultaneously;
    - Direct evaluators to review certain assertions;
    - Perform searches of key issues/items;
    - Identify assertion changes and issues during discussions;
    - Generate relevant reports;
    - Take advantage of assertion tables that are provided in Excel to input assertions data efficientl into the tool

2.8. What are some best practices for negotiating or creating appropriate source selection criteria to ensure that I get the appropriate rights to support the noncommercial software I'm acquiring for the entire life cycle?

Response

Conforming noncommercial acquisitions to the DFARS regulations is challenging. A key issue is planning and understanding the full life-cycle needs of the program, as these needs often change based on world events. This challenge exists in both sole source and competitive acquisitions in areas such as requirements generation, acquisition planning, drafting the solicitation/RFP, proposal analysis (competitive and noncompetitive), negotiation, award, and administration. Construction of the RFP is always difficult and can be complicated and potentially contentious for IP rights issues. The real key is appropriate planning and discussions with the entire IPT team as well as inclusion of some potentially nontraditional members to your IPT, such as logisticians and software maintainers. Further, how an RFP is created, what is expected in a proposal under sole source, the criteria used in a competition, and how the criteria are evaluated are all critical components of a successful strategy.

Beyond getting the right players, it is important for the program manager/technical team and contracting team to be in sync regarding the long-term needs of the program. What kinds of IP rights are necessary, and how does one create flexibility and plan appropriately for the financing of such. For instance, for software created under independent research and development (IRAD), the offerors proposed solutions in which one subcomponent or subsystem has technical data that was created with IRAD, which subjects this subcomponent or subsystem to the IRAD rules defined in the DFARS. This can have a significant impact to the government's sustainment strategy. It is critical to identify potential issues upfront and plan flexibility into the solicitation.

Expressly address the software product according to the needs of your program and the circumstances surrounding your acquisition. If the appropriate IP rights are lacking in the contract, the program will risk having insufficient rights in the end product. To avoid this situation, the solicitation must clearly inform the offerors of the end state that the Government wants delivered and how. It is also important to have the entire team carefully review the terms and conditions in each proposal and to include that in your negotiation position. Often, that is where the IP rights issues and areas of contention are detailed. Teams frequently overlook this area or fail to see it as an opportunity for negotiation. Because IP rights are valuable to both the contractor and the Government, they are an area ripe for negotiation.

The solicitation gives you the best opportunity to indicate exactly what you want. Ensure that you indicate the CDRLs you want to be delivered, etc. If the software is more complex, you will likely need engineering assistance to write a CDRL that specifies what should be delivered in view of the rights being acquired and what will be needed to exercise them. You should refer to the formal DFARS definition of software, as this will ensure that all elements sufficient to recreate the software are delivered to the Government.

Chapter 3 – Maximizing Unlimited Rights

The unique requirements of the Government are such that it has extremely broad authority to use and disseminate technical data and computer software regardless of how it was funded, such as when technical data is needed for OMIT purposes. Also, FFF information can be broadly disseminated because it should not implicate the proprietary interests of a contractor.

A large portion of this chapter is directed to obtaining technical data for "OMIT" purposes. The term "OMIT" does not appear in the DFARS. Rather, it is a reordered acronym that refers to the technical data "necessary for installation, operation, maintenance, or training purposes (other than detailed manufacturing or process data)." The Government is entitled to UR in OMIT data regardless of how the item to which the data pertains is funded.

The term "OMIT" can and is employed in slightly different ways in many solicitations because, depending on the service, program, and technology involved, the articulation of what constitutes "maintenance" must change. For example, for a fighter aircraft, "maintenance" must be defined broadly enough so that the USAF can repair the aircraft and return it to its original level of functionality. So, in a solicitation for a fighter aircraft, the terms "depot-level maintenance" and "organizational level maintenance" will typically be set forth in broad terms that justify the need for UR in this information. This practice is consistent with the USAF's longstanding aim to accomplish all levels of maintenance—from flight line through back shop to depot-level—organically, by contract, or through a blend of the two, depending on what best meets mission requirements.

3.1. What can the PMO reasonably expect to obtain as OMIT data?

Response

The Government, not the contractor, determines what is "necessary for installation, operation, maintenance, or training purposes." If the PMO's position differs from the contractor's, Government personnel should defend their position and not acquiesce to assertions that do not meet the program's needs. The PMO should expect and encourage pre-solicitation discussions with industry about the Government's maintenance concepts for the system to be acquired. These discussion should include expressly defining what the Government considers a part of "maintenance" (as well as "installation," "operation," and "training," though these three terms tend to be less contentious, since contractors less frequently hope to gain future business in these areas than in maintenance).

After contract award, the PMO may receive data necessary for OMIT that is accompanied by restrictive markings, which are inappropriate for UR information. Experienced acquisition professionals can all testify to having received data that seemed plainly necessary for training or maintenance needs, but which the contractor marked with "Government Purpose" or "Limited" rights. When this occurs, the Government must protect its rights. This includes defending an expansive—yet reasonable—definition of these terms, even if the contract is otherwise silent on what they may mean. Contracts are known to have gaps.

As far as what types of information may be necessary for OMIT, the PMO should insist that technical manuals, provisioning data, and proposed spare parts lists be delivered with UR, as these are all necessary for OMIT purposes. Other types of information, such as product drawings and models, may be outside the definition of OMIT data, but these types of data should be examined on a case-by-case basis. Such data may also be better classified as detailed manufacturing or process data (see Section 3.3.) if they constitute higher level engineering data of a sort not typically used by maintainers or operators.

When establishing expectations for OMIT data, PMOs should employ a team approach and consult with logistics, test, engineering, configuration management personnel. Look to legal professionals or other experts as necessary to form a Government position on a missing term or to define how a term should be understood. Pursue negotiation where it is appropriate. Negotiation can often result in terms acceptable to both parties if both are willing to be reasonable.

3.2. I am confident that certain technical data is OMIT. What should I do if a contractor either refuses to deliver the data or marks it restrictively?

Response

As indicated above, the Government generally decides what data is necessary for OMIT, in part because the Government has the final responsibility for determining the maintenance concepts that will meet the warfighter's readiness goals. Establishing requirements for OMIT, approving contract documents for obtaining OMIT data, and determining whether an offeror's proposal meets those requirements are inherently governmental functions governed by FAR 7.5.

Assuming the contract clearly requires the delivery of certain OMIT data (whether or not the contractor lists the data as necessary for operations, maintenance, installation, or training), if the contractor delivers the data with restrictive markings beyond the copyright notice allowed in DFARS 252.227-7013(f), DFARS 252.227-7013(h) provides the procedures for removing the markings. See Section 5.2 for details on these procedures.

If a contractor refuses to deliver the OMIT data at all, the contracting officer should direct the contractor to the contractual requirement to provide the data and withhold payment under DFARS 252.227-7030 as appropriate. If no contractual requirement currently exists, the contracting officer should invoke DFARS 252.227-7027, Deferred Ordering of Technical Data or Computer Software, if possible, or look to other remedy-granting clauses in the contract to obtain performance. Appropriate legal and contract remedies should be pursued if the contractor refuses performance, including the delivery of data necessary for OMIT.

While it is advisable that the PMO take into account the contractor's recommended maintenance plan, the Government ultimately defines the requirements necessary for OMIT. The contractor may not unilaterally define what the government requires to perform its mission, including its operations, maintenance, installation, or training mission. To avoid any ambiguity, the contract should clearly state from the outset what data are required to be delivered throughout the course of performance. In order to avoid a later dispute as to whether delivery of a particular data item is necessary for OMIT, consider establishing a separate CDRL exhibit specifically for OMIT data and associate the data item with that CLIN via a CDRL. In this way, it will be clear that all data delivered within that CDRL are considered necessary for OMIT and delivered with UR.

3.3. What is "detailed manufacturing and process data" (DMPD)? Under what circumstances must a contractor deliver this, and how does this categorization affect the government's rights?

Response

Detailed manufacturing and process data is defined as "technical data that describes the steps, sequences, and conditions of manufacturing, processing or assembly used by the manufacturer to produce an item or component or to perform a process." DMPD is unique, because it is specifically excluded from the grant of UR that is associated with OMIT data. But that does not mean this data cannot be acquired. It only means the Government's rights in the data may be restricted if it was developed at private expense.

Coming to agreement with a contractor on what is and is not DMPD can be difficult, especially in a sole source environment. Oftentimes, a PMO may not even believe it is asking for DMPD, but the contractor will insist it is. When these issues can be resolved in a source selection, they should be. The more the information is needed for reprocurement and the less it is needed for maintenance, the more likely the data will be considered DMPD. So if the same reprocurement ends can be achieved in other ways, it is probably best to pursue those ways rather than battle over DMPD. That is essentially the guidance in the DFARS.

None of this is to say DMPD is off limits. It also doesn't mean DMPD cannot be obtained with UR when the item, component, or process (ICP) that it pertains to was developed exclusively at Government expense. It just means that delivery of DMPD may not be necessary to meet the program's objectives. Particularly in the case of commercial derivative aircraft, the Government may be able to negotiate acceptable and cost-effective terms that are similar to those used by commercial operators and also meet the program's needs. Unlike most OMIT data, which the Government may share with non-government entities due to its UR license, DMPD provided under an access-only license might be limited to viewing by Government personnel. Source selection and PMO personnel must therefore determine whether and when these limitations meet the Government's mission requirements, and in what circumstances the Government must instead receive DMPD as a deliverable, and with what license rights.

Ultimately, the Government—not a contractor—must determine data delivery requirements, including DMPD delivery requirements. While 10 U.S.C. § 2320(a)(2)(H) likely prohibits the Government from conditioning contract award on a contractor's providing, for example, UR in its DMPD, the GAO has affirmed that the law permits the Government to require delivery of DMPD consistent with mission requirements, and the Government may give greater evaluation credit in a source selection (consistent with the published evaluation criteria) to an offeror willing to provide the Government more favorable license rights in delivered DMPD. Carefully articulating Government requirements for both DMPD delivery and license rights during the source selection process will ensure effective mission accomplishment long after contract award.

3.4. How does the commercial nature of a supply to be delivered under a contract affect the government's right in associated OMIT data?

Response

DFARS 252.227-7013 and -7015 address IP rights in noncommercial and commercial technical data, respectively. The Government's substantive rights in delivered OMIT data are effectively identical for both commercial and noncommercial technical data: there are no limitations on the Government's ability to use, modify, reproduce, perform, display, release, or disclose the data, or to allow others to do so on its behalf. Further, DFARS section 227.7102-1(3) extends this prerogative to data describing "modifications made at Government expense to a commercial item or process in order to meet the requirements of a Government solicitation." In short, once the Government has received OMIT data under a contract CDRL, the Government may do virtually anything it needs to with that data, even if that data pertain to a commercial item.

With that said, commercial OMIT data may not be as extensive as noncommercial data due to the different maintenance concepts employed by DoD and commercial operators. It is useful to keep this distinction in mind.

3.5. When should I consider negotiating for rights in technical data necessary for OMIT? What other complications do negotiations for OMIT create? Is it worth the trouble?

Response
The program manager must determine, as part of the Acquisition Strategy, all technical data that will be necessary to execute the program through its entire life cycle. The program manager must then determine what level of IP rights in that technical data is required for program execution. The program manager can then decide whether it would be in the best interest of the Air Force to negotiate a lesser level of IP rights than the Government would otherwise be entitled to receive in technical data necessary for OMIT with a corresponding reduction in the cost/price the offeror proposes to develop and produce that weapon system. This analysis must be based on the details of a particular program, such as market research, potential level of competition, developmental status of the system (e.g., the system will be developed under the resulting contract or a nondevelopmental item is being acquired), or maintenance/sustainment philosophy in order to answer the following questions:

- To whom will the program need to release or disclose a specific item of technical data?
- For what purpose will the program need to release or disclose that item?
- During what period does the program have to release or disclose that specific item?

For example, suppose the system, subsystem, or component in question cannot be repaired by Air Force personnel or contractors due to anti-tampering features—which means that a failed system, subsystem, or component will be replaced but not repaired. Under such circumstances, it would not make economic sense to acquire the technical data needed to repair that system, subsystem, or component, much less UR to that technical data. Instead, the PMO should ensure that it acquires the installation data that will be needed for the repair-and-replace maintenance philosophy. Data to repair the item, on the other hand, is not very valuable due to the maintenance philosophy.

Another example may be where market research indicates there are few potential competitors, that no likely competitor would be willing to deliver all technical data required by the program, or that no likely competitor would be willing to deliver technical data necessary for OMIT subject to UR. In any of these cases, the program could analyze whether potential competitors might be willing to deliver all necessary technical data if the program agreed to a level of rights lower than UR but that still allowed for program execution throughout the life cycle of the program. In contrast, if competitors have the necessary organization, experience, configuration control processes, and technical skills—or the ability to obtain them—the program manager should seek to acquire at minimum GPR to such technical data in order to complete maintenance/sustainment of the system, subsystem, or component, and thereby reduce the total life-cycle cost of the program.

So a lot can depend on the maintenance/sustainment philosophy, as well as the market realities. The more these issues can be resolved when the market is competitive, the better.

3.6. I am in a sole source environment, and the contractor is refusing to agree to any OMIT requirements. How should I handle this? Is the situation different during pre-award negotiations than for modifications to an existing contract?

Response

While a competitive environment provides the Government excellent leverage in seeking data deliverables and licenses necessary for future system sustainment (including OMIT and, in certain circumstances, system modifications), the relationship is reversed when the parties contract on a sole source basis. As the sole source, contractors attempt to hold back data to maximize revenue and profits. Whether this is legitimate behavior or not, it is a reality: contractors play hardball.

As such, the Government will need to employ creative techniques to reach a reasonable outcome. There will be times when it is impossible to persuade a contractor to provide data sufficient to compete all future sustainment efforts (i.e., the contractor may be able to hold back enough data to ensure its future involvement in some sustainment activities). Still, if Government negotiators plan well, and far enough in advance, and if they show sufficient resolve in the face of a contractor's professed unwillingness to provide sufficient data and licenses, they can lay the foundation for reaching a reasonable outcome.

The Strategy

Step 1: Recognize that this is more of a negotiation challenge than a legal one, which means that while the solutions will involve good advocacy, they will require more than mere knowledge of, or citation to, law or policy. Because of this, while an attorney may sometimes be the best spokesman for the Government during IP rights negotiations, the Government must absolutely employ a team approach, bringing expertise to bear from multiple functional areas, including program management, engineering, contracting, logistics, and configuration management.

Step 2: Nevertheless, there may be some legal authority that can strengthen the Government's negotiating position. For instance, the PMO may be able to leverage other laws and regulations when purchasing commercial derivative aircraft to obtain the data it needs (see, e.g., Section 3.7). Also, clearance authorities should require that acquisition strategies comply with 10 U.S.C. § 2320(e), which requires that those strategies "provide for technical data rights needed to sustain . . . systems and subsystems over their lifecycle." Justification and Approval documents can explicitly condition sole source award on the Government obtaining sufficient IP rights to compete future sustainment activities that are the most cost effective. Then, if a contractor offers unacceptable terms during follow-on contract negotiations, Government negotiators may avoid an impasse by reminding the contractor that they do not possess the authority, per the approved Acquisition Strategy, to enter into an agreement that effectively precludes contracting out sustainment efforts to anyone other than the sole source prime contractor.

Step 3: Ultimately, the Government must be willing to forego a bad deal, or even a deal that is attractive in the short term, to ensure it gets a good one in the long run. This will mean, among other things, that Government negotiators must calculate the life-cycle cost differential between sustainment based on the contractor's proposed data deliverables and licenses, and sustainment based on the Government's desired maintenance concept with all the IP rights that requires. Having made this calculation, the Government must then refuse to accept diminished IP rights unless the contract price is so low that it makes up for likely future price premiums. This will rarely be the case, so Government negotiators will normally need to be committed to acquiring sufficient IP rights up front, even at greater cost, understanding that these IP rights will ultimately pay for themselves through future cost avoidance.

Best Practice

Outdo the contractor in preparation and tenacity. Determine what data deliverables and license terms the Government requires and make these clear to the contractor from the outset of negotiations. Know what data deliverables and licenses are worth by evaluating different lifecycle cost scenarios as accurately as possible. Then be willing to walk away from negotiations rather than accepting terms that may be pennywise but pound foolish. Finally, offer any concessions you can that do not threaten minimum requirements (e.g., consider trading down from unlimited to GPR where possible, in exchange for broader delivery of data). Refer to Section 5.3 for additional ideas.

3.7. I heard that the Federal Aviation Administration (FAA) requires certain types of technical data to be provided to the owner of an aircraft without restriction. How can I use this requirement to my advantage?

Response

The FAA, pursuant to 14 CFR 21.50(b), requires that "design approval holders" (normally the OEM), "furnish a complete set of Instructions for Continued Airworthiness (ICA) to the owner of each type aircraft, aircraft engine, or propeller upon its delivery, or upon issuance of the first standard airworthiness certificate for the affected aircraft, whichever occurs later." The design approval holder is required to make the ICA "available to any other person required by this chapter to comply with any of the terms of those instructions" as well as to "make available changes to the ICA to any person required by this chapter to comply with any of those instructions."

This means that as a condition of obtaining an FAA Type-Certificate, the design approval holder has agreed to provide the ICA to the owner/operator (the Air Force) under a license that enables the ICA to be distributed to any 3rd party contractor who must comply with the ICA (i.e., any contract maintenance provider).

ICA requirements apply to aircraft, rotorcraft, engines, propellers and their parts. The contents of the ICA are defined in detail in the Code of Federal Regulations. In general, ICA encompasses:

- All Airworthiness Limitations
- All maintenance and repair instructions essential to the continued airworthiness of the product
- All recommended maintenance, inspection, and overhaul information
- O-/I-Level instructions
    - Installation, servicing, inspection, storage, etc.
    - Maintenance scheduling information
    - Maintenance manuals
- D-Level instructions overhaul manuals
    - Mandatory for engines and propellers
    - Depends on Airworthiness Limitations and recommended maintenance programs for aircraft and aircraft appliance

Thus, it can be helpful to include ICA-type data requirements as a baseline in your commercial-derivative acquisitions. Any deltas for military purposes can be negotiated or procured from there.

ICA requirements can be leveraged if you are supporting a commercial derivative aircraft that has an FAA Type-Certificate, or if you are supporting an engine or a propeller on a commercial derivative aircraft with a Type-Certificate. ICA requirements can be leveraged during any phase of the life cycle.

Since the Air Force has not aggressively leveraged FAA rules to obtain ICA, you may encounter resistance from the OEM when attempting to trigger ICA requirements. It may be helpful to remember two points:

- The OEM is required to provide ICA in order to obtain a Type-Certificate from the FAA. This requirement is independent of the contract between the OEM and the Air Force.
- The FAA has already determined that OEMs cannot include restrictive rights statements (e.g., "Proprietary" or "Limited Rights") in the ICA (see, http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgPolicy.nsf/0/757c84ac9becec27862579d00054df95/$FILE/PS-AIR-21.50-01.pdf).

The Strategy

Step 1: If you are acquiring or may potentially acquire a commercial derivative aircraft, require offerors to deliver ICA under a separate CDRL. It may be necessary to write a one-time use DID until the Air Force develops a permanent DID. This should be accomplished even if the maintenance concept has not been fully developed in every acquisition involving commercial derivative or commercial type aircraft, engine, or propeller

Chapter 4 – Software Acquisition

Software has become a critically important part of nearly every system procured by the Air Force. Management of the licensing issues associated with the acquisition and sustainment of software presents some unique challenges that the PMO must address. This chapter provides some tips on handling issues related to commercial computer software, a complex topic with many unique factors to consider. It also addresses software maintenance, providing a plan to posture the PMO for success during the O&S phase. Finally, the chapter concludes with a trio of white papers that cover emerging topics in software acquisition.

4.1. Commercial Computer Software

4.1.1. What do I need to know about commercial computer software acquisition? Do mandatory sources exist? Are there other resources that can assist my acquisition?

Response
Commercial computer software is probably one of the more complex commercial items an agency can buy. This is because the FAR and DFARS guidance, though straightforward, does not hint at some of the complexities lurking behind their high-level policies. When it comes to ensuring the software is properly classified, knowing which terms and conditions apply, and filling the gap left by the absence of a standard contract clause, numerous complexities may accompany these acquisitions.

In general, commercial software is purchased through preferred purchasing agreements and similar buying programs. You can find the precedential list of buying programs in AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*. If the software is available through one of these sources, then one of these buying programs should be a part of your acquisition.

When it comes to enterprise software—which can generally be thought of as commercial off-the-shelf (COTS) software that tends to be used enterprise-wide—you should be using *DOD's Enterprise Software Initiative (ESI)*. The DoD CIO has created ESI to standardize software purchasing processes and asset management for many types of COTS software and commercial IT. ESI promotes the use of enterprise software agreements (ESAs) to obtain favorable terms and pricing for commercial software and related services. When buying commercial software, it is best to become familiar with ESI and how it can support your acquisition, particularly in instances where the item being acquired is used across the Air Force.

When the software being acquired will not be used enterprise-wide and is not available through one of the above buying programs, then the determination as to whether the software is a commercial item and the terms, conditions, and other requirements are appropriate must be made by the PMO. This can be challenging, particularly when the software being acquired is not COTS but still a commercial item. Though the next few sections will walk you through some of the more relevant topics, the PMO should seek help, including guidance from program counsel, when making these determinations. While the resources listed below are helpful, an accessible advocate is invaluable to equipping you for success.

The Strategy
Step 1: Begin with AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*, particularly Chapter 3, Software Asset Management. There you will find guidance regarding mandatory sources, enterprise ver-

sus nonenterprise software, proper asset management, and software reuse and disposal. The AFMAN primarily deals with COTS software.

Step 2: Become familiar with DoD's ESI by reading DFARS Subpart 208, DFARS PGI 208.74, and the ESI web site at http://www.esi.mil. The Software Buyer's Checklist available through the ESI web site is particularly helpful.

Step 3: The Air Force web sites at http://www.netcents.af.mil and https://www.afway.af.mil are also useful for explaining available Air Force buying programs.

4.1.2. Does the Government purchase commercial computer software on the same terms provided to the public? Does that mean I don't have to review the vendor's licensing terms?

Response

Yes and no. DoD purchases commercial computer software on the same terms provided to the public, provided that those terms meet the needs of your acquisition, your agency, and Federal law. But the PMO still needs to review those terms to ensure they meet these various needs.

Among these groups of needs, the legal requirements are probably easiest to address. The other two groups are contingent on circumstances unique to the acquisition. For example, cybersecurity requirements can be much more stringent depending on the type of information being stored and exchanged. As such, Air Force PMOs should identify any unique circumstances to their proposed use or need of a commercial software item prior to making a purchase. Then analyze the software license to ensure these circumstances can be accommodated. Where terms need to change, negotiate with the vendor to reach an acceptable outcome.

Market research is extremely important in commercial item acquisitions. When it comes to requiring a certain term or condition, having market research to show that the desired term is acceptable in the commercial practice can fend off challenges that the requirement is unreasonable should they be presented.

The Strategy

Step 1: Identify the needs of your agency and acquisition.

Step 2: Review the software license to ensure it is acceptable considering these constraints. To do this, break the license down into manageable parts and deal with each part individually. For example, though many types of terms may be in a license, if you segregate them into categories for what you can accept, cannot accept, and what can be negotiated, you will have started on a good path for finding an acceptable outcome.

- Category 1: Terms that are consistent with Federal law, meet agency needs, but differ from the default terms contained in the FAR/DFARS. Many commercial license terms will generally fall within this category. These terms can be accepted, unless they conflict with the FAR/DFARS (e.g., FAR 52.212-4 and other mandatory terms), in which case they can be accepted only when the FAR/DFARS allows those terms to be modified or tailored. The decision to accept Category 1 terms is committed to the discretion of the contracting officer.

- Category 2: Terms that are consistent with Federal law but do not meet the needs of your acquisition or agency. These terms should be removed from a licensing agreement or should be modified or addressed elsewhere in the contract. If an agency requires a particular term to be included in the license to meet its needs, then the requested term should reasonably reflect those needs and not be unduly restrictive of competition. A standard license for non-COTS software is not required to be accepted as is; rather it is a starting point to determine terms that meet the agency's needs. It is also critical to carefully review the language in the license describing the ways in which the software may be used to be certain it will meet the agency's needs. When software will be modified to meet DoD requirements, take additional steps to ensure there is a meeting of the minds as to which terms will govern the software in its modified form.

- Category 3: Terms that are inconsistent with Federal law. There is no authority to accept these terms. The license terms must be rejected by the agency, renegotiated, or otherwise excised from the contract. Consult with program counsel when dealing with this situation.

4.1.3. If another program or agency has already accepted the vendor's commercial license, can I just accept them without further review?

Response
In short, no you shouldn't. When ordering commercial software from an existing purchasing vehicle, such as an ESA, a Federal supply schedule (FSS), another mandatory source, or from the DoD inventory, you can expect that the software will be provided with pre-existing terms. Those terms may have been negotiated, but even if they were, they were unlikely to have been negotiated for your particular acquisition. As such, you should review the terms of a commercial computer software license to ensure that they meet the needs of your acquisition and are consistent with Federal law.

DFARS 208.7403(3) probably says this best with reference to DoD's ESI program. That section directs acquisition officials, upon finding commercial software on an ESA, to ensure that the terms of the agreement meet the requirements of their program before making the purchase. This direction supports the DoD policy to acquire commercial software under standard terms except when those terms do not meet agency needs or are inconsistent with Federal law.

While you can expect that, before purchasing software from a mandatory source or other Air Force-wide buying program, offending terms and conditions may have been excised, you cannot expect that those terms were negotiated with the needs of your acquisition in mind. In other words, while these outlets may have alleviated some of the burdens of purchasing commercial software, by no means have they alleviated all. Before making the purchase, the contracting officer must still confirm that the terms of the license meet the needs of the acquisition and his or her agency and that they are consistent with Federal law.

When ordering from an existing purchasing vehicle, review the terms that apply to your procurement and deal with any terms that do not meet the needs of your acquisition or are inconsistent with Federal law.

The Strategy
This strategy is taken from a DoD ESI example.

Step 1: Begin by reviewing the *ESI Software Buyer's Checklist* for guidance, then review any guides or other instructions on how to order from the purchasing vehicle you intend to use.

Step 2: Review the terms of the purchasing vehicle's agreement to learn which terms and conditions have already been addressed. Become familiar with these terms prior to making a purchase, because those terms are incorporated into the order. A term already incorporated into the existing purchasing vehicle cannot be excised by the order, but those terms can be strengthened or enhanced.

Step 3: Address any discrepancies between the existing terms and the needs of your acquisition either directly with the vendor of with the purchasing agency that controls the purchasing vehicle.

4.1.4. I am purchasing commercial services from a vendor who will write software* to meet the needs of my program. How should I handle this situation?

Response
The challenge with commercial services acquisitions where writing software is one of the tasks to be performed is that, when using the DFARS, no term or condition exists to allocate rights in software the contractor creates. If you are ordering under an FSS through GSA, or through some other agency using the standard FAR terms, this may not be the case, but it depends on whether the software being written is repurposed software or software that is “first produced in the performance of the contract.” This could leave quite the gap when modifying software, firmware, or other software required to make your software work. Thus, you should handle the software products of commercial service contracts deliberately and with careful market research and adequate planning.

To do this, it is best to deal expressly with rights in the software/firmware the vendor will be creating/modifying rather than rely on the presumed application of a default term. Come to a meeting of the minds on this subject matter and your bargain will be more complete and easier to enforce should there be a disagreement later.

One way to deal expressly with rights in the software is to treat the acquisition as a Special Work under DFARS 252.227-7020. Read the prescriptions for this clause to see whether it should apply to your acquisition. If not, you can apply DFARS 252.227-7014 to the software and expressly agree in the contract that the work product will be noncommercial software even though the product of a commercial contract. Though treating the end product as noncommercial, this clause is robust enough to preserve the commercial status of various software components on which the final product may rely. Lastly, you can negotiate your own license to “fill the gap” so long as it meets your needs and is subject to the usual caveats regarding negotiations.

Because you are contracting using commercial procedures and practices, you should be prepared for complaints that your requirement for rights in the software are harmful to competition or inconsistent with commercial practices. The keys to responding to these complaints are (1) to document a reasonable basis for your requirement and (2) to supplement that requirement with market research showing that commercial practices support your requirement. All kinds of commercial practice exist, so targeting your market research appropriately can be very important in this regard.

The Strategy
Expressly deal with the software product according to the needs of your program and the circumstances surrounding your acquisition.

Step 1: Look to the DFARS sections referenced above for guidance. If the contract is silent, you risk having no rights in the end product other than the implied rights to use what’s made available to you. This means you also need to be clear in the contract, likely through a CDRL, to specifically identify the software deliverables that you want to be delivered.

Step 2a: If the software comprises simple scripts, then having the scripts may be sufficient along with instructions as how to use them.

Step 2b: If the software is more complex, you will likely need engineering assistance to write a CDRL that specifies what should be delivered in view of the rights being acquired and what will be needed to exercise them.

Step 3: For more complicated efforts, a categorization and prioritization of the software should be requested and specific instructions levied so as to require the software code to be delivered. These instructions should include complete and usable guidance that will allow the software to be recreated as originally intended without additional cost, services, licenses, or maintenance fees.

> * Please note that the term “software” is inclusive of the following: creation/design of new software, modifying software, modifying firmware, or using utilization services with some modification of software, creation of new software, or modification of firmware for making embedded software work.

4.1.5. My program is charged with acquiring a major system, and commercial computer software will likely be part of the product baseline. How can I ensure that such software will meet the needs of my program and be consistent with Federal law?

Response
The challenge with a major system acquisition is that, inevitably, commercial software will find its way into the baseline, and the FAR/DFARS provides no clear means for handling it. This is problematic because a recent agency board decision treated a commercial software license as a contract of adhesion that was binding due to the Government’s passive assent to its terms. In that decision, no express acceptance was required to terms the Government was ultimately found to have breached.

Thus, in a major system acquisition, PMOs should communicate their requirements and limitations for accepting commercial computer software and express to vendors how they will review and accept those terms over the course of the acquisition. For example, a PMO may allow a vendor to purchase from an approved Government source, which can be beneficial for software being used enterprise-wide. The PMO can also dictate its own process for reviewing and accepting computer software. Regardless, it is incumbent on Air Force PMOs to deal with commercial computer software licenses in a way that ensures the accompanying terms do not frustrate the needs of their acquisition.

As part of the RFP, communicate to offerors how commercial computer software will be handled during your acquisition, preferably through assertion, evaluation, and express acceptance.

Even when a contractor provides commercial software obtained through the ESI program or from an existing supply schedule (FAR Part 51), the commercial software license should be reviewed for consistency with Federal law and the requirements of your program. When ordering from these sources, the terms of your contract will very likely be subordinate to the existing terms, which means it is paramount to work through any issues or inconsistencies before acceptance.

The Strategy
Step 1: Have offerors specify commercial software license terms as part of their proposal, either through Section L or a clarification as to the scope of DFARS 252.227-7017.

Step 2: Consider also including a Section H requirement describing how commercial computer software will be treated during the acquisition. For example, it is best to condition acceptance on compliance with FARS/DFARS policies and express acceptance by the contracting officer.

Step 3: During source selection, evaluate, consistent with Section M, commercial licenses for offending terms and either classify noncompliance as a risk or make proposal acceptability contingent on consistency with the needs of your acquisition, agency, and Federal law.

4.1.6. How do I know whether the software I'm buying should be treated as a commercial item? Should I accept the vendor's assertion or make my own determination?

Response

The challenge of making commercial item determinations for software is that almost all software could be encompassed by the broad and almost limitless commercial item definition in FAR 2.101. That said, it would be a mistake to assume that this makes all software commercial. Software can be licensed under drastically different terms and conditions. If one treats the wrong software as commercial, the Air Force could be left paying for it in perpetuity, even though the Air Force paid to develop the software in full.

This risk is present even when the Air Force is merely modifying software to meet its needs rather than developing software from the start. When modifications rise to the level of "development," the Air Force should be getting more generous licensing terms than what a commercial license typically provides (see DFARS 252.227-7014). Thus, to protect the Air Force's interest, commercial item determinations involving software should be handled carefully.

The key to making a proper commercial item determination for software is to rely heavily on market research and to become familiar with the many examples provided by DoD's Commercial Item Handbooks. The best practice is to have gathered sufficient research to support your determination that (1) the software itself, (2) the terms of its license, and (3) its pricing are consistent with the commercial marketplace.

The Strategy

Step 1: Begin with the market research required by the FAR. This will inform you as to whether the software should be treated as a commercial item or has previously been determined to be a commercial item. It will also show what price is fair and reasonable and under what terms the software should be licensed.

Step 2: As part of your market research, identify whether the software you intend to buy is available through buying programs like DoD's ESI program or an FSS. If so, then the software very likely should be properly classified as a commercial item.

Step 3: Before making your determination, become familiar with resources such as the DoD Commercial Item Handbook or those made available through the DCMA Commercial Item Group. These resources often include examples that can guide your decision making.

Step 4: Make your commercial item determination consistent with what your market research supports and using the guidance and analogous examples available through DoD channels.

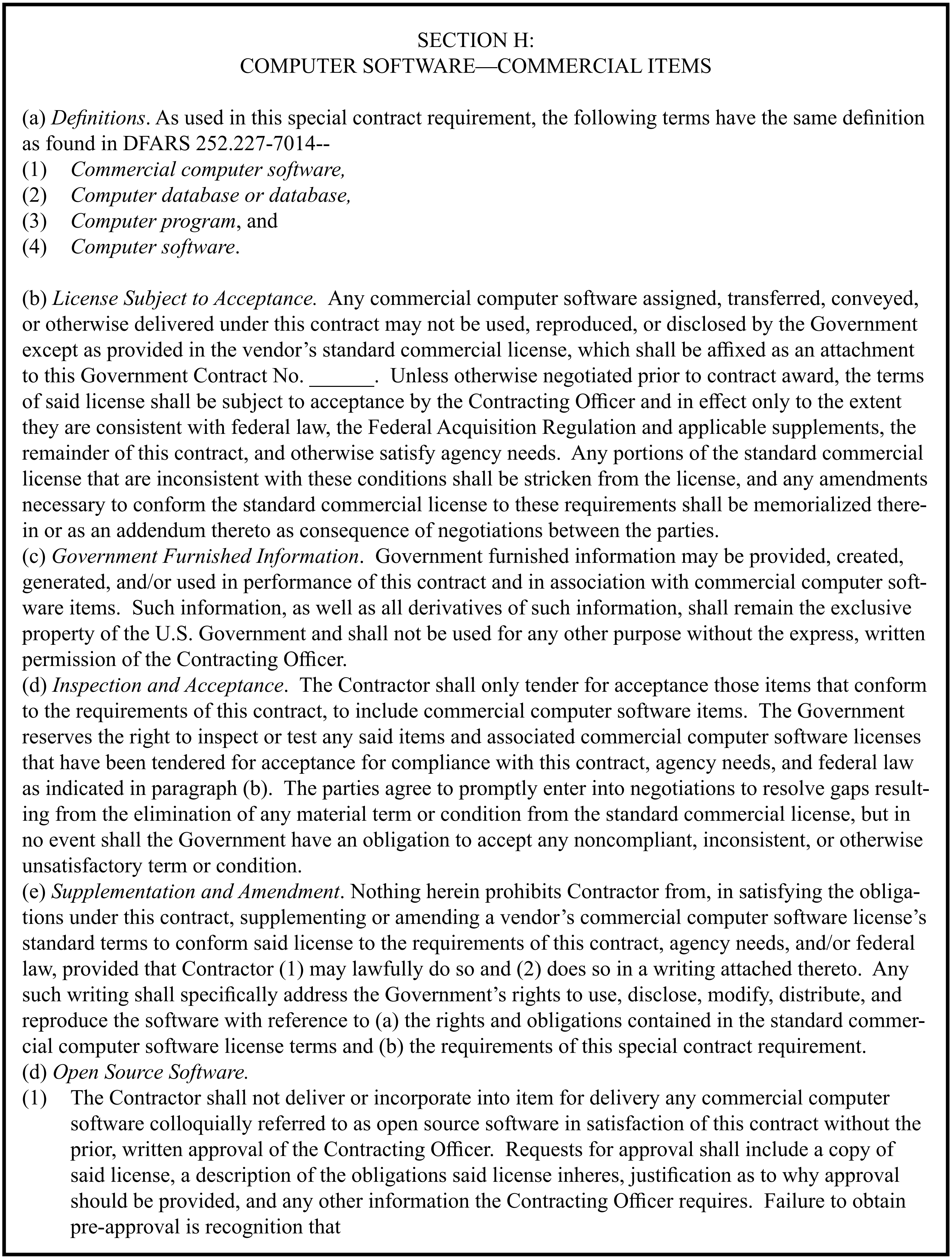


Figure 15. Sample H-Clause for Review and Acceptance of Commercial Software

SECTION H:
COMPUTER SOFTWARE—COMMERCIAL ITEMS

(a) *Definitions*. As used in this special contract requirement, the following terms have the same definition as found in DFARS 252.227-7014--

(1) *Commercial computer software,*
(2) *Computer database or database,*
(3) *Computer program*, and
(4) *Computer software*.

(b) *License Subject to Acceptance.* Any commercial computer software assigned, transferred, conveyed, or otherwise delivered under this contract may not be used, reproduced, or disclosed by the Government except as provided in the vendor's standard commercial license, which shall be affixed as an attachment to this Government Contract No. ______. Unless otherwise negotiated prior to contract award, the terms of said license shall be subject to acceptance by the Contracting Officer and in effect only to the extent they are consistent with federal law, the Federal Acquisition Regulation and applicable supplements, the remainder of this contract, and otherwise satisfy agency needs. Any portions of the standard commercial license that are inconsistent with these conditions shall be stricken from the license, and any amendments necessary to conform the standard commercial license to these requirements shall be memorialized therein or as an addendum thereto as consequence of negotiations between the parties.

(c) *Government Furnished Information*. Government furnished information may be provided, created, generated, and/or used in performance of this contract and in association with commercial computer software items. Such information, as well as all derivatives of such information, shall remain the exclusive property of the U.S. Government and shall not be used for any other purpose without the express, written permission of the Contracting Officer.

(d) *Inspection and Acceptance*. The Contractor shall only tender for acceptance those items that conform to the requirements of this contract, to include commercial computer software items. The Government reserves the right to inspect or test any said items and associated commercial computer software licenses that have been tendered for acceptance for compliance with this contract, agency needs, and federal law as indicated in paragraph (b). The parties agree to promptly enter into negotiations to resolve gaps resulting from the elimination of any material term or condition from the standard commercial license, but in no event shall the Government have an obligation to accept any noncompliant, inconsistent, or otherwise unsatisfactory term or condition.

(e) *Supplementation and Amendment*. Nothing herein prohibits Contractor from, in satisfying the obligations under this contract, supplementing or amending a vendor's commercial computer software license's standard terms to conform said license to the requirements of this contract, agency needs, and/or federal law, provided that Contractor (1) may lawfully do so and (2) does so in a writing attached thereto. Any such writing shall specifically address the Government's rights to use, disclose, modify, distribute, and reproduce the software with reference to (a) the rights and obligations contained in the standard commercial computer software license terms and (b) the requirements of this special contract requirement.

(d) *Open Source Software.*

(1) The Contractor shall not deliver or incorporate into item for delivery any commercial computer software colloquially referred to as open source software in satisfaction of this contract without the prior, written approval of the Contracting Officer. Requests for approval shall include a copy of said license, a description of the obligations said license inheres, justification as to why approval should be provided, and any other information the Contracting Officer requires. Failure to obtain pre-approval is recognition that

> Contractor has investigated the risks, the Government requirements, and concluded that all obligations can be reconciled and satisfied.
>
> (2) Contracting Officer approval shall only be provided in writing. The Contractor shall indemnify and save and hold harmless the Government, and its officers, agents, and employees acting for the Government, against any liability, including costs and expenses, for the Government's non-compliance with any open source software license not previously approved by the Contracting Officer.
>
> (f) *GSA Schedule Contracts*. Unless expressly incorporated therein, nothing in this special contract requirement shall apply to commercial computer software items acquired under a GSA schedule contract when said item has been acquired with the prior authorization of the contracting officer for the purposes of this contract.
>
> (g) *Notice*. The Contractor shall affix a notice substantially as follows to any commercial computer software delivered under this contract:
>
> Notice—Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction and disclosure are as set forth in Government Contract No. ________________.

4.2. Software Maintenance

4.2.1. What noncommercial computer software, data, and documentation should I look to acquire in a request for proposal to ensure that the Government can either sustain software organically or place it into competition for sustainment for the life cycle of my weapons system?

Response

The Government may choose to sustain software organically or place it into an open competition for life-cycle sustainment of a weapon system. This could cover numerous types of software, including embedded, mission support, IT and business type systems. Modern weapon systems are composed of multiple software subsystems potentially maintained by numerous teams. The software change rate for those subsystems varies from minimal (e.g., flight controls) to significant (e.g., stores management, electronic warfare, etc.) over the course of the weapon system life cycle. The Government should evaluate the potential change rate when looking to sustain software either organically or by placing it into open competition. The return on investment for software with anticipated low change rate may not be worth the associated cost of standing up this effort.

The Government must determine the noncommercial software that will be sustained for a weapon system. After identifying the software for sustainment, the Government should analyze the type of software category and consider acquiring the items listed below for sustainment purposes. Once the list of items is selected, the Government must request the information through a corresponding CDRL to ensure delivery. As industry continues to lean towards Agile Software Development, the Government must consider periodic updated deliveries of items throughout the acquisition of a weapon system.

- Plans
    - Software Development Plan
    - Software Installation Plan—for user sites
    - Software Transition Plan—to the support agency
- Concept/Requirements
    - Operational Concept Description
    - System/Subsystem Specification
    - Software Requirements Specification—the requirements to be met by a Computer Software Con-

    - figuration Item
    - Interface Requirements Specification
- Design
    - System/Subsystem Design Description
    - Software Design Description—the design of a Computer Software Configuration Item
    - Database Design Description Interface Design Description (IDD)
- Qualification/Test products
    - Software Test Plan —for conducting qualification testing
    - Software Test Description—cases/procedures for qualification testing
    - Software Test Report—results of qualification testing
    - System Test Plan
    - System Test Description
    - System Test Report
- User/Operator manuals
    - Software User Manual—instructions including installation
    - Software Input/Output Manual—instructions for users of a batch or interactive software system that is installed in a computer center
    - Software Center Operator Manual—instructions for operators of a batch or interactive software system that is installed in a computer center
    - Computer Operation Manual—instructions for operating a computer
- Support Manuals
    - Computer Programming Manual—instructions for programming a computer
    - Firmware Support Manual—instructions for programming firmware devices
- Software
    - Software Product Specification—the executable software, the source files, and information to be used for support
    - Software Version Description—a list of delivered files and related information
    - Source code
    - Executable code
- Additional “non MIL-STD 498” items
    - Software Development Environment, including but not limited to compilers, software tools, software licenses, and the configuration of the environment
    - Where applicable, modeling and simulation of the subsystem/system
    - Software Test Environment, including but not limited to simulations, test assets, software licenses, testing tools (automated or custom built) and scripts, etc…
    - Build scripts

The Strategy

Step 1: Determine the acquisition and system sustainment strategy for software. This is documented in the LCSP.

Step 2: Based upon the LCSP, determine the software that will be sustained organically and/or placed in open competition.

Step 3: Develop corresponding CDRLs in the RFP for the noncommercial computer software, software documentation, and data.

Step 4: Keep the following concepts in mind:

- If no CDRL is associated with a technical data or computer software item, the contractor is under no obligation for delivery. After contract award, it will be cost prohibitive to attempt to obtain technical data or computer software items, including source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, firmware, and related material.

- Commercial software IP rights can be modified through the use of a SNLR license. Ensure that required commercial items are identified by the prospective contract bidder and an SNLR license is included to allow Government use and access. Ensure that any restrictions on the use of commercial items are also identified.
- Simulations and scripts used to compile, build, and test software components are often overlooked when identifying deliverables. Ensure that these items and any restrictions on their use are identified, along with associated SCRs and CDRLs, for delivery to the Government.
- Consider consulting with software sustainers and developers to ensure the correct and proper deliveries are identified, ordered, and delivered to enable software sustainment strategies.
- Target data delivery to the Government by IOC (initial operational capability) to allow time to establish Core maintenance by IOC+4.
- Consult with software sustainment experts to assist in the identification and evaluation of the necessary data.

4.2.2. What data and documentation should I look to acquire to ensure that the Government can develop organically or place into competition Test Program Sets (TPSs) to support Intermediate Level (I-Level) and/or Depot Level (D-Level) avionics repair?

Response

The Government may choose to repair Line Replaceable Units (LRU) and/or Shop Replaceable Units (SRU) for the life cycle of the weapon system. Although some may be deemed throw-away items, typically for a major weapon system, the majority are repaired and placed back into the supply chain. To efficiently diagnose malfunctioning LRUs/SRUs, the Government must develop TPS software. Currently, the directed and preferred Automated Test Equipment for the Air Force is the Versatile Depot Automated Test System (VDATS).

The Government must identify the LRUs/SRUs that will be repaired for the life cycle of the weapon system. For each LRU/SRU identified, the Government should require the OEM to deliver to the Government, in a usable format, the data, drawings, software, and documentation needed to establish test, repair, and maintenance of the items. Without the information listed below, the Government will incur additional costs for reverse engineering or may not be able to develop the TPSs needed for maintenance.

- General Data Requirements:
    - LRU and SRU schematics and LRU interconnect drawings
    - Assembly drawings including parts layouts
    - Parts lists
    - Power requirements
    - OEM acceptance test requirements and procedures including OEM factory test source code, if applicable
    - OEM Test Requirements Document (TRD)
    - Required for LRUs
- Additional Data as Applicable:
    - Non-standard parts specifications
    - Data for programmable read-only memory, erasable programmable read-only memory, electrically erasable programmable read-only memory, and ultraviolet erasable programmable read-only memory.
    - Programmable Logic Device Joint Electronic Device Engineering Council (JEDEC) files, equations and/or function tables

    - Data for Field-Programmable Gate Arrays, Application Specific Integrated Circuits, and Custom Integrated Circuits. This includes Detailed Description Documents, Source Control Drawings, schematics, Very High Speed Integrated Circuit Hardware Description Language (VHDL) Models, Boundary Scan information (including models and test data), Register Maps, and Theory of Operation, as needed to understand functional requirements and to allow generation of functional test software.
    - Firmware listings and source code for memory components
    - Central Processing Unit Assembly Program Listings
    - Embedded LRU software required for testing and the associated documentation (e.g., Built-In Test Software, Test Operational Flight Program (OFP), and Operating System Software)
    - Design specifications and Interface Control Documents/System Interface Description Document
    - Special fixtures required for LRU testing and drawings for noncommercial Aircraft Mounting Trays
    - Logic diagrams
    - Timing specifications
    - Cooling requirements
    - LRU Chassis drawings
    - Altered Item drawings
    - Special Tooling or Unique Repair Data that may be required during TPS Development
    - LRU Extender Card drawings if available
- Additional Information:
    - A gap analysis between test requirements and VDATS capabilities must be completed
    - Identify any Environmental Stress Screening (ESS) requirements for test and repair (post manufacturing)
    - Is a follow-on system test required after an end-to-end test for a particular LRU?
    - Provide all security requirements as applicable. For example, hardware and embedded software classification levels, Security Technical Implementation Guides followed (including allowances), and Basic Input/Basic Output (BIOS) passwords and settings.

The Strategy
Step 1: Identify LRUs/SRUs that require I-Level/D-level avionics repairs

Step 2: Include delivery option in the RFP for the delivery of the data identified above in usable format to generate TPSs for I-Level/D-Level maintenance

Step 3: Order/purchase needed OEM data (prime and/or suppliers) identified above, in a usable Government format, for each LRU/SRU requiring I-Level/D-Level maintenance

Step 4: Target data delivery to the Government by IOC to allow time to develop TPSs and establish Core depot maintenance capablity by IOC+4.

Step 5: Consult with software sustainment experts for assistance in the identification and evaluation of the necessary data.

4.3. Other Software Topics

4.3.1. White Paper on Open Source Software

1. Open-source software (OSS) is a leveraging opportunity that encourages reuse, modularity, and cost savings. Use of OSS requires the same compliance as any commercial software purchased and utilized within a development environment. These steps include following the end-user license agreement (EULA) and providing information technology oversight to ensure usage complies with the licensing agreement. Programs should incorporate OSS with minimal risk to the Government.

2. OSS is not a free license. A license agreement requires some sort of return for the developing organization. Many OSS that do not have monetary requirements are attempting to generate advertising or encourage the enhancement of the codebase by the user community. Some instances of this are called “copyleft,” where any changes or modifications must be fed back into the community. Furthermore, there are some licenses that have specific requirements that state obscure details such as allowing unfettered access to the development environment or providing public release of all source code utilizing the OSS.

3. Permissive licenses generally only require keeping the copyright notice of the original author. This is the preferred licensing method. Examples of this type are MIT/X11, BSD, and Apache clauses.

4. Restrictive licenses generally require some sort of requirement to either contribute back to the codebase or require some sort of insight by the community to how it is being used. This can vary, but is unique based on the license being used. Use of this type of license should be determined on a case-by-case basis utilizing software experts as well as legal and financial support. Restrictive licensing can fall into two categories, referred to as *weak* and *strong*.

- A *weak* restrictive license can be used similar to a permissive license with no modifications to the licensed code. However, any changes to that code require updates to the community for further development of the codebase, at large. Furthermore, modified code must be distributed as a whole with the final product. Examples of this are Eclipse Public License (EPL), Lesser General Public License (LGPL), and Mozilla Public License (MPL).
- A *strong* restrictive license goes a step further and not only requires updates to the community, but also requires that any codebase compiled with this software must also be shared with the community. Examples of this are General Public License v3.0 (GPL 3) and Affero General Public License (AGPL). Use of any of these licenses should be done with extreme caution and extensive review.

4. While there have been many studies done by FFRDCs and other DoD-supported actions, the only guidance published is the memorandum from the DoD CIO in 2009, “Clarifying Guidance Regarding Open Source Software (OSS),” which clarified conflicting guidance in DoDI 8500.2 and DoDD 8320.02 to encourage the use of OSS in DoD, where applicable. Moreover, use of the software must follow the Designated Approval Authority’s guidance.

5. Legal review generates additional concerns with liability and distribution. Each license can have specific wording that limits the ability for the government to agree to the license. With commercial software, the license can be negotiated with the owner. With OSS, most software is a contribution from a whole community and would require concurrence with everyone in that community to change the license. While it could be possible to contact everyone on a very small codebase, most OSS have hundreds of contributors making it improbable to contact and receive complete concurrence. Assuming the license cannot be modified, each area of the license that conflicts with our ability to comply must be addressed individually. Below are some instances and recommended mitigations.

- Indemnification. The government cannot agree to this statement, but it appears in most OSS. However, the risk of litigation for this clause is low as long as the software stays within the U.S. Government (USG) for government use. Once this software gets used in any type of Foreign Military Sales (FMS) or used on a common component with civilian aircraft, the risk amplifies if an incident occurs that relates to this software. For the majority of purposes, this is a low risk to accept.
- Distributor fees. The government is not selling this software as long as it stays within the USG. This risk is very low. However, any sales of software with this statement in the license should be reevaluated (FMS and other types of non-USG sales).
- Laws and statutes outside of U.S. Federal law. Some licenses refer to laws, statutes, and regulations that are outside of Federal law. The USG cannot be bound by any other law than Federal law and any references to jurisdictions outside of U.S. Federal courts cannot be agreed. The risk is very low. The USG must stay within the Federal courts and cannot be overruled.
- Commercial product distribution. These statements discuss the protection of the authors of the software and provide information for settlement negotiations. The USG cannot obligate funds for this event, and lawsuits outside the fiscal year would result in an Anti-Deficiency Act (ADA) violation. The USG cannot enter into this type of agreement. The risk is low for all code staying within the USG.
- Granting access to modified codebases. These statements grant others the right to material located within the confines of our data protection venues. This can also be referred to as “rights of inspection” of either the source code it is included with or the facilities. For any system at or above the FOUO level, this clause is unacceptable. This is a medium risk.
- Defective software requiring the USAF to assume the cost. These statements cannot be accepted by the USAF. A violation of this clause would likely trigger an Anti-Deficiency Act violation. The risk is high.
- Acceptance of the license by its use. The USG cannot enter into an agreement without a signature. A violation of this could trigger the requirement of a contract being put in place between the authors and the USG. The risk is low.

6. Use of OSS falls into four basic use cases. Based on the category, it depends on which licenses can be utilized, and what actions have to be taken when derivative software is delivered.

- OSS is utilized for development support or testing, but is not modified. This is common with a specialty library, such as an encryption library or data manipulation library.
- OSS is utilized for development support or testing, but is modified. This is done by adjusting the OSS to meet a specific environment or purpose. As engineers utilize OSS and identify improvements or adjustments, they can make changes to increase performance or adaptability to the process.
- OSS is packaged with the product, but not modified. This is common with libraries that are not part of a language standard, but are extensions that decrease development time by leveraging already functioning code.
- OSS is packaged with the product and modified to support the requirements. This can happen to adjust an extension to the environment or improve its performance.

7. OSS use should be considered as it can decrease development time and testing. However, programs should carefully consider the licenses associated with each OSS and the potential impacts of the various licenses. In addition, programs should request that developers include associated EULAs with any OSS code utilized.

4.3.2. White Paper on Involving Software Experts in Acquisition Planning

1. Encouraging experienced software engineers to assist with headquarters and PMO activities early in the development life cycle is an important leveraging opportunity. From the outset in the development of an initial request for proposal requirements and sustainment strategies, through depot activation of capabilities, the importance of involving software experts cannot be overstated.

2. As weapon systems become more integrated and dependent on software to execute what was once a mechanical function for most federated aircraft avionic systems, software expertise during the initial planning stages of a modification or new weapon system is a critical component of program success. Most PMOs lack experienced software sustainment personnel who can provide insight into the long-term life-cycle requirements necessary to ensure viable weapon system sustainment. Without this expertise, critical activities necessary to capture the technical baseline, reduce sustainment costs, and prevent vendor lock are often overlooked. By including software personnel early in a program development, items such as special contract requirements, contractor deliverable documents, specially negotiated licenses, contract line items, systems integration and testing approaches, acquisition strategy, sustainment strategy, use of open source licenses, COTS, simulation requirements, and systems integration laboratory development can be reviewed for completeness, thus providing a greater opportunity for success.

3. Source selection is also a critical time for software expertise involvement. Once RFP requirements are established, having the right personnel on hand to evaluate an offeror's proposal can eliminate unnecessary headaches and cost overruns during EMD or Production. Experienced software personnel can provide guidance and insight into the effectiveness of the contractor's proposal and implications. Whether in the area of engine trending/analysis software, commodities test program set software, avionic operational flight program, ground/support software, or use of simulations for risk/cost reduction, the involvement of software expertise provides the program with the opportunity to identify high-risk items and mitigate those risks before the contract is signed.

4. Embedding software expertise with the original equipment manufacturer during EMD is another area that can provide an enormous return on investment. The insight and experience gained by undertaking this seemingly small step facilitates knowledge transfer early in the program, leading to decreased depot activation timelines, reductions in depot activation costs, increased reliability of commodities test program sets, increased sustainability of software solutions, and increased visibility into the technical baseline. The insight of experienced eyes onsite during manufacturing development can also identify potential problems before they become issues.

5. As stated early in this paper, most PMOs lack the software experience to make informed decisions regarding software sustainment. This highlights a need for embedding experienced software engineers in PMOs to assist. PMOs in general lack the manning authorizations to increase staff to compensate for the shortfall of minimal software experience. Therefore it is incumbent upon these PMOs to mitigate the risk through use of either contractor or organic software expertise. In recent years, PMOs have looked to depot complexes to provide the required level of embedded software engineering expertise. The guidance gained through this relationship has proven to be a win-win for those PMOs choosing to participate. They have obtained the experience required without an increase in authorized staffing, while the software groups acquired insight into the modifications or weapon system development required for life-cycle sustainment activities.

6. Through software expertise involvement early in the system life cycle, future weapon systems can achieve recapture of the technical baseline, reduce sustainment costs and prevent vendor lock. In an environment of increasing software reliance, increasing development costs, decreased staffing, and decreased budgets, involvement of experienced software personnel is a critical component for the success of our weapon systems.

4.3.3. White Paper on Common Pitfalls with App Development and Purchasing

1. The increasing use of Government-owned mobile devices (i.e., telephones and tablets) is generating interest in the use of additional software applications (apps) for these devices. The interest can take the form of users desiring to purchase commercially developed apps from third-party app marketplaces (e.g., Apple App Store, Google Play). Users may also express interest in developing custom-written software to serve mission needs. From an acquisition attorney perspective, several contract and fiscal law issues must be considered. However, the purchase or development of apps also implicates other equities, such as software licensing, information technology management, and cybersecurity.

2. When users present mobile app software as a requirement, acquisition attorneys look for streamlined ways to facilitate the acquisition. AFMAN 17-1203 dictates that all Air Force software will be procured using applicable enterprise buying programs, with enterprise license agreements at the Air Force, joint, or DoD level serving as the primary source for software.[1] The same AFMAN provides a catch-all, requiring "all commercial off-the-shelf (COTS) license requirements [to be] purchased using approved DoD/AF Enterprise Licenses Agreements (ELAs), DoD ESI [Enterprise Software Initiative][2] or approved DoD/AF contract vehicles."[3] For desktop and server software, numerous blanket purchase agreements are in place, often based on GSA Federal Supply Schedule contracts. However, there is no enterprise-wide strategy for mobile app acquisitions.

3. App Marketplace Purchases. None of the existing blanket Air Force, joint, or DoD contract vehicles provide for purchases from an app marketplace. One approach to purchasing from an app marketplace could be to use a new or pre-existing contract vehicle to work directly with the software manufacturer, who could then in turn issue a redemption code to retrieve the software from an app marketplace. Another approach could be to use a Government Purchase Card (GPC) to purchase app marketplace credits, which could then be used to purchase the desired software. This acknowledges that the app marketplace is, in fact, a third-party payment processor. The use of GPCs for third-party payment processors is allowed under a 2007 OUSD policy memo.[4] The GPC approach, while subject to the limitations of the micro purchase threshold (currently $5,000 for most situations),[5] could be an effective means to acquire app marketplace software for specific operational needs. O&M funds would be appropriate for use here.

[1] AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*, 18 May 2018, para. 3.2, et seq.

[2] More information about DoD ESI is available at http://www.esi.mil.

[3] AFMAN 17-1203, para. 1.2.8.3.

[4] Office of the Under Secretary of Defense, "Use of Third Party Payments – Policy Change," dated 17 October 2007, http://www.acq.osd.mil/dpap/pdi/pc/docs/10-17-2007_Third_Party_Payments.pdf. "[W]here it is identified that the purchase will be processed via a third party merchant, the cardholder should make every attempt to choose another merchant with whom to procure the goods and/or services. If it is still found necessary to procure using a third party payment merchant, the approving officer must ensure there is adequate supporting documentation showing that there was a detailed review of the purchase and that the use of the third party payment merchant was unavoidable." The original memo predated today's app marketplaces and contemplated purchases via eBay. However, the third-party nature of the app marketplace parallels eBay's model.

[5] See, Office of the Under Secretary of Defense, "Government-wide Commercial Purchase Card Guidance Related to Class Deviation 2017-O0006, Increased Micro-purchase Threshold dated July 13, 2017," dated 21 July 2017, https://www.acq.osd.mil/dpap/policy/policyvault/USA002333-17-DPAP.pdf. See also, DFARS 213.301.

4. App Development Services. Clients seriously seeking to develop custom-written apps in-house are also likely to have that type of software development service on contract already, to have done so successfully in the past, or at least to have utilized a task order against another Air Force or DoD contract vehicle. RDT&E, or a mix of RDT&E and O&M funds could be appropriate for use here. However, it is possible that creative uniformed or civilian employee members of client organizations may possess the skills to develop apps in-house. While this does not present contract or fiscal concerns, the resulting software, like any software, must still be vetted before being installed on Government IT systems.[6]

5. Intellectual Property Concerns. Concerns regarding intellectual property interests abound in this arena, and are substantially beyond the scope of what can be discussed here. A few of the issues include U.S. Government copyright limitations under 17 U.S.C. § 105, Air Force guidance for copyright and trademark,[7] and click-wrap licenses. Click-wrap licenses are of particular note here because the app marketplaces from Apple and Google contain objectionable/unenforceable license terms.[8] AFLCMC's Business Enterprise Systems Directorate is continuing work to resolve these concerns for a consistent solution across the Air Force.

6. Cybersecurity. While cybersecurity is not directly an acquisition concern, it is inextricably interwoven into all software purchases. With hundreds of thousands of apps available on app marketplaces, innumerable threat vectors are possible when installing apps onto Government-owned devices. While Apple and Google do screen for cybersecurity concerns, the Air Force applies higher scrutiny before software can be installed. In practice, this means that software must be vetted and approved before installation. Enterprise-wide software approval is managed by SAF/CIO A6. Consultation with the NAF or MAJCOM A6 or local communications squadron is recommended before purchasing software. The SAF/CIO Cybersecurity Compliance Branch maintains the "Air Force Evaluated Products List (EPL)" of already-approved software.[9] It is useful for the acquisition attorney to highlight cybersecurity vetting and compliance with clients. From the client perspective, it serves no useful purpose to purchase software if the local communications squadron will not allow that software to be installed on computers or mobile devices.

7. Example. Recently, an end-user client presented a requirement for an app to be installed on the iPads carried in the flight bags of pilots on several airframes across a MAJCOM. This app is called GoodReader. It is one of the highest rated PDF apps in the Apple App Store. It can do things with PDF files that the native iPad PDF software cannot, namely, allow the viewing of multiple PDF files simultaneously. Pilots desired the ability to view multiple flight bag documents at once, creating the requirement for GoodReader.

[6] AFMAN 17-1203, para. 3.4.1.

[7] See AFI 51-303, *Intellectual Property*, 22 June 2018, paras. 6 and 7.

[8] This issue of problematic license terms in click-wrap extends beyond just user agreements, through to the programs for software developers themselves (e.g., "Apple App Store Developer Program" and "Apple Development Enterprise Program"). Those programs must be utilized in order to place any developed software onto an app marketplace.

[9] The software certification process is detailed here: https://cs2.eis.af.mil/sites/10007/sc/SitePages/Home.aspx. The Air Force Evaluated Products List of approved software is here: https://cs2.eis.af.mil/sites/10336/Lists/COTSGOTS%20Software/EPL.aspx.

In this case, the end-user client wanted to utilize a GPC to buy this GoodReader app for about 2,000 flight bag iPads, at a total cost of $9,800. The client turned to the GPC because other acquisition vehicles were not available. There are no established enterprise BPAs or other vehicles that would be applicable here. Apple and Google are unwilling to enter into contracts with the Government for utilization of their respective app marketplaces. While use of a GPC is appropriate for purchases under the micro purchase threshold, here the total cost exceeded the threshold, and splitting the purchase to get the amount under the threshold is prohibited. For purchases over the micro purchase threshold, another approach is necessary. This could include contracting directly with the app developer for the purchase amount. The app developer could then in turn provide a redemption code that the end-user client could use to download the app from an app marketplace.

The acquisition attorney can add value to the client by stepping back and asking what is really happening. Here, the end-user client wanted to install new software that is not part of the standard Air Force software build for iPads. In the GoodReader example, the cybersecurity issue takes on added importance because this specific app has a history. In 2012, an Air Force contract for some 21,000 flight bag iPads was cancelled because GoodReader was the PDF viewer application on those iPads. The small software company that makes GoodReader is owned and operated by a Russian national. The 2012 contract cancellation caused quite a stir in the civilian media.[10]
In the GoodReader example, the app eventually was approved—in 2016—to run on Air Force iPads.

[10] *See*, "Air Force Does an About-Face with iPad Order," *The Washington Post*, https://www.washingtonpost.com/business/technology/air-force-does-an-about-face-with-ipad-order/2012/02/23/gIQAOCxMWR_story.html?utm_term=.7e8b1709c378, 23 February 2012; Eric Lai, "Should the U.S. Air Force Kill a 21,000 iPad Deployment Over a PDF Reader?," *Forbes*, https://www.forbes.com/sites/sap/2012/02/23/should-the-u-s-air-force-kill-a-21000-ipad-deployment-over-a-pdf-reader/#2ae94eed7467, 23 February 2012; Bob Brewin, "Air Force Special Operations Cancels iPad Buy," *Nextgov*, https://www.nextgov.com/cio-briefing/2012/02/air-force-special-operations-cancels-ipad-buy/50676, 21 February 2012. Note that GoodMobile (currently in use for email on Government iPhones) and GoodReader (the software at issue here to read PDF files on Government iPads) are not made by the same company. Good Technology, manufacturer of GoodMobile, is a subsidiary of BlackBerry. It has no affiliation with Good.iWare and GoodReader.

Chapter 5 – Battling Vendor Lock

Few issues may be more frustrating to a PMO than trying to overcome “vendor lock”—the situation where the Air Force depends on a single supplier for sustainment support. This chapter details strategies the PMO can use to avoid taking actions early in the life cycle that may result in vendor lock. It also provides some tips that programs in the O&S phase may use to extricate themselves from vendor lock.

5.1. Asserted Restrictions

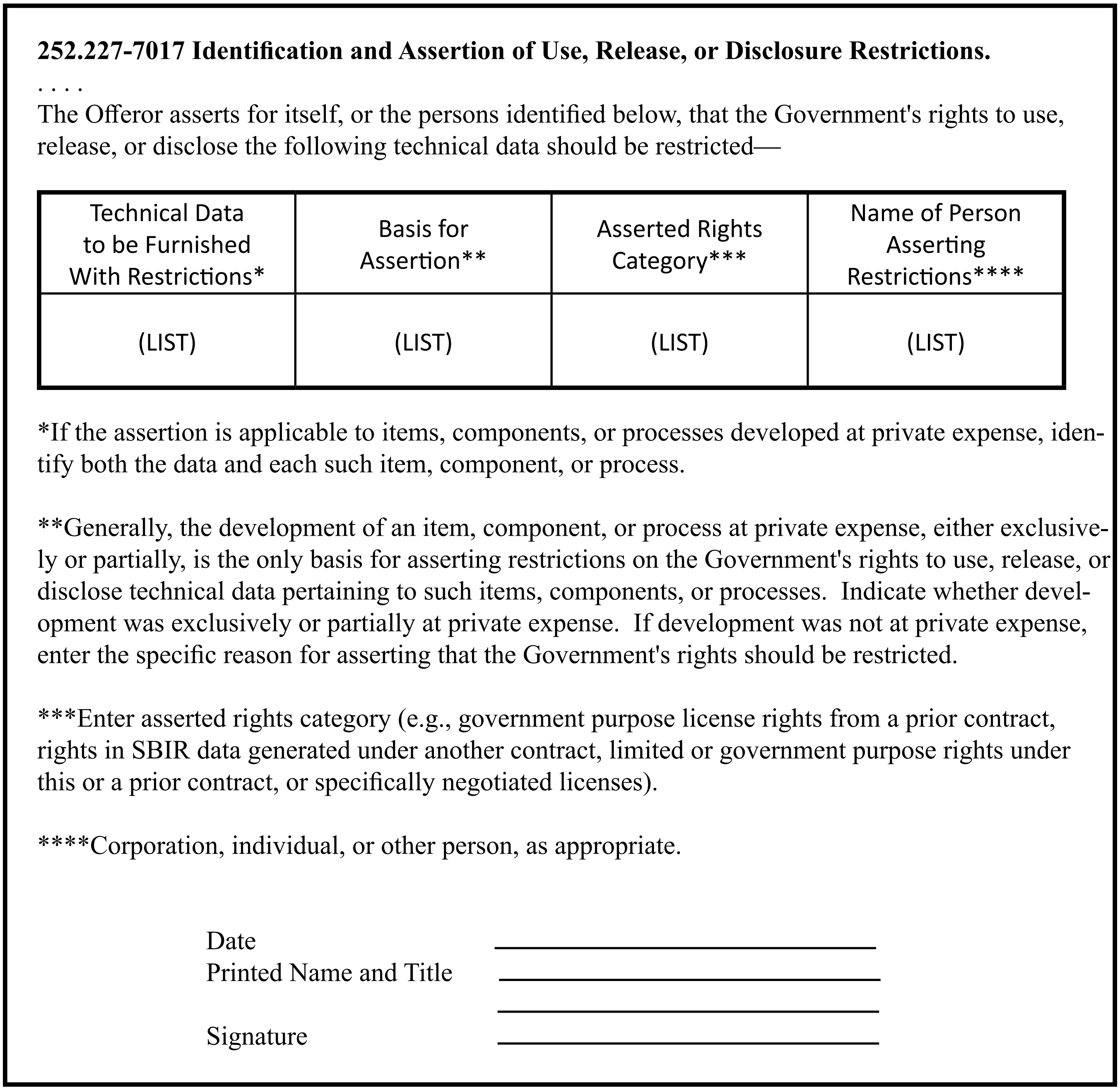
A foundational aspect of the DFARS scheme for managing data and software is the requirement that contractors assert restrictions on data and software to be delivered. These assertions are typically a prerequisite before the Government is obligated to respect any restrictive markings. You will see that concept played out in some of the issues that follow. The format and timing of how assertions are made is carefully prescribed by the DFARS, and abiding by these rules can avoid unnecessary markings and the additional procedures that removing them may require. If there is one issue in data and software acquisition that most often results in vendor lock, it is an overuse of restrictive markings. Limiting them requires deliberate and careful management of the assertions process and a readiness to deal with restrictive markings as they come in.

5.1.1 I know that contractors are responsible for asserting any restrictions on technical data and computer software. How exactly are contractors required to assert those restrictions?

Response

To find the answer, look to DFARS 252.227-7017, which requires offerors to specifically list any asserted restrictions and attach them to their offer. Assertions must be made on any restrictions to technical data or computer software that will be delivered with other than UR. These assertions are made in the form of a table as provided in Figure 16, which is directly from the DFARS:

Figure 16. Sample Assertion Table



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

. . . .

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

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

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

**Generally, the development of an item, component, or process at private expense, either exclusively or partially, is the only basis for asserting restrictions on the Government's rights to use, release, or disclose technical data pertaining to such items, components, or processes. Indicate whether development was exclusively or partially at private expense. If development was not at private expense, enter the specific reason for asserting that the Government's rights should be restricted.

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

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

Date ______________________________
Printed Name and Title ______________________________
____
Signature ______________________________

The assertions table included in the contractor's proposal gives the Government insight into restrictions that the contractor will impose on specific deliverables. It also is a tool for managing restrictive markings applied to individual deliverables. In source selection, the table should be closely scrutinized to determine how any asserted restrictions will affect the Government's ability to use the technical data or computer software internally and how they might affect life-cycle objectives. Since assertions are required to be made at the item/component/process level, the Government should not accept "class" or "group" assertions that are included in the table.

The Strategy

Step 1: DFARS 252.227-7017 language, "Identification and Assertion of Use, Release, or Disclosure Restrictions," should be included in Section L of all RFPs. This information is critical to understanding and evaluating proposed restrictions on the Government's ability to use or disclose delivered technical data or computer software.

Step 2: In general, the contractor may assert something other than UR to data only if the item/component/process to which the data pertains (1) was developed exclusively or partially at private expense or (2) if the Government previously agreed to restrict the data, such as through a special license. The table requires the contractor to make assertions on the technical data to be furnished with restrictions at the item/component/process level.

Step 3: The Government is entitled to UR in certain types of technical data, regardless of who developed it. This includes technical data required for OMIT data, as well as FFF data. This is true for both commercial items and noncommercial items so long as the item is not software. None of this technical data should be included in the assertions table.

5.1.2 How do I use the assertions table during contract administration to preserve the Government's rights and avoid vendor lock? Just because something is asserted to be restricted, does that mean the assertion cannot be challenged or questioned?

Response

You want to use the assertions table in two ways. First, no data or software should be marked restrictively unless the restriction was first asserted in the assertions table. Second, once an assertion is made, the Government must respect it unless the Government decides to challenge it. When an assertion is likely to have life-cycle impacts, such as by leading to vendor lock, the Government should begin scrutinizing it by initially requesting the contractor provide evidence to support the restriction. If the evidence does not satisfy the Government, the restriction may be challenged in accordance with procedures in DFARS 252.227-7019 and/or -7037.

All noncommercial technical data and computer software should be examined when delivered to determine whether they contain restrictive markings, and only restrictions made in the assertions table should be allowed. When a restrictive marking cannot be associated with an assertion, the Government handles the marking according to whether it is unjustified or nonconforming. In this way, Government personnel and other individuals who receive the documents will not be confused as to the Government's rights in the data or software and neither will the Government's rights be unduly limited.

5.1.3. Is there a specific form contractors use when asserting restrictions? What is the assertions table that I hear others talking about?

Response

Contractors may assert restrictions on the Government only by using the format/content prescribed at DFARS 252.227-7013 and/or 7014. This table is *not* to be confused with the Data Accession List, which identifies internal data that has been generated by the contractor in compliance with the work effort described in the SOW.

The assertions table included in the contractor's proposal gives the Government insight about restrictions that the contractor will impose on specific deliverables. The table should be closely scrutinized to determine how any asserted restrictions will affect the Government's ability to use the technical data or computer software internally and to share it with other parties. Since assertions are required to be made at the item/component/process level, the Government should not accept "class" or "group" assertions that are included in the table. The Government should also ensure that OMIT and FFF technical data are not included in the table.

The Strategy

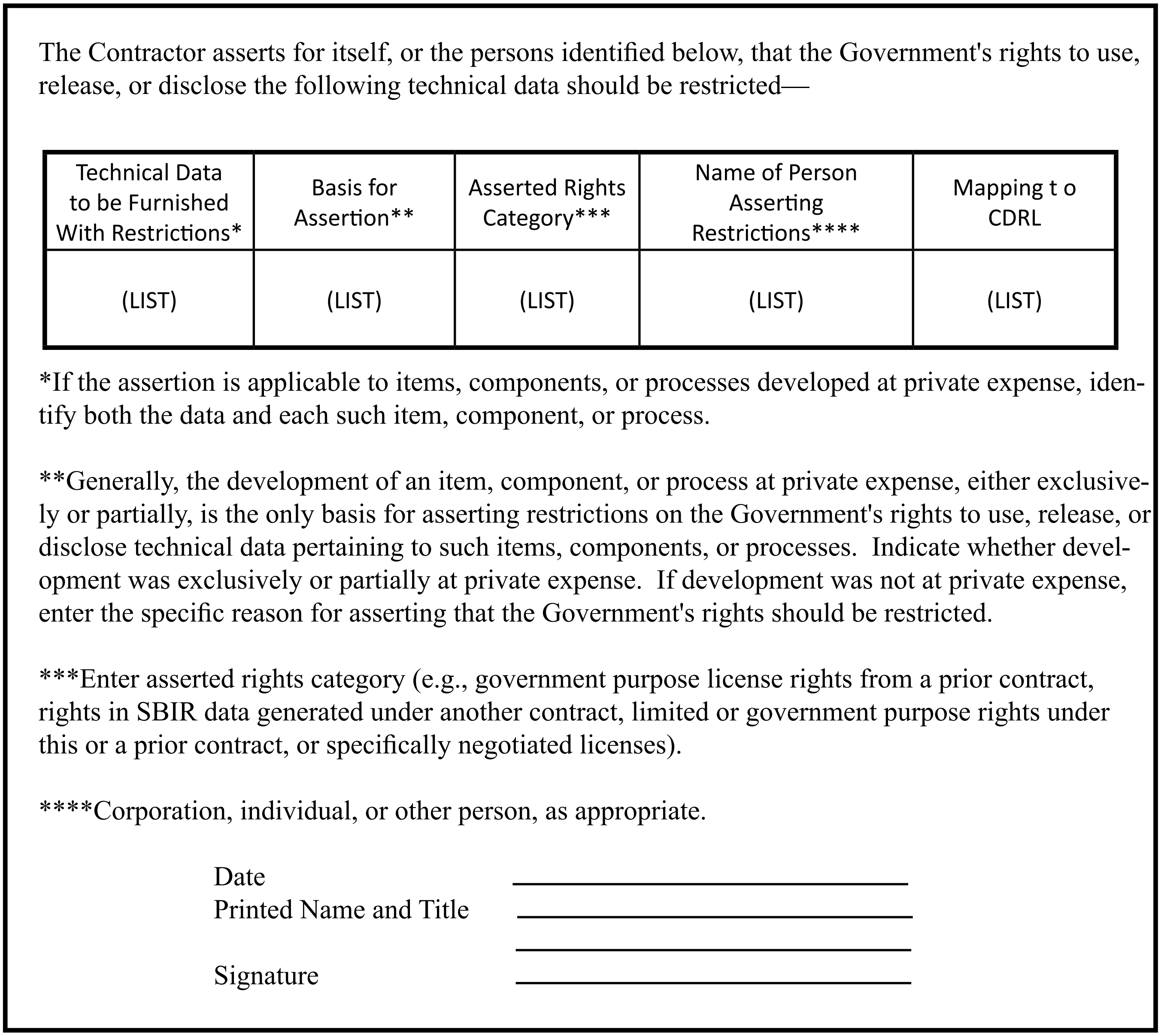
Step 1: In general, the contractor may only assert something other than UR to data if the item/component/process to which the data pertains was developed exclusively or partially at private expense. The table requires the contractor to make assertions on the technical data to be furnished with restrictions at the item/component/process level.

Step 2: The Government is entitled to UR in certain types of technical data, regardless of who developed it. This includes technical data required for OMIT data, as well as FFF data. Other exceptions can be found at DFARS 252.227-7102-1(a). None of this technical data or computer software should be included in the assertions table.

5.1.4. Is there any information that may not be in the assertions table that I should specifically request contractors to include as part of the RFP (e.g., commercial software)?

Response
As a suggested best practice, Figure 17 includes a column titled as "Mapping to CDRL," which provides a cross-reference notation to the CDRL number (e.g., C003) for which the technical data or software will be delivered to the Government with restriction. The CDRL should also have a mapping or cross-reference back to the assertion table (e.g., A003).

Figure 17. Sample Assertion Table with CDRL Mapping



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

Technical Data to be Furnished With Restrictions*	Basis for Assertion**	Asserted Rights Category***	Name of Person Asserting Restrictions****	Mapping t o CDRL
(LIST)	(LIST)	(LIST)	(LIST)	(LIST)

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

**Generally, the development of an item, component, or process at private expense, either exclusively or partially, is the only basis for asserting restrictions on the Government's rights to use, release, or disclose technical data pertaining to such items, components, or processes. Indicate whether development was exclusively or partially at private expense. If development was not at private expense, enter the specific reason for asserting that the Government's rights should be restricted.

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

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

Date ______________________________
Printed Name and Title ______________________________
____
Signature ______________________________

5.1.5. What information should I keep off the assertions table (OMIT, FFF, those not based on a deliverable, etc.)?

Response
Assertion tables should include only technical data and software to be delivered to the Government with "less than" unlimited rights. Thus, OMIT and FFF data should not be included in the table because, by law, the Government is always entitled to unlimited rights in these categories of data.

5.1.6. The contractor is asserting restricted rights in the software source code, but government purpose rights in the object/executable code. Is that proper?

Response
This is not typical but the strategy can most probably be explained as follows. The contractor is attempting to be generous in offering GPR for the software object code, which is of very limited use to third parties who in the future may seek to maintain the software or develop new features to the initial software package. However, by restricting the Government's rights to the software source code, the contractor is significantly reducing the possibility that third parties will be able to maintain, modify, or expand on the initial software package.

5.1.7. The contractor is making other assertions I consider questionable as part of the proposal. Should I challenge them? If I decide not to challenge, how do I preserve the Government's right to challenge them later?

Response
Yes, you can challenge a contractor's assertions documented on an assertion table provided to the Government during the source selection/proposal process. If a decision is made against challenging at the time, the Government may still challenge the same restriction during contract administration and even up to three (3) years after contract close out. Best practice is to put the contractor on "notice" of the disagreement and that the Government may elect to challenge the restriction at a later date.

5.1.8. If I enter into an SNLR license with the contractor, which is placed on the assertions table, can I challenge it later if I decide that that license should not apply?

Response
The answer depends on a number of other factors:

- Is the later challenge based on new information?
- Which party drafted the SNLR?
- Any other relevant licensing factors

In this situation, it is highly advisable to seek the opinion of the PMO attorney or other appropriate legal representative.

5.1.9. After contract award, how are contractors to make new or updated assertions? How should I handle them?

Response
Per DFARS 252.227-7013(e)(3), contractors can make additional assertions of restrictions after contract award as long as the restrictions are based on new information or inadvertent omissions—unless the new assertion of restriction would have materially affected the source selection/procurement decision.

5.1.10. The contractor has provided deliverables with restrictions not on the assertion table. How should I handle these?

Response
Per DFARS 252.227-7013(e)(2), contractors may deliver technical data or software with restrictions only if it is first documented in an assertion table that becomes an attachment to the contract. Thus, if the contractor delivers technical data or software with restrictions “not” first documented in an assertion table, the delivery should be rejected until the restriction is documented and verified.

5.1.11 The contractor is marking other documents with restrictive markings that do not appear in the assertions table. Should I ignore these if they are not formal deliverables?

Response
Do not ignore these markings if the documents constitute technical data or software. Any technical data or software delivered to the Government with less than unlimited rights should be documented in an assertion table before delivery—whether a formal CDRL delivery or not.

5.1.12. I’ve directed the contractor to remove restrictive markings on deliverable and non-deliverable information, yet the contractor has not complied. Is there something I can do to see that the contractor respects the contract?

Response
Restrictive markings fall into two distinct categories: (1) unjustified and (2) nonconforming. Each category is handled differently.

- Unjustified Markings—these restrictive markings follow the correct format/content prescribed in DFARS 252.227-7013, but they are placed on technical data or software in error. The only way to remove these restrictions is with the contractor’s approval or by using the challenge procedures in DFARS 252.227-7019 and/or -7037. Figures 18 and 19 outline the validation timelines based on whether the contractor responds to the government’s challenge.

- Nonconforming Markings—these restrictive markings are not defined in the contract (e.g., proprietary). These markings can be removed by the contractor or the Government by following the procedures in DFARS 252.227-7013(h)(2).

Figure 18. Validation Timeline for Unjustified Markings When the Contractor Responds to Challenge Notice

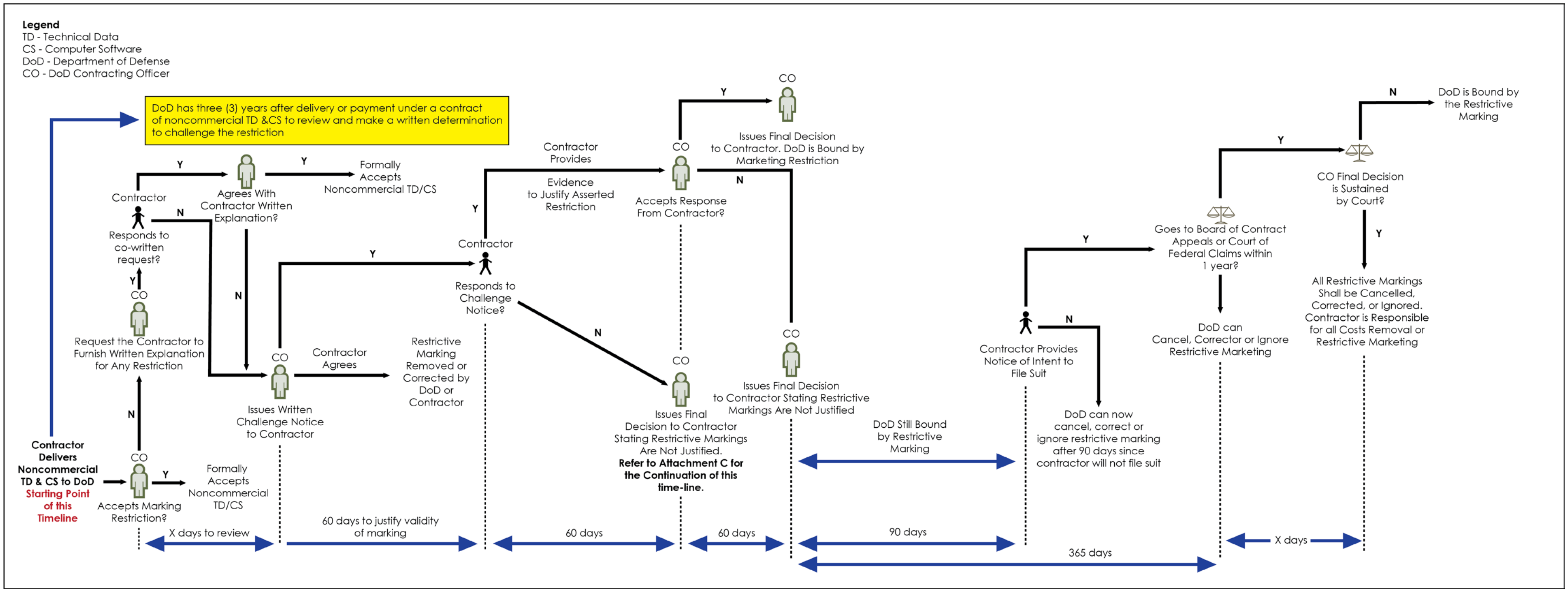
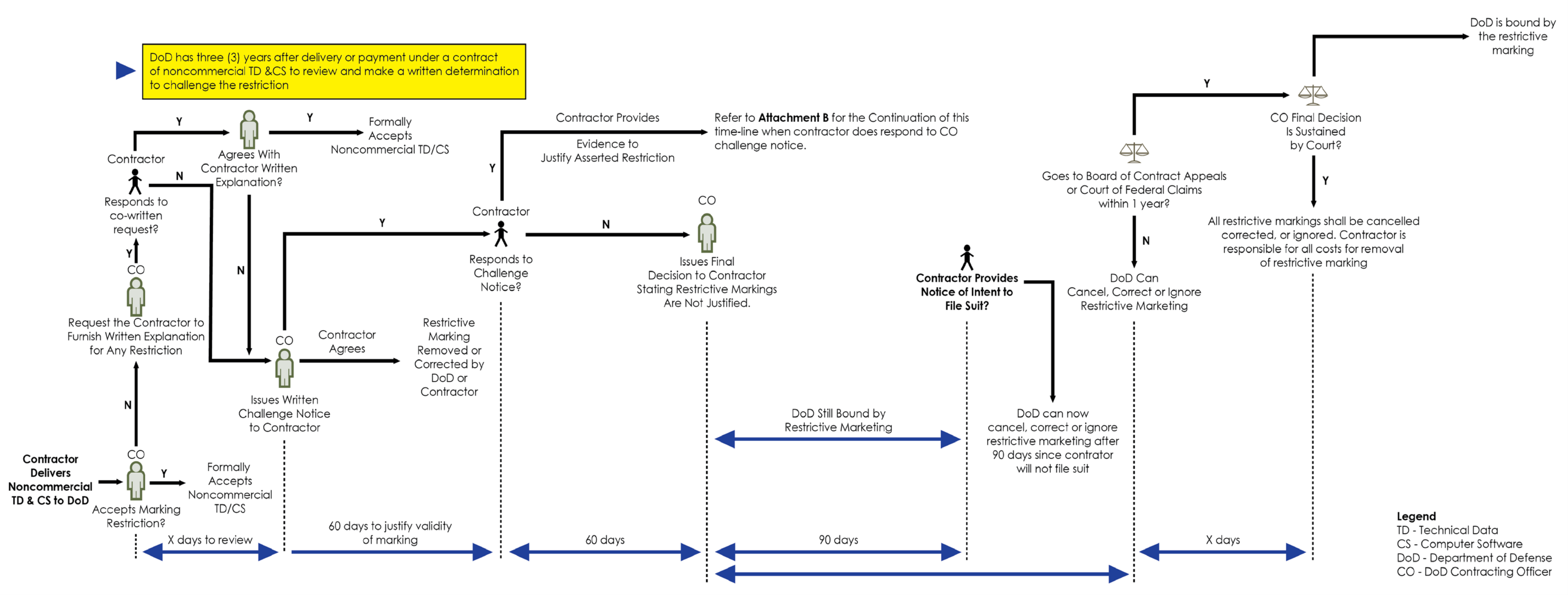

Legend
TD - Technical Data
CS - Computer Software
DoD - Department of Defense
CO - DoD Contracting Officer
DoD has three (3) years after delivery or payment under a contract of noncommercial TD &CS to review and make a written determination to challenge the restriction
Contractor Delivers Noncommercial TD & CS to DoD
Starting Point of this Timeline
CO
Accepts Marking Restriction?
Y
Formally Accepts Noncommercial TD/CS
N
CO
Request the Contractor to Furnish Written Explanation for Any Restriction
Y
Contractor
Responds to co-written request?
Y
Agrees With Contractor Written Explanation?
Y
Formally Accepts Noncommercial TD/CS
N
N
CO
Issues Written Challenge Notice to Contractor
Contractor Agrees
Restrictive Marking Removed or Corrected by DoD or Contractor
Y
Contractor
Responds to Challenge Notice?
Y
Contractor Provides Evidence to Justify Asserted Restriction
CO
Accepts Response From Contractor?
Y
CO
Issues Final Decision to Contractor. DoD is Bound by Marketing Restriction
N
CO
Issues Final Decision to Contractor Stating Restrictive Markings Are Not Justified
N
CO
Issues Final Decision to Contractor Stating Restrictive Markings Are Not Justified.
Refer to Attachment C for the Continuation of this time-line.
DoD Still Bound by Restrictive Marking
Contractor Provides Notice of Intent to File Suit
N
DoD can now cancel, correct or ignore restrictive marking after 90 days since contractor will not file suit
Y
Goes to Board of Contract Appeals or Court of Federal Claims within 1 year?
DoD can Cancel, Correctort or Ignore Restrictive Marketing
Y
CO Final Decision is Sustained by Court?
N
DoD is Bound by the Restrictive Marking
Y
All Restrictive Markings Shall be Cancelled, Corrected, or Ignored. Contractor is Responsible for all Costs Removal or Restrictive Marketing
X days to review
60 days to justify validity of marking
60 days
60 days
90 days
365 days
X days

Figure 19. Validation Timeline for Unjustified Markings When the Contractor Does Not Respond to Challenge Notice on Noncommercial Technical Data


DoD has three (3) years after delivery or payment under a contract of noncommercial TD &CS to review and make a written determination to challenge the restriction
Contractor Delivers Noncommercial TD & CS to DoD
CO
Accepts Marking Restriction?
Y
Formally Accepts Noncommercial TD/CS
N
Request the Contractor to Furnish Written Explanation for Any Restriction
CO
Y
Contractor
Responds to co-written request?
Y
N
Agrees With Contractor Written Explanation?
Y
Formally Accepts Noncommercial TD/CS
N
CO
Issues Written Challenge Notice to Contractor
Contractor Agrees
Restrictive Marking Removed or Corrected by DoD or Contractor
Y
Contractor
Responds to Challenge Notice?
Y
Contractor Provides Evidence to Justify Asserted Restriction
Refer to **Attachment B** for the Continuation of this time-line when contractor does respond to CO challenge notice.
N
CO
Issues Final Decision to Contractor Stating Restrictive Markings Are Not Justified.
DoD Still Bound by Restrictive Marketing
Contractor Provides Notice of Intent to File Suit?
DoD can now cancel, correct or ignore restrictive marketing after 90 days since contrator will not file suit
Goes to Board of Contract Appeals or Court of Federal Claims within 1 year?
N
DoD Can Cancel, Correct or Ignore Restrictive Marketing
Y
CO Final Decision Is Sustained by Court?
Y
All restrictive markings shall be cancelled corrected, or ignored. Contractor is responsible for all costs for removal of restrictive marking
DoD is bound by the restrictive marking
X days to review
60 days to justify validity of marking
60 days
90 days
X days
Legend
TD - Technical Data
CS - Computer Software
DoD - Department of Defense
CO - DoD Contracting Officer

5.1.13. At contract award, the contractor asserted that various aspects of the end item were developed at private expense. Before receiving the deliverables, how is the Government to know whether these assertions are accurate or should be challenged?

Response

Contractors are required to assert, before contract award, whether any technical data or computer software deliverables will be delivered to the Government with less than UR. Though this is the rule, these assertions are hardly ever clear, nor are they binding. Rather, they are subject to validation by the Government. When the assertions cannot be validated by the Government, the assertions no longer control how deliverables should be marked.

The Government cannot challenge every assertion. Many assertions may have little impact on a program's life-cycle objectives, but the Government has to be prepared to challenge assertions when they frustrate the Government's life-cycle needs or some reason exists to suspect the assertions are inaccurate. If the assertions are inaccurate and not challenged, they can severely limit the Government's options over the life cycle.

To know when to challenge an assertion, monitoring contract performance is key. So is adhering to discipline when accepting assertions before contract award. Though challenging assertions at the source selection and formation stages is not always feasible, ensuring those assertions are unambiguous, have a clear basis, and do not infringe on the Government's express requirements is essential. What this means is that assertions should be (1) based on requirements stated in a CDRL or other express requirement, (2) accompanied by a basis that asserts development at private expense, and (3) related to an item, component, or process likely to be used or delivered as part of the contract. The aim is to have items identified in the assertions identified with enough clarity and specificity that they can be related to activities occurring under the contract. When assertions are made in this manner, relating the assertions to contract activities is much easier.

Many management and engineering processes concerning contract performance reveal insightful details about what is occurring with the end item design. When the items making up the end item design can be associated with the items identified in the assertions, it can be relatively straightforward to evaluate the contractor's assertions and to know when to challenge them. For example, much of the information provided for purposes of Earned Value Management (EVM) can be used to uncover how contract funding is being allocated among contract activities, which can be further related to the end item design using other EVM data. When the EVM story does not match what the contractor previously asserted, the time to challenge those assertions is ripe.

Some useful EVM data products include:

- Integrated Master Plan—outlines the development of the end item through the system engineering process in an event-centered fashion. The Integrated Master Plan is useful for putting all contract relationships in one picture.
- Integrated Master Schedule (DI-MGMT-81650)—traces tasks to events found in the Integrated Master Plan and the statement of work to elements of the WBS. The Integrated Master Schedule is useful for highlighting where development activities occur and how they relate to the WBS.
- Contract Work Breakdown Structure (WBS) (DI-MGMT-81334)—specifies hardware and software items associated with each WBS element while also providing cost and purchase explanations for each element. The WBS is useful for highlighting those items being developed rather than purchased. Along with the Integrated Master Schedule and Integrated Master Plan, the WBS can provide a reason to challenge a contractor's prior assertion.
- Contract Funds Status Report (DI-MGMT-81468)—associates contract funds (including appropriation type) with each WBS element.
- Cost/Schedule Status Report (DI-MGMT-81467)—associates cost and schedule information with WBS

elements and includes narratives on significant variances. The Cost/Schedule Status Report is useful for associating contract funds with potential development activities identified from the WBS analysis.
- Integrated Program Management Report (DI-MGMT-81861A)—a collection of EVM data including some of items above.

Relate the contractor's original assertions to the product baseline, such as through a diagram or outline that readily conveys assertions with the baseline. As the product baseline becomes more and more defined, and as contract performance information becomes easier to associate with the baseline, look for inconsistencies to form the basis of a challenge.

The Strategy

Someone in the PMO should be charged with reviewing contractor EVM data and other contract performance information and relating it to the contractor's original assertions. A successful approach could do the following:

Step 1: Begin at the contract formation stage by ensuring all assertions made per DFARS 252.227-7017 are (1) based on requirements stated in a CDRL or other express requirement, (2) accompanied by a basis that asserts development at private expense, and (3) related to an item, component, or process likely to be used or delivered as part of the contract.

Step 2: Take stock of the contract performance information to be provided under the contract. Then, designate one or more persons, or a team, to review this information soon after it is delivered to compare it to the contractor's original assertions.

Step 3: Initiate a challenge under DFARS 252.227-7019, -7037 anytime contract performance information does not match or is otherwise inconsistent with the contractor's original assertions. Use this information throughout the challenge process to assert the Government's interests and to strengthen its bargaining position.

5.2. Restrictive Markings

Any data delivered to the Government with restrictive marking must have the markings verified before acceptance. Taking a structured and rigorous approach to this verification process enables the PMO to identify and address inappropriate markings early in the life cycle. This will avoid potentially lengthy conflicts later on, when restrictive markings may inhibit the program from executing as intended.

5.2.1. My PMO is contemplating a contract under the Small Business Innovation Research (SBIR) Program. What data rights markings should I verify for noncommercial technical data and noncommercial computer software generated under a SBIR award?

Response

When noncommercial technical data or computer software will be generated during performance of contracts under the SBIR program, DoD uses DFARS 252.227-7018, Rights in Noncommercial Technical Data and Computer Software—Small Business Innovation Research (SBIR) Program.

DFARS 252.227-7018 requires the contractor to mark all technical data and computer software that qualify for such markings. "When only portions of a page of printed material are subject to the asserted restrictions, such portions shall be identified by circling, underscoring, with a note, or other appropriate identifier."

When the Government receives data with unjustified or nonconforming markings, Government employees and other recipients may become confused as to the Government's rights.

DoD obtains SBIR data rights in noncommercial technical data and noncommercial computer software generated under an SBIR contract. SBIR data rights provide the Government limited data rights in such noncommercial technical data and restricted data rights in such noncommercial computer software during the SBIR data protection period commencing with contract award and ending five years after completion of the project under which the noncommercial technical data and noncommercial computer software were generated. SBIR data rights apply only during occurrences of Phase I, II, and III SBIR awards. Upon expiration of the protective period, the Government has unlimited data rights in the SBIR noncommercial technical data and noncommercial computer software. For a more descriptive explanation of these phases and how SBIR data rights markings and legends are applied, refer to the Small Business Administration's SBIR tutorials 1 and 2. All marking legends must strictly adhere to the language used in the DFARS clauses, as shown in Figure 20.

The Strategy

Step 1: Inspect all noncommercial technical data and noncommercial computer software delivered to the Government before acceptance of that data.

Step 2: Determine which data contain the correct markings and which do not.

Step 3: For the data with unjustified or nonconforming markings, the Government should seek to have the markings removed before distribution to Government personnel and other individuals.

5.2.2. I work in a PMO, and I just received delivery of drawings from contractor Aircraft–R-Us. One noncommercial technical drawing had two separate data rights marking legends. One marking legend stated "government purpose rights," and the other marking legend stated "limited rights" for a specific item on that drawing. Should that drawing have two separate markings stamped on it, and if so how do I distribute this drawing?

Response

Having two separate marking legends on a noncommercial technical drawing can be correct, assuming, (1) the legends are conforming and justified, and (2) the item listed on the drawing with a limited rights legend is either circled, underscored, with a note, or other appropriate identifier.

This specific drawing can be distributed in several ways depending on the document requirements:

- If you are distributing the whole document, you would have to treat it as subject to the most restricted level of rights contained anywhere in the document. In this case, the drawing would be treated as limited rights (LR). If you treated the drawing as subject to GPR, you are going beyond your license rights as to that portion that is subject to LR.

- In practice, it would depend on the document owner's requirements. If LR are sufficient for the requirement (for example, if you needed to provide the document only to Government employees), you could distribute the whole document. If you needed to distribute it more extensively (for example, if you need to provide the document to other companies/vendors to meet the Government's requirement), it is likely the DoD PMO would redact the portion subject to LR, and then the document could be treated as subject to GPR.

- Another option would be for the DoD PMO to attempt to negotiate a higher level of rights in the portion of the drawing that is subject to LR—to a level that would allow the whole document to be distributed as required (either GPR or SNLR).

5.2.3. I received a technical manual as a deliverable. The contractor marked the bottom of each page "Contractor Proprietary. Do Not Copy or Distribute Without the Written Permission of the Contractor or the Government." There are no other markings on the technical manual. What can I do with the manual? Can I delete or ignore this marking? Do I have to leave the marking on the document and honor it? If I can remove the markings, what can I do with the manual?

Response

Contractors are allowed to place certain markings on technical data and computer software delivered to the Government during performance of a contract. The appropriate markings, however, are very specific, and they depend on the rights the Government has in the data or software and whether the item the data or software relate to is commercial or noncommercial. In order to restrict the Government's rights by marking data or software, the contractor must first inform the Government (generally before contract award) that there will be restrictions by identifying the restrictions in an assertion attached to the contract (see Section 5.1). If the technical data or software is noncommercial and the contractor has provided an assertion for it, the contractor can then mark the document with a legend that is spelled out in the contract clauses that matches the assertion. The marking must, however, strictly follow the language set out in the applicable clauses in the contract. If it does not, it is a nonconforming marking, and the Government should pursue remedies that are also spelled out in the contract that allow the Government to have the contractor remove the marking or, if the contractor does not, to have Government personnel remove the marking. Until the issue is resolved and the contracting officer (CO) directs that a marking can be removed, all Government employees should honor the marking. Refer to Figures 21 and 22 for sample redacted CO letters related to nonconforming markings.

The markings on the technical manual are nonconforming markings (i.e., they are not one of the markings that contractors are allowed to place on technical manuals to limit the Government's use of them). The CO should first request that the contractor remove the entire nonconforming marking. If the contractor refuses to remove the marking or does not respond, the CO can notify the contractor of the nonconforming marking via a formal CO letter. The contractor has 60 days to remove or correct the marking. If the contractor fails to remove the marking, the Government can ignore/correct/remove the marking and may be able to charge the expense of correction or removal to the contractor. Since the contractor has not included an authorized marking on the technical manual that would limit the Government's use, once the nonconforming marking is removed or corrected, you are free to use and copy the document, and you may distribute the document inside or outside the Government (subject to other restrictions, such as export control and classification of course).

The Strategy

Step 1: The Government representative designated to receive deliverables should examine all technical data deliverables (here the technical manual) to make sure they do not contain nonconforming marks. If a deliverable contains a nonconforming marking, the representative should notify the responsible CO and should not distribute the deliverable.

Step 2: All Government representatives that have access to the technical manual should respect the markings until otherwise directed by the CO.

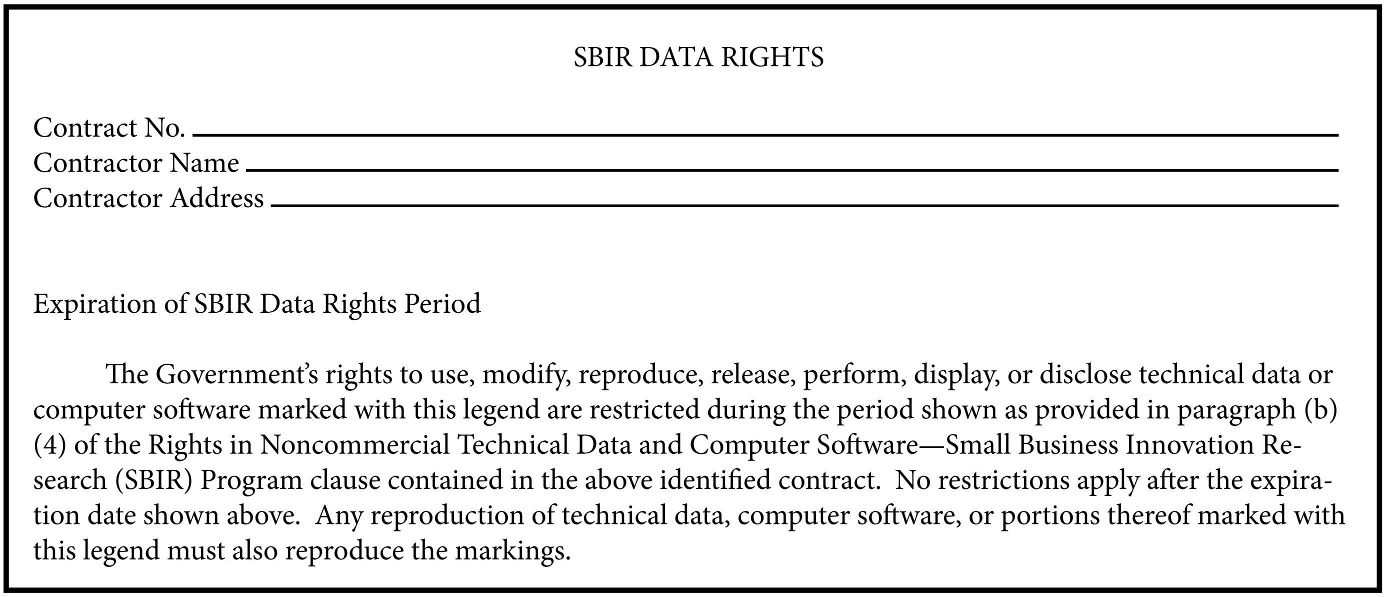
Step 3: After discussions with team members, the CO may request that the contractor correct or remove the nonconforming marking from the technical manual (Figure 21).

Step 4: If the contractor refuses to remove the marking, the CO should send a CO letter formally notifying the contractor of the nonconforming marking on the technical manual and informing the contractor it has 60 days to remove the marking in accordance with the DFARS clauses in the contract (Figure 22).

Step 5: If the contractor fails to remove the marking within 60 days, the CO can direct the removal of the nonconforming marking from the technical manual. The PMO can also discuss whether it would like to seek to recoup from the contractor the cost of removing the marking (an unusual step).

Step 6: Since the contractor failed to mark the technical manual with an authorized marking that restricts the Government's right to use the document, the Government has UR in the document, and it can be freely used (subject to export control, classification, etc.).

Figure 20. Sample of SBIR Data Rights Legend



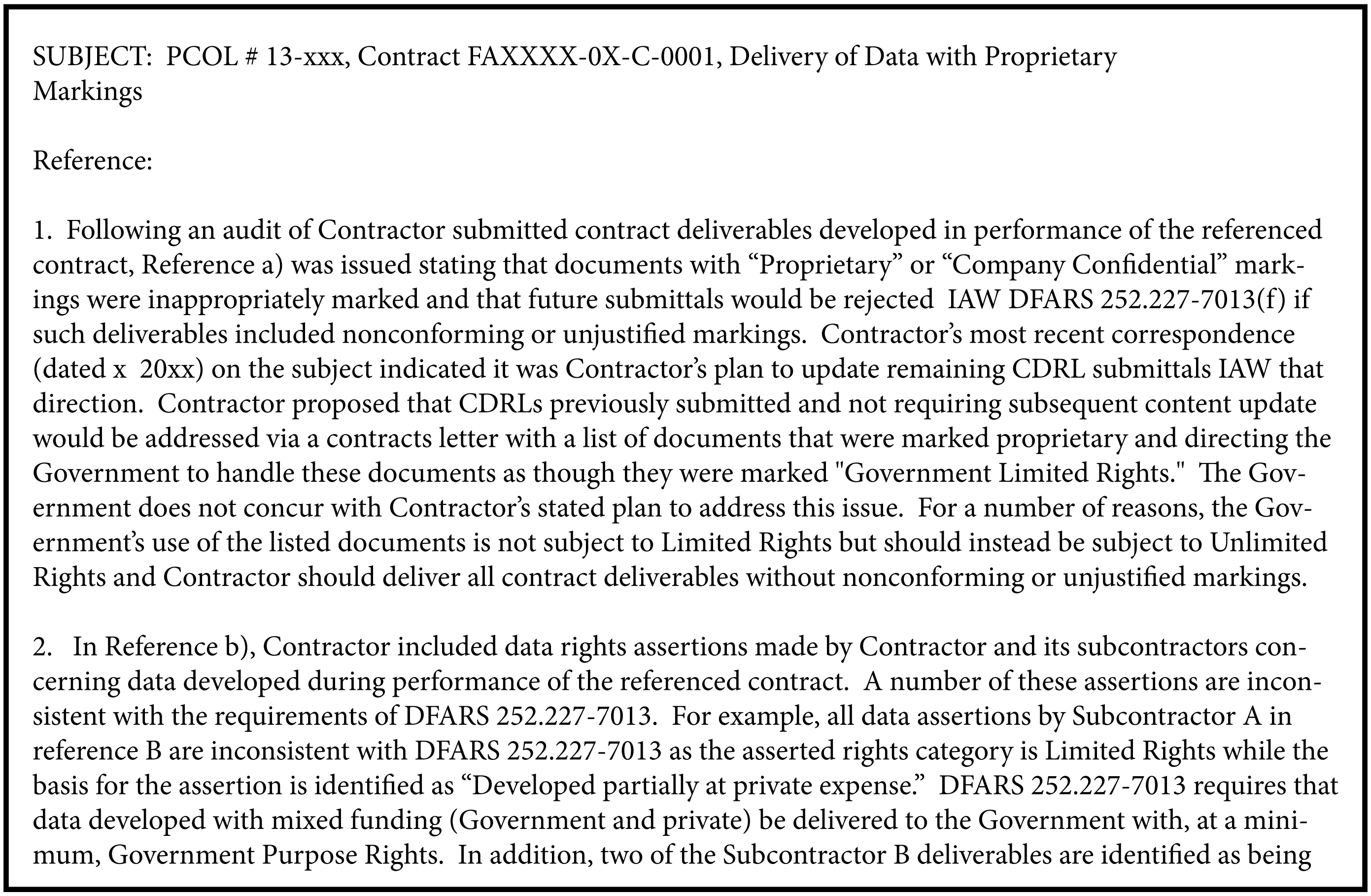
SBIR DATA RIGHTS

Contract No. ______________________________
Contractor Name ______________________________
Contractor Address ______________________________

Expiration of SBIR Data Rights Period

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

Figure 21. Sample Letter 1



SUBJECT: PCOL # 13-xxx, Contract FAXXXX-0X-C-0001, Delivery of Data with Proprietary Markings

Reference:

1. Following an audit of Contractor submitted contract deliverables developed in performance of the referenced contract, Reference a) was issued stating that documents with "Proprietary" or "Company Confidential" markings were inappropriately marked and that future submittals would be rejected IAW DFARS 252.227-7013(f) if such deliverables included nonconforming or unjustified markings. Contractor's most recent correspondence (dated x 20xx) on the subject indicated it was Contractor's plan to update remaining CDRL submittals IAW that direction. Contractor proposed that CDRLs previously submitted and not requiring subsequent content update would be addressed via a contracts letter with a list of documents that were marked proprietary and directing the Government to handle these documents as though they were marked "Government Limited Rights." The Government does not concur with Contractor's stated plan to address this issue. For a number of reasons, the Government's use of the listed documents is not subject to Limited Rights but should instead be subject to Unlimited Rights and Contractor should deliver all contract deliverables without nonconforming or unjustified markings.

2. In Reference b), Contractor included data rights assertions made by Contractor and its subcontractors concerning data developed during performance of the referenced contract. A number of these assertions are inconsistent with the requirements of DFARS 252.227-7013. For example, all data assertions by Subcontractor A in reference B are inconsistent with DFARS 252.227-7013 as the asserted rights category is Limited Rights while the basis for the assertion is identified as "Developed partially at private expense." DFARS 252.227-7013 requires that data developed with mixed funding (Government and private) be delivered to the Government with, at a minimum, Government Purpose Rights. In addition, two of the Subcontractor B deliverables are identified as being

provided with Limited Rights while the basis for the assertion was "Partially Developed at Private Expense." As set forth above, these deliverables also should be provided with, at a minimum, Government Purpose Rights.
3. The Government does not concur with Contractor's proposed plan to address this issue for the additional reason that the Government does not agree that all of the previously delivered documents that were marked with nonconforming Proprietary or Confidential markings are subject to Limited Rights. Instead some of those previously delivered documents are subject to Unlimited Rights. For example, the Configuration Management Plan (CMP), which is included in the documents that Contractor proposes be treated as subject to Limited Rights, was initially submitted in 200x without any restrictive markings. While the subsequent Revision 1 submission included a "Proprietary" marking, all subsequent revisions (2 through 6) were not marked as "Proprietary" and did not contain any conforming
restrictive markings as required by DFARS 252.227-7013. Pursuant to DFARS 227-7103-10(c), technical data delivered without restrictive markings is presumed to be delivered with Unlimited Rights.

Consequently, Limited Rights is an unjustified marking for the CMP or any other deliverable
previously delivered to the Government without conforming markings (i.e. Limited Rights, Government Purpose Rights, Special License Rights, etc.).

4. These apparent inconsistencies and incorrect data rights assertions are noted in advance of your final CDRL submissions. Please ensure that any data rights marking on all contract deliverables delivered to the Government are correct, in compliance with DFARS clause requirements and can be adequately justified. As stated in Reference a), any contract deliverables with nonconforming or unjustified markings will be rejected. Further, outstanding data rights issues may delay the acceptance of CLINS 100x, 100x and/or 100x pending resolution of these issues.

5. Contractual questions or correspondence should be directed to xxx.

Figure 22. Sample Letter 2

SUBJECT: Notice of Non-Conforming Markings on CDRL Deliverables for Contract FAXXXX-XX-C-XXXX, (PCOL 1X-000X)

1. The Government received CRDL A0XX containing drawings on [x 20xx].

2. The Government's review revealed that the drawings contained nonconforming markings.

a. The drawings are stamped with a proprietary marking.

NOTICE: The data in this document incorporates proprietary rights of CONTRACTOR. Any party accepting this document does so in confidence and agrees that it shall not be duplicated in whole or in part, without the written consent of CONTRACTOR.

3. The markings at issue are not authorized markings under DFARS 252.227-7013 and, therefore, are nonconforming markings in accordance with DFARS 227.7103-12.

4. Per DFARS 227.7103-12(a)(2), the Government is providing Contractor the opportunity to correct the nonconforming markings and return CDRL A0XX deliverable no later than [x 20xx]. If Contractor fails to correct the markings and redeliver the documents by [x 20xx], the Government will correct or strike the nonconforming markings at Contractor's expense.

5. The Government will address other data rights issues concerning other CRDL deliverables in a separate letter. If there are any questions, please contact the undersigned at

5.2.4. Is there a standard process to review IP markings on all noncommercial technical data and computer software before the Contracting Officer formally accepts the data?

Response

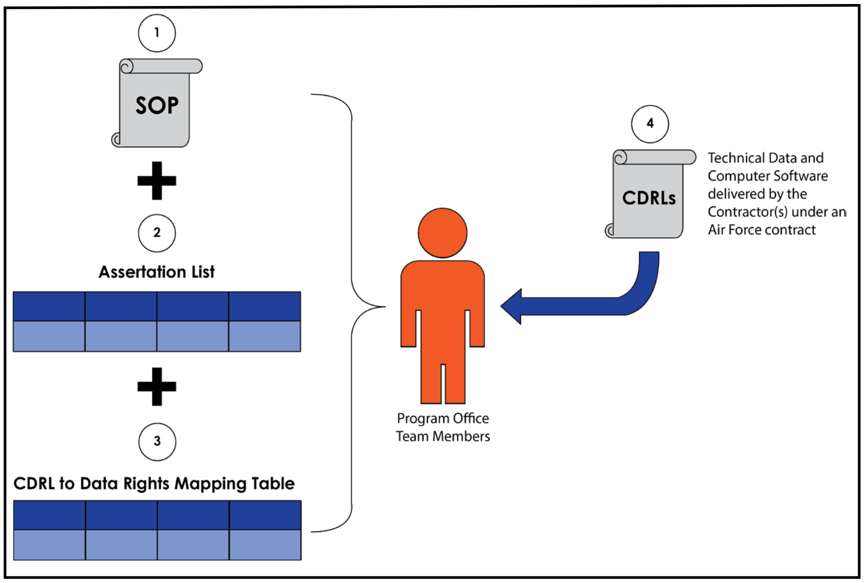
The Air Force has some leverage to have a contractor delete nonconforming/unjustified markings affixed to noncommercial technical data and computer software prior to formally accepting the data. Therefore, the Air Force must ensure the markings on all data delivered are correct and reflect the Air Force's rights in the data prior to accepting that data.

Do not assume all the data markings from the contractor(s) are correct. The PMO should verify all data markings to ensure they are 100% consistent with the contractual requirements. The Air Force has remedies in the contract to address nonconforming and unjustified markings, but the earlier the issue is addressed the more likely it is that less time and resources will have to be devoted to it. A team of individuals within the PMO should be assigned the responsibility to validate markings on all data before it is formally accepted. If the team needs training, DAU CLM 076 is a great place to start.

The Strategy

Step 1: The PMO reviewers collect copies of the following documents before starting the process of verifying the markings on all data. Refer to Figure 23.

Figure 23. Documents for Marking Verification


1
SOP
2
Assertion List
3
CDRL to Data Rights Mapping Table
4
CDRLs
Technical Data and Computer Software delivered by the Contractor(s) under an Air Force contract
Program Office Team Members

a. An SOP document that explains how to verify IP rights markings affixed to data delivered to the government.

b. Assertion List. The Assertion List in concert with the appropriate DFARS clauses for noncommercial technical data and computer software obligates the contractor to comply with three critical contract procedures to restrict the government's use of delivered data: asserting, marking, and justifying. These procedures force the contractor to clarify its positions on the government's rights in the data to be delivered to the government under the contract and should be used to highlight any areas of disagreement between the parties. The DFARS requires that the contractor make a proper assertion identifying all data to be delivered with less than UR before award. The assertions must be included in the offeror's proposal (and incorporated into the contract) or made before delivery (and justified as a "new" assertions or assertions based upon an "inadvertent omission" not affecting source selection). Refer to Table 3 for a fictitious Assertion List completed by the offeror.

c. Data Rights Pricing/Mapping Tables (not included in all Air Force contracts). The PMO should develop this table (or similar) prior to releasing the RFP and later attach it to the contract. An example is shown in Table 4.

d. All contractual CDRLs delivered to the PMO.

Table 3. Fictitious Example of an Assertion List Table

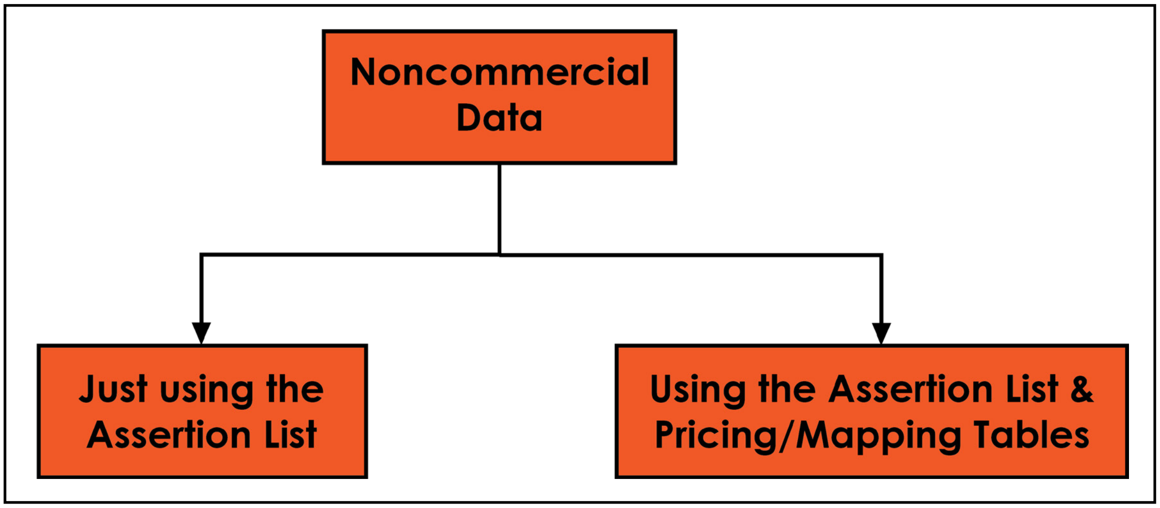
Technical Data or Computer Software to be Furnished with Restrictions	Basis for Assertion	Asserted Right Category	Name of Person Asserting Restrictions
Radiation detector, 3D design as record in drawing No. 123-4433, dated 4 Sept 2018	Developed exclusively at private expense	Limited Rights	HI Robotics Inc, (32827)

Table 4. Fictitious Data Rights Pricing/Mapping Table for Noncommercial Technical Data and Computer Software

Column 1	Column 2	Column 3	Column 4
CDRL Number	Data Item Title (DID Title & Name)	Asserted Rights Category	License Price or Estimated Cost
A001	DI-NDTI-80603A Test Procedures	Unlimited	
A002	DI-XXX	Unlimited	
A003	DI-XXX	Government Purpose Rights	

Step 2. The reviewers, based on the documents provided above, begin the process of comparing the marking affixed to a CDRL to either the Assertion List (Table 3) or to the Data Right Price/Mapping Table (Table 4) for any inconsistencies. Figure 24 provides a potential path the reviewers can take. Step 3 provides the marking/legend verification process when only using an Assertion List. Step 4 provides the marking/legend verification process if using the Data Rights Pricing Table/Mapping Table.

Figure 24. Review Process

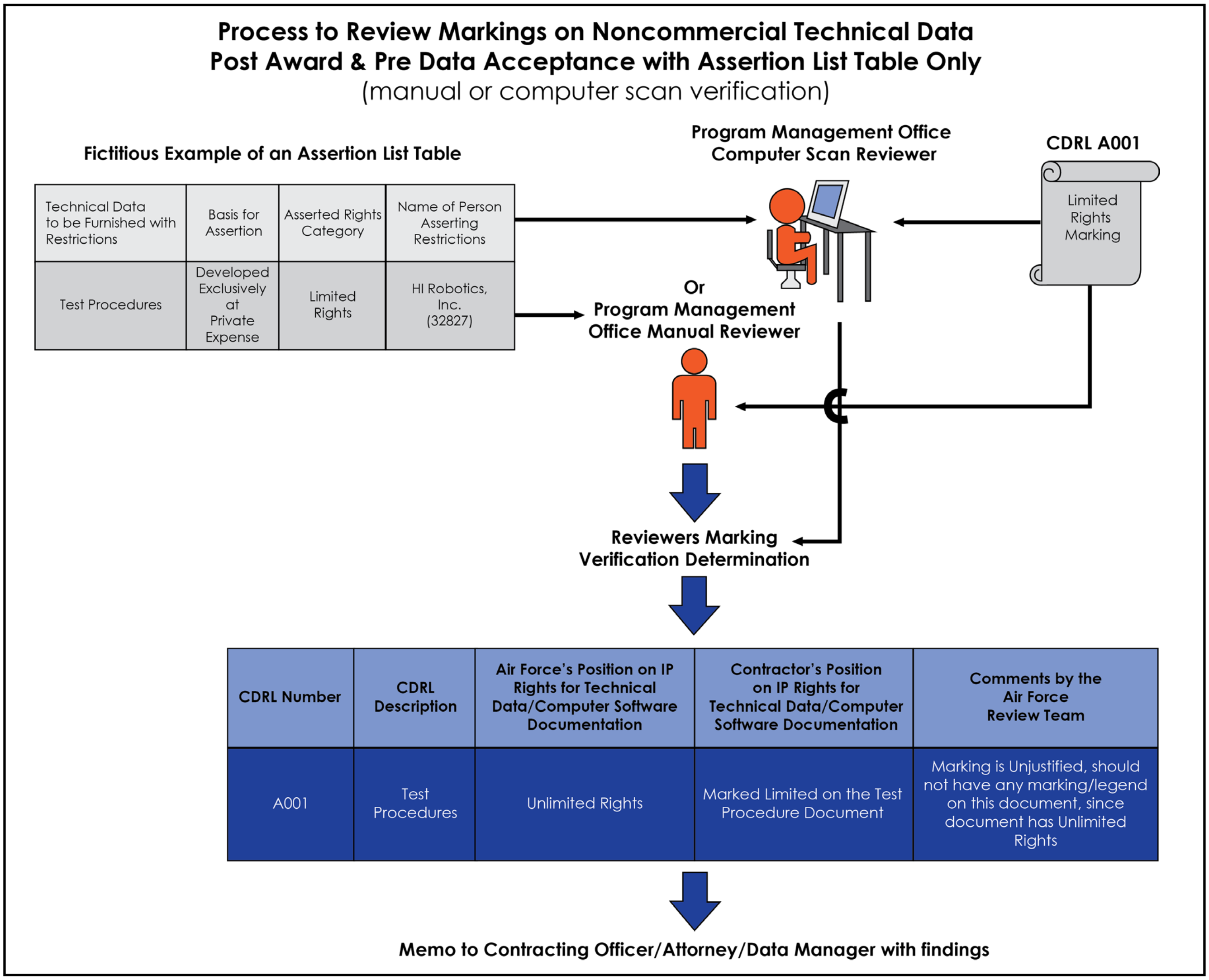

Noncommercial Data
Just using the Assertion List
Using the Assertion List & Pricing/Mapping Tables

Step 3. Figure 25 provides a notional graphical process to verify markings on noncommercial technical data using only the Assertion List Table. The timeline for this review is post award and before any data acceptance by the Contracting Officer. This process can either be accomplished by scanning (automatic) or by manual review of all the data. The process is as follows:

a. Reviewers read the Marking Verification SOP document to understand and therefore ensure all procedures are followed correctly;
b. The Contracting Officer provides the Assertion List to all reviewers;
c. The CDRLs are given to the reviewers either in hard or soft copy;
d. The reviewers compare (computer scan or manually) the Assertion List rights category to the marking affixed to the data. Review all data for nonconforming or unjustified markings (see Section 5.1.12).
e. All findings are presented in a Word document to the Contracting Officer/Attorney/Data Manager.

Figure 26 provides a notional graphical process to verify markings on noncommercial computer software using only the Assertion List Table. For noncommercial computer software, the team should scan every source line of code to ensure no nonconforming or unjustified markings are contained therein. Reviewers should research whether automated tools may be available to facilitate this review. The timeline for this review is post award and prior to the Contracting Officer/Contracting Officer Representative formally accepting any data. The PMO would implement similar processes to verify the markings as noted in Step 2 above.

Figure 25. Process to Review Markings on Noncommercial Technical Data Post Award and Pre Data Acceptance with Assertion List Table Only



Process to Review Markings on Noncommercial Technical Data
Post Award & Pre Data Acceptance with Assertion List Table Only
(manual or computer scan verification)

Fictitious Example of an Assertion List Table

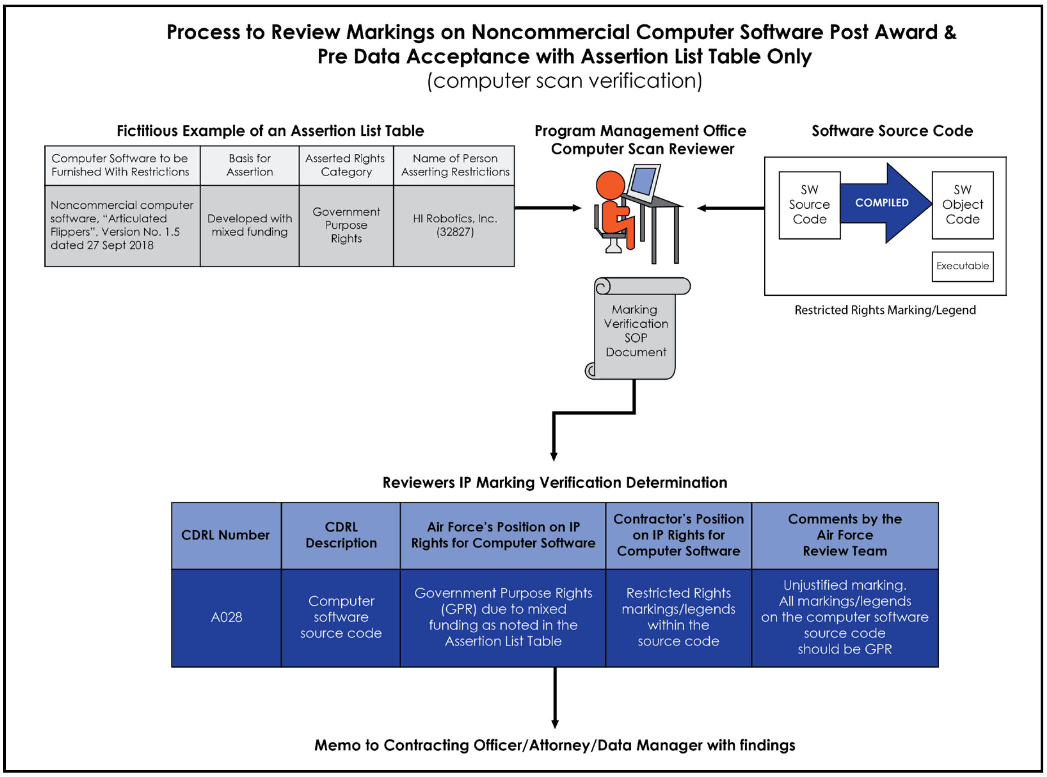
Technical Data to be Furnished with Restrictions	Basis for Assertion	Asserted Rights Category	Name of Person Asserting Restrictions
Test Procedures	Developed Exclusively at Private Expense	Limited Rights	HI Robotics, Inc. (32827)

Program Management Office Computer Scan Reviewer
CDRL A001
Limited Rights Marking
Or
Program Management Office Manual Reviewer
Reviewers Marking Verification Determination

CDRL Number	CDRL Description	Air Force's Position on IP Rights for Technical Data/Computer Software Documentation	Contractor's Position on IP Rights for Technical Data/Computer Software Documentation	Comments by the Air Force Review Team
A001	Test Procedures	Unlimited Rights	Marked Limited on the Test Procedure Document	Marking is Unjustified, should not have any marking/legend on this document, since document has Unlimited Rights

Memo to Contracting Officer/Attorney/Data Manager with findings

Figure 26. Process to Review Markings on Noncommercial Computer Software Post Award and Pre Data Acceptance with Assertion List Table Only



Process to Review Markings on Noncommercial Computer Software Post Award & Pre Data Acceptance with Assertion List Table Only
(computer scan verification)

Fictitious Example of an Assertion List Table

Computer Software to be Furnished With Restrictions	Basis for Assertion	Asserted Rights Category	Name of Person Asserting Restrictions
Noncommercial computer software, “Articulated Flippers”, Version No. 1.5 dated 27 Sept 2018	Developed with mixed funding	Government Purpose Rights	HI Robotics, Inc. (32827)

Program Management Office Computer Scan Reviewer
Software Source Code
SW Source Code
COMPILED
SW Object Code
Executable
Restricted Rights Marking/Legend
Marking Verification SOP Document

Reviewers IP Marking Verification Determination

CDRL Number	CDRL Description	Air Force's Position on IP Rights for Computer Software	Contractor's Position on IP Rights for Computer Software	Comments by the Air Force Review Team
A028	Computer software source code	Government Purpose Rights (GPR) due to mixed funding as noted in the Assertion List Table	Restricted Rights markings/legends within the source code	Unjustified marking. All markings/legends on the computer software source code should be GPR

Memo to Contracting Officer/Attorney/Data Manager with findings

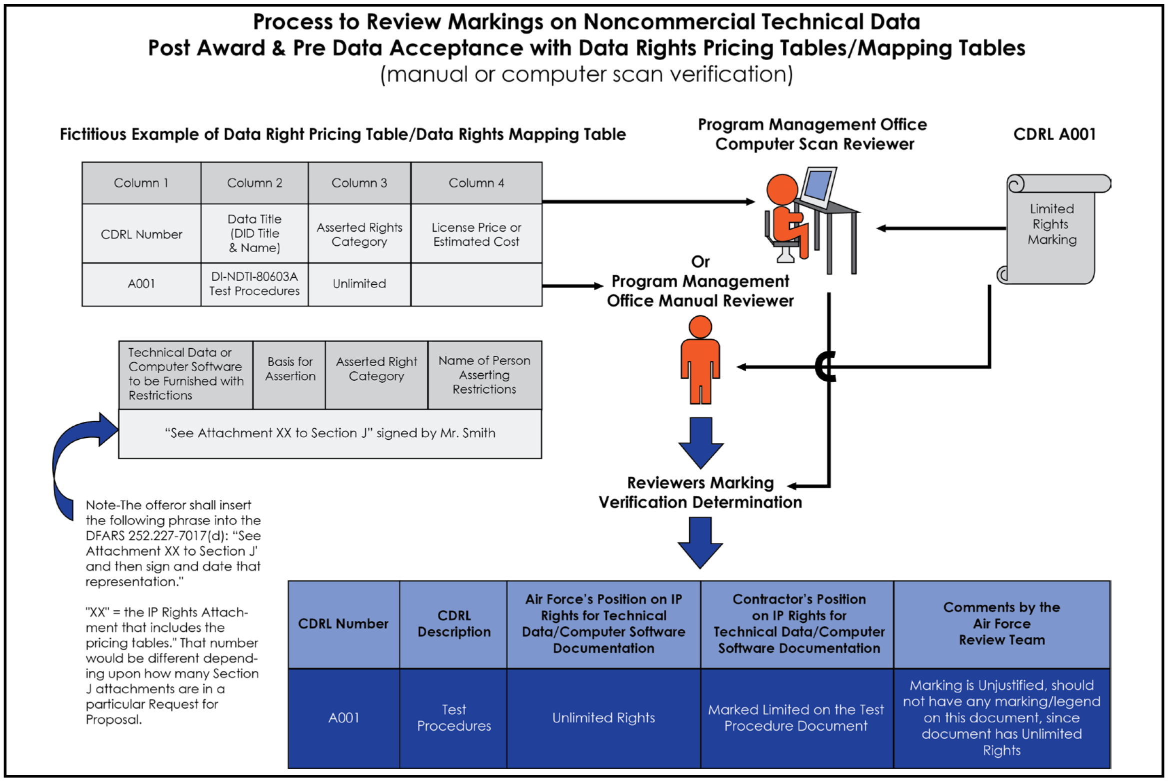
As identified in Figure 26, the Contractor did not properly affix the correct marking on the computer software source code (it is an unjustified marking). The computer software source code must match the Assertion List, which stated the source code would be delivered to the government with GPR. If the PMO had not implemented this marking-verifying process, the Air Force would have accepted this computer software source code (i.e., signed the DD250) with restricted rights. And that would mean the Air Force could never compete maintenance of that source code.

Once the reviewers have completed this process, they send a consolidated memo to the Contracting Officer listing all their findings and discrepancies. The Contracting Officer and attorney inform the contractor of the discrepancies and work with them to resolve all marking discrepancies. Once those discrepancies have been corrected, the Contracting Officer/Contracting Officer Representative signs the DD Form 250 (or equivalent) signifying final acceptance of the data.

Step 4. When using the Data Rights Pricing/Mapping Tables to verify the markings on noncommercial technical data, the Assertion Table will not be utilized. The notional process for this marking verification/validation is depicted in Figure 27, and is as follows:

- The Contracting Officer notes in Section L of the RFP, “The offeror shall insert the following phrase into the DFARS 252.227-7017(d): “See Attachment X [“X” = the IP Rights Section J Attachment that includes the Data Rights Pricing Tables/Mapping Tables; that number would be different depending upon how many Section J attachments are in a particular Request for Proposal] to Section J and then sign and date that representation.” This approach prevents the creation of any inconsistencies between the Assertion List and the Data Rights Pricing Table/Mapping Table;
- The Contracting Officer provides the Data Rights Pricing Table/Mapping Table to all the team reviewers;
- Each reviewer is provided the specific CDRLs for their review;
- The reviewer (either by a computer scan or manual scan) reviews the marking/legend on the CDRL deliverable, and ensures it matches the IP rights listed in the Data Right Pricing Table/Mapping Table. Review all Data for nonconforming or unjustified markings (See Section 5.1.12.).
- Each reviewer documents their findings and submits a report to the Contracting Officer/Attorney/Data Manager.

Figure 27. Process to Review Markings on Noncommercial Technical Data Post Award and Pre Data Acceptance with Data Rights Pricing Tables/Mapping Tables (manual or computer scan verification)



Process to Review Markings on Noncommercial Technical Data
Post Award & Pre Data Acceptance with Data Rights Pricing Tables/Mapping Tables
(manual or computer scan verification)

Fictitious Example of Data Right Pricing Table/Data Rights Mapping Table

Column 1	Column 2	Column 3	Column 4
CDRL Number	Data Title (DID Title & Name)	Asserted Rights Category	License Price or Estimated Cost
A001	DI-NDTI-80603A Test Procedures	Unlimited	

Technical Data or Computer Software to be Furnished with Restrictions	Basis for Assertion	Asserted Right Category	Name of Person Asserting Restrictions
“See Attachment XX to Section J” signed by Mr. Smith			

Note-The offeror shall insert the following phrase into the DFARS 252.227-7017(d): “See Attachment XX to Section J' and then sign and date that representation.”

"XX" = the IP Rights Attachment that includes the pricing tables." That number would be different depending upon how many Section J attachments are in a particular Request for Proposal.

Program Management Office
Computer Scan Reviewer
CDRL A001
Limited Rights Marking
Or
Program Management Office Manual Reviewer
Reviewers Marking Verification Determination

CDRL Number	CDRL Description	Air Force's Position on IP Rights for Technical Data/Computer Software Documentation	Contractor's Position on IP Rights for Technical Data/Computer Software Documentation	Comments by the Air Force Review Team
A001	Test Procedures	Unlimited Rights	Marked Limited on the Test Procedure Document	Marking is Unjustified, should not have any marking/legend on this document, since document has Unlimited Rights

As shown in Figure 27, the reviewer noted that CDRL A001 (Test Procedures) should not have any marking affixed to it because the contractor agreed prior to award that the government would acquire UR to all content delivered pursuant to that CDRL; nevertheless, the contractor has attempted to restrict the government's ability to use, release, and disclose that CDRL outside the government by affixing an LR restrictive marking to that document. This is an example of an unjustified marking. The reviewer created the IP Marking Verification Determination table as shown in Figure 27 and submitted the findings via a report to the Contacting Officer, Attorney and Data Manager.

When using the Data Rights Pricing/Mapping Tables to verify/validate the markings on noncommercial computer software source code the Assertion Table will not be utilized. The notional process for this marking verification/validation is depicted in Figure 28, and the following steps are:

a. The Contracting Officer notes in Section L of the Request for Proposal, “The offeror shall insert the following phrase into the DFARS 252.227-7017(d): “See Attachment X [where “X” = the IP Rights Attachment that includes the Data Rights Pricing Tables/Mapping Tables; that number would be different depending upon how many Section J attachments are in a particular Request for Proposal] to Section J and then sign and date that representation.” This prevents any discrepancies between the Assertion List and the Data Rights Pricing Table/Mapping Table;

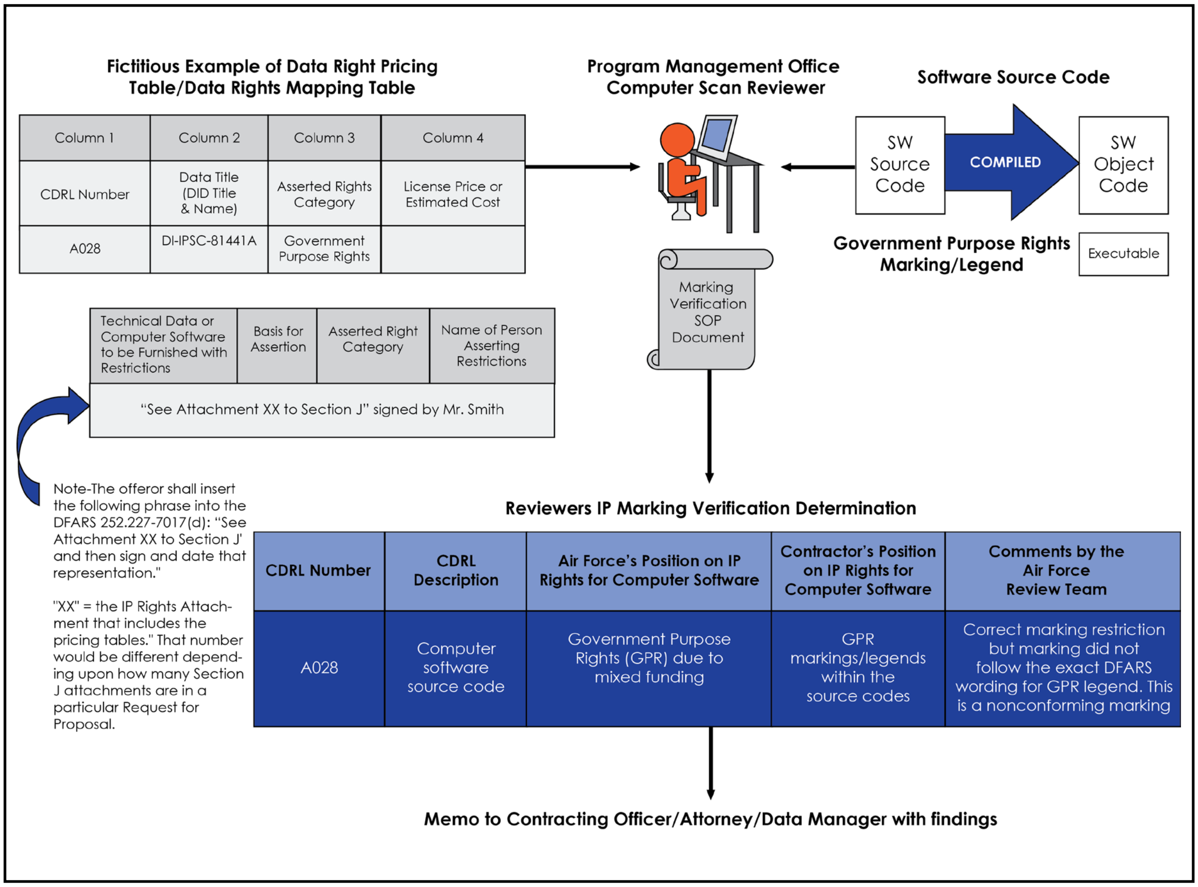
b. The Contracting Officer provides the Data Rights Pricing Table/Mapping Table to all the team reviewers;

c. Each reviewer is provided the specific CDRLs for their review;

d. The reviewer (computer scan only, cannot be done manually) scans all the source code. The computer scan should print out all the markings on the computer source code so the reviewer can match the marking(s) to the IP rights listed in the Data Right Pricing Table/Mapping Table (Column 3). Review all data for nonconforming or unjustified markings.

e. Each reviewer documents their findings and submits a report to the Contracting Officer/Attorney/Data Manager.

Figure 28. Process to Review Markings on Noncommercial Computer Software Post Award and Pre Data Acceptance with Data Rights Pricing/Mapping Tables Only



Fictitious Example of Data Right Pricing Table/Data Rights Mapping Table
Program Management Office Computer Scan Reviewer
Software Source Code
SW Source Code
COMPILED
SW Object Code
Government Purpose Rights Marking/Legend
Executable
Marking Verification SOP Document
Reviewers IP Marking Verification Determination
Memo to Contracting Officer/Attorney/Data Manager with findings

Column 1	Column 2	Column 3	Column 4
CDRL Number	Data Title (DID Title & Name)	Asserted Rights Category	License Price or Estimated Cost
A028	DI-IPSC-81441A	Government Purpose Rights	

Technical Data or Computer Software to be Furnished with Restrictions	Basis for Assertion	Asserted Right Category	Name of Person Asserting Restrictions
"See Attachment XX to Section J" signed by Mr. Smith			

Note-The offeror shall insert the following phrase into the DFARS 252.227-7017(d): "See Attachment XX to Section J' and then sign and date that representation."

"XX" = the IP Rights Attachment that includes the pricing tables." That number would be different depending upon how many Section J attachments are in a particular Request for Proposal.

CDRL Number	CDRL Description	Air Force's Position on IP Rights for Computer Software	Contractor's Position on IP Rights for Computer Software	Comments by the Air Force Review Team
A028	Computer software source code	Government Purpose Rights (GPR) due to mixed funding	GPR markings/legends within the source codes	Correct marking restriction but marking did not follow the exact DFARS wording for GPR legend. This is a nonconforming marking

As shown in Figure 28, the reviewer noted that CDRL A028 (computer software source code) had the correct marking/legend, but the contractor did not follow the GPR marking required by the DFARS. This is an example of a nonconforming marking. The reviewer created the table as shown in Figure 28 and submitted the findings via a report to the Contacting Officer, Attorney and Data Manager.

5.3. Other Ideas for Addressing Vendor Lock

5.3.1. What do I do when I need IP and either don't have the appropriate rights (i.e., UR or GPR) or don't have the data at all?

Response

AF programs will encounter numerous challenges over their life cycle requiring government license rights of contractor-created technical data, commonly referred to as "technical data rights." These challenges include increasing costs, sustainment strategy changes, obsolescent parts, and system improvements in order to preserve operational availability and maintainability. Organizations tasked with sustaining a program, such as cognizant PMOs and supply chain organizations are impacted the most by this. The best time in a program's life cycle to acquire technical data rights is when negotiating a program's initial contract. At that point, the government has the most control over what development tasks it will pay for and thus what technical data rights it can obtain. A program will then spend the following decades of its life cycle acquiring, maintaining, or losing technical data rights. A program has a chance to acquire additional tech data for a system every time it issues a new contract or through reverse engineering efforts. However, industry will aggressively seek to undermine these efforts in order to make programs more dependent on their services. Pressure from industry, shortfalls in initially ordered technical data, and poor data rights education within the government make the lack of technical data a constant problem for programs in the O&S phase.

Specific solutions to O&S technical data rights problems vary depending on the nature of the technical data and the specifics of each contractor agreement. Experience shows that dealing with IP is a “leverage” game. Industry is traditionally much more effective at protecting their leverage and will often “no bid” attempts to acquire additional data rights or will charge an unrealistic price for it. Air Force organizations routinely fail to do their homework and find ways to maximize their technical data leverage, instead opting to award sole source contract after sole source contract. The following strategy will help an organization acquire needed technical data or plan on how to acquire it at a later time. Employ this strategy with assistance from your legal team and designated Air Force IP POCs.

The Strategy

Step 1: Search for the needed technical data or comparable technical data. This may not be a trivial task for older systems. Narrow the search by segregating system elements using the system WBS and focusing on finding data for the most critical elements. All or a portion of the needed data may be in required deliverables like test reports or in delivered data like FFF data and OMIT data to which the government automatically has UR. The Defense Federal Acquisition Regulation Supplement (DFARS) section 227.7103-5c states, the government can use even LR technical data they have in their possession in an emergency. Air Force organizations should also reach out to other government agencies who might have data from similar programs and U.S. allies who might have had data delivered to them through their own contractor agreements. Data rights secured by one government organization are almost always available for use by any other government organization.

Step 2: Perform a cost-benefit or economic analysis of the system. This analysis will quantify the value of the needed technical data to the program and list what the cost would be to recreate it. An organization should be familiar with building this type of system in order to accurately evaluate the impact of missing tech data. This analysis will provide strong justification for either a sole source, competitive, or organic effort. OMB Circular No. A-131 (Revised) dated December 26, 2013 (Value Engineering) describes this type of analysis, which will ultimately determine “fair and reasonable” prices for tech data and provide a documented rationale for further actions, such as reverse engineering.

Step 3: Ask the industry partner for the technical data and document the answer. If they refuse to provide necessary data needed to sustain the system, subsystem, or component, this will also provide justification for further actions. However, an industry partner may accommodate the government in order to keep up a good working relationship or may be willing to license rights to the data for a reasonable price. It is important to be specific about technical data inquires, like “the control drawings to the nose cone assembly,” since this will help them accurately assess the data’s value to their business. Even data provided at no cost to the government will require a contract modification or a formal agreement so as not to be an illegal “gift.”

Step 4: Do market research to determine if new or existing solutions could replace parts of the system missing technical data and document the result. Integrating new parts of a system is easier for systems designed to be “modular” and requires the data needed to interface with the rest of the system. The government can obtain solutions organically or through industry. If using industry, DFARS 217.7103 states the government cannot require offerors to give up rights as a requirement for contract award and so the government must indirectly meet this need. It does this by clearly stating the tasks it needs data to perform and then asking industry for a data-provisioning plan and a WBS showing predicted funding sources for each part of the system. This method gives the government all the information it needs to assess, and later acquire, needed data while allowing industry the flexibility to use government funds to develop non-priority solutions or use proprietary solutions to meet those same needs. The feasibility of using a new or existing solution usually depends on whether the original industry partner will integrate that solution into the system or not. The government must take on the role of system integrator to avoid this constraint.

Step 5: Reverse engineer the system or sub-system to get the needed technical data. Reverse engineering is a legal way to create technical data packages and is usually the only option when a vendor cannot or will not meet the government's cost, quality, or schedule requirements for technical data. Many times, simply the implied threat of reverse engineering will bring down costs. DFARS Procedures, Guidance, and Information (PGI) 217.7504 identifies reverse engineering as "a last alternative" for significant cost savings and when authorized by your contracting authority. These stipulations should be easy to meet after documenting the previous steps in this strategy. DFAR 252.227-7014 forbids the DoD from reverse engineering commercial software code. Most federal laboratories and all the Air Force depots have the capability to do reverse engineering. In addition, many government organizations are building this capability through partnerships with universities and local businesses. DOD Manual 4140.01 vol. 9 even allows industry to borrow government parts through the Replenishment Parts Purchase or Borrow program for reverse engineering (also called "design replication"). Reference the Reverse Engineering Handbook (MIL-HDBK-115A) for additional guidelines on reverse engineering.

5.3.2. During the O&S Phase, how do I determine what rights in technical data and computer software I actually have?

Response

Air Force programs will find it necessary throughout their life cycles to determine what data rights they have to various systems. This information helps programs know what technical data they are missing, what systems/parts are suitable for competitive acquisitions or alternative sources of repair, and whether contractor markings on delivered technical data are correct. Identifying what rights the government has to various systems requires a thorough analysis of related contract documentation. This task can initially be resource intensive, but is a critical step in safely navigating the IP challenges surrounding a program's technical data rights. Programs should perform this task periodically throughout O&S and when data rights issues arise.

The government determines what data rights it has based on what data rights clauses are in the relevant contracts, what type of data it is, who paid for development of the ICP, and what data (including technical data, computer software and documentation) the government ordered or will order. The following strategy helps programs identify and use this information to meet their technical data needs.

The Strategy

Step 1: Identify what categories of technical data are required. Contracts containing the standard data rights clauses grant the government different levels of rights based on the type of data. A program's legal and contracting teams should determine what data rights language is in their contracts. Commercial software licenses and any SNLR licenses grant the government rights according to what the license says. Any contracts not containing the correct data rights clauses are by default SNR licenses. Regulation does not consider data used for source section or contract administration as technical data and also severely limits its use. The government automatically receives UR to data describing the FFF of an ICP, data resulting from government requested testing, and data used for OMIT. If dealing with FFF or OMIT data, skip down to step 5. The rest of this strategy will identify a program's rights to data outside of the previously listed categories including noncommercial software code/documentation, detailed design documentation, and detailed manufacturing data.

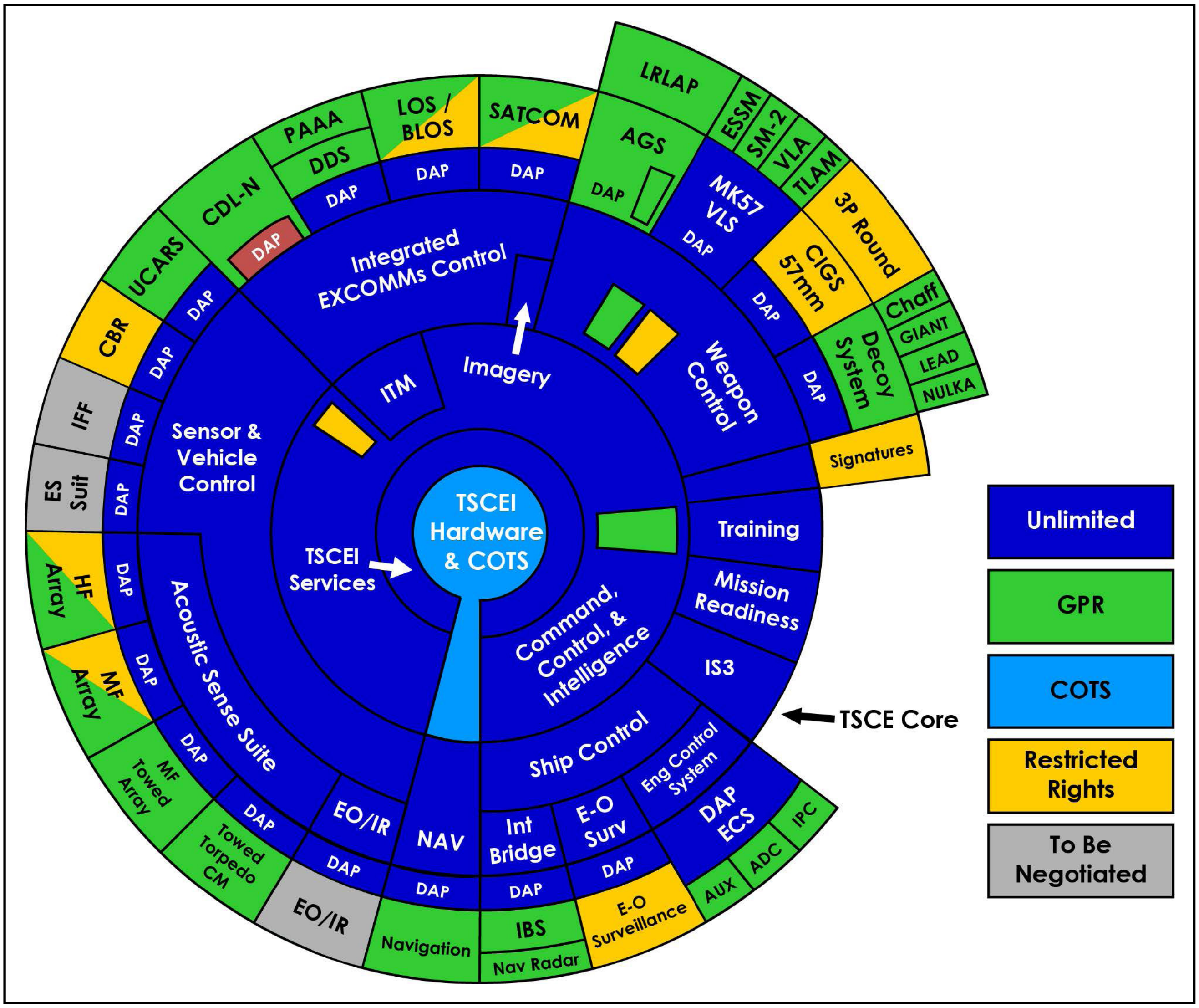
Step 2: Deconstruct selected technical systems using their WBS. Starting with the highest priority ICPs, find the technical systems that contain those ICPs and use those system's respective WBSs to separate the systems into their lowest level line replaceable unit (LRU)/shop replaceable assembly elements. DFARS 227.7103 calls for a source of developmental funds determination to be made when deciding technical data rights (aka, "license rights") and the DFARS 252.227-7013, -7014, -7015 clauses defining funding sources at the lowest practicable level, which is usually the lowest level WBS elements. For noncommercial software, this should be at the level of its software subroutines or modules. Lower levels of code would not be useful and thus not "practicable." If industry mixes private and government funds at a lower level than this, then the government receives GPR to that ICP. This WBS will eventually become an invaluable data rights tool once the program maps WBS elements to funding sources.

Step 3: Review program and contract documentation to identify the funding sources for WBS elements. DoD regulation grants rights to whoever funded development of the ICP the technical data describes, not who funded creation of the data. Possible documentation includes contracts, status reports, integrated master schedules (IMS), integrated master plans (IMP), DALs, rights assertion tables (RATs), earned value management (EVM) records, etc. This information will be effective only if blessed by a program's legal and contracting teams. For noncommercial items, the program can request that industry justify restricted or limited data assertions (see Section 5.1). For commercial items, regulation assumes industry paid for development and so grants the government only limited or restricted rights. However, if the commercial designation is incorrect, the government can challenge it. Commercial items are items used for "purposes other than governmental purposes," not just items sold to the public (FAR 2.101 Definitions). Once this document review is complete, the program will have a legally sound understanding of which ICPs they developed at least in part at government expense and what resulting data industry should deliver with at least GPR.

Step 4: Archive and disseminate supporting data rights information. Programs can streamline responding to future data rights challenges by making contracts and other supporting documentation accessible to program, sustainment, and legal teams throughout a given weapon system's life cycle. Organizations must keep contracts containing data rights information, which provide copyright licenses to the government, for the life of a weapon system or risk revoking those rights. A PMO can simplify this information and share it with their teams by color coding (red, green, yellow, etc) the system WBS elements based on what rights the government has to them (UR, limited/restricted, GPR, etc.) and documenting the information in a graphic similar to Figure 29. When shared, this color-coded WBS will empower teams by putting legally enforceable and easily readable data rights information in the hands of those who regularly validate contractor markings and make data-based program decisions.

Step 5: Leverage information about funding sources to strategically order technical data. The government is not entitled to delivery of data it did not order. However, if the government paid for development of an ICP then it is entitled to order data describing that ICP at minimal or no cost (DFARS 252.227-7018). For ICPs developed or partially developed with government funds (corresponding to UR or GPR), the program should order copies of all detailed manufacturing data and production-level technical data packages in accordance with MIL-STD-31000, technical data packages (TDPs), software documentation, and source code. For non-developmental/commercial ICPs or ICPs developed exclusively at private expense (corresponding to LR or restricted rights for software), the program should order FFF and control data. The government should almost always order OMIT data since they receive UR to it (see Section 3.5.). For other categories of data, a program should order it as needed according to their respective industry agreements. A program can use a DAL along with the DFARS deferred ordering clause in order to review what technical data industry will create and then order this data as needed throughout the life of a contract (see Section 1.3.1). Normally, a program has until the three years after the last item delivered under a contract or the last payment, whichever is later, to review or challenge a data rights assertion (DFARS 252.227-7037). Ordering the correct technical data will maximize data rights/return on investment and guide various program life-cycle decisions throughout O&S.

Figure 29. Sample Naval Total Ship Computing Environment Infrastructure (TSCEI) color coded WBS showing levels of government rights to TSCEI Hardware and COTS system elements. A circular WBS displays lowest level elements around its perimeter



Chapter 6 – Integrated Data/Digital Environments

Acquisition policy documents encourage digital data concepts of operations that allow every activity associated with a program to cost-effectively create, store, access, manipulate, and exchange digital data. When a program is considering the options on how to implement such policy, the term "Integrated Digital Environment," or "IDE," is frequently mentioned.

An IDE is a data storage and information management system that permits authorized users to electronically create, view, annotate, manipulate, deposit/upload, retrieve/download, and exchange data created and utilized during the period of performance of the contract. An IDE is a tool for sharing technical data with government users to implement digital data operations over the life cycle of an acquisition program. An IDE provides a data repository for electronically available data deliverables. The goal is to obtain an efficient, contractually implementable means for the electronic transfer of digital data between the Government and the contractor.

The arrangement allows for access to and/or delivery of technical data required by the PMO and supporting staff such as engineers and logisticians. References to IDEs have been around over 20 years and can be found in the Defense Acquisition Guidebook and AFPAM 63-128 among other places. Successful implementation of the IDE requires extensive contractual negotiations and collaboration with the contractor and ground rules laying out the Government's data management needs over the life cycle of the system.

The IDE consists of three parts:

- The data environment (normally a web-based platform such as Microsoft SharePoint®)
- The data that resides within that environment
- The IP rights the contractor will grant to the Government to both the data environment and the data that resides within that environment

While many PMOs authorize their contractors to establish such systems, in most cases they fail to describe the concept of operations (CONOPS) for such systems in enforceable contract language. As a result, contractors may exploit such a single-point failure in the PMO's management infrastructure by perpetrating unilateral shutdowns/lockouts as a means of gaining leverage over the PMO or inappropriately restricting the Government's use of data residing or delivered on the IDE.

6.1. What regulations and policies apply to a contractor data repository/IDE?

Response

When an IDE is to be used, certain considerations should be made during the acquisition planning, solicitation, and contract formation and administration stages to ensure successful data operations in the digital realm.

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.

Industry partners have been strongly encouraged to develop and implement IDE solutions that best meet the needs of their preferred business model. The program IDE should take maximum advantage of and have minimum impact on existing industry solutions, and the program manager should use existing infrastructure (e.g., Internet or wireless LANs) when practicable. During execution, the program manager should address the status and effectiveness of the IDE at milestone reviews and at other appropriate decision points or program reviews.

With regard to regulations that apply to IDEs, DFARS 227.7207, "Contractor data repositories," states: "Follow 227.7108 when it is in the Government's interests to have a data repository include computer software or to have a separate computer software repository. Contractual instruments establishing the repository requirements must appropriately reflect the repository manager's software responsibilities." The referenced DFARS 227.7108, "Contactor data repositories," goes on to provide additional detail as follows:

(a) Contractor data repositories may be established when permitted by agency procedures. The contractual instrument establishing the data repository must require, as a minimum, the data repository management contractor to—
  (1) Establish and maintain adequate procedures for protecting technical data delivered to or stored at the repository from unauthorized release or disclosure;
  (2) Establish and maintain adequate procedures for controlling the release or disclosure of technical data from the repository to third parties consistent with the Government's rights in such data;
  (3) When required by the contracting officer, deliver data to the Government on paper or in other specified media;
  (4) Be responsible for maintaining the currency of data delivered directly by Government contractors or subcontractors to the repository;
  (5) Obtain use and non-disclosure agreements (see 227.7103-7) from all persons to whom GPR data is released or disclosed; and
  (6) 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 made by the data repository contractor or its officers, employees, agents, or representatives.

(b) If the contractor is or will be the data repository manager, the contractor's data management and distribution responsibilities must be identified in the contract or the contract must reference the agreement between the Government and the contractor that establishes those responsibilities.

(c) If the contractor is not and will not be the data repository manager, do not require a contractor or subcontractor to deliver technical data marked with LR legends to a data repository managed by another contractor unless the contractor or subcontractor who has asserted LR agrees to release the data to the repository or has authorized, in writing, the Government to do so.

(d) Repository procedures may provide for the acceptance, delivery, and subsequent distribution of technical data in storage media other than paper, including direct electronic exchange of data between two computers. 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.

Additionally, Air Force Instruction (AFI) 63-101/20-101 para 4.7.4.2 states the PM shall "Provide digital product design data, during O&S, to a DoD standardized product data management system (e.g. the Joint Engineering Data Management Information and Control System) for common government storage, maintenance, access, and control. If a prime contractor central repository is used instead of a government maintained and controlled facility, appropriate data access and retrieval rights for government personnel must be ensured through specified inclusion in the contract."

The Strategy
Step 1: When planning an acquisition, implement digital data operations accounting for the entire life cycle and leverage existing infrastructure.

Step 2: Capture the Government's vision for digital data operations for the life cycle in a CONOPS for digital data in the solicitation.

Step 3: Ensure that the contractual instrument establishing the data repository enforces, as a minimum, the requirements of DFARS 227.7108.

Step 4: If a contractor will be providing the Government access to an IDE, consider using the checklist (Figure 30), which provides a list of talking points for discussion during legal review. When contracting for an IDE, the goal should be to provide an efficient, contractually implementable means for the electronic transfer of digital data between the Government and the contractor, all in a way that supports the Government's requirements. Among those needs should be a clear understanding of how the IDE fits into the long-term picture and recognition that the IDE is a service available only for the duration of the contract.

6.2. What is a CONOPS for an IDE, and what information should be considered in deciding what it should include?

Response
When the Data Management Strategy requires an IDE, a CONOPS (sometimes referred to as a Government Concept of Operations, or GCO) plays a vital role in defining expectations for the resulting product. It succinctly expresses the data management strategy in terms of needs and expectations for the program. A CONOPS is a product of the program's data management planning and will become part of the RFP and ultimately the SOW in the final contract. It should specify the level of detail necessary for contractors to create proposals that will meet the data management strategy needs of the program yet be thoughtfully written in order to maximize flexibility in proposing solutions. The technical data is the foundation for supporting weapons systems, so a well written CONOPS plays a vital role in acquiring solutions that ultimately meet program data needs.

IDE/CONOPS requirements will invariably differ from program to program. However, many aspects of technical data for consideration will be consistent across all of them. Below is a list of considerations that should be addressed when formulating a CONOPS for an IDE. (See GEIA-HB-859.)

Types of data required—frequency of use, timeliness of access or delivery to
Use and review and approval processes
Use, locations and functions
Hardware and software systems—current and future for consideration
Data interchange requirements—format, media, applicable standards, and existing capabilities
Access requirements and concurrent user requirements
Data management responsibilities
Data flow among sites/facilities
Identification of data integration between disciplines
Methods to be used to exchange data
Rules defining when data are considered to be "delivered"

Rules regarding approval of electronically delivered data
Rules for notification that data is available for access
Disposition of data on the IDE after the period of performance ends
Additional requirements that may apply due to the specific data types, formats, or other peculiarities should be considered.

Examples might include:

Government IP rights
Data markings such as rights, contract numbers, DoD distribution statements, export control, and destruction notices
CAD and model data requirements and software for viewing/using
Product and manufacturing information (PMI)
Metadata

6.3. If the Government wants a contractor to establish an IDE as part of the execution of a contract, what terms should be included in the solicitation? SOW/PWS? Contract? If a contractor proposes to provide the Government with "access" to documentation or software through an IDE, what should be included in a related agreement to protect the Government?

Response
If program managers determine it is in the Government's interest to establish an IDE, they must understand they may be placing the program in a vulnerable position if no enforceable CONOPS for that IDE is included into the resulting contract and the contractor decides to unilaterally shut off the PMO's access to that IDE. Contracting officers should bring to their leadership and other personnel's attention the mandates in the DFARS, AFI 63-101/20-101, and AFPAM63-128 that require the CONOPS for a contractor IDE to be included in the RFP and the resulting contract. Next, the contracting officer should work with other professional disciplines—i.e., intended users, information technology professionals, and program attorneys—to incorporate appropriate language into RFPs and contracts that describe the CONOPS for the IDE the contractor will be required to create and maintain for that program during the period of performance of the contract.

Because inclusion of an IDE concept in a Section H clause could have a significant cost or administrative impact on contractors, use of such a clause may require approval of USD(O&S)/DPAP and publication for comment in the Federal Register. FAR 1.301(b); DFARS 201.304(1)(i)(B); AFFARS 5301.304. It is advisable therefore that contracting officers carefully tailor the recommendations provided below for inclusion into Sections B, C, and J of an RFP.

The Strategy
Step 1: Contracting officers should meet with PMO personnel and IT professionals familiar with the capabilities of commercial IDE software applications to hammer out the proposed CONOPS.

Step 2: So the PMO will understand what it is paying for and enhance its ability to make informed decisions, establish a separate CLIN in Section B that will require the offeror to create and maintain an IDE.

Step 3: Add a tasking statement in the SOW that requires the contractor to create and maintain an IDE in accordance with its proposed CONOPS for that IDE.

Step 4: Include instructions in Section L that require offerors to propose a CONOPS for their IDEs. That CONOPS should address the following topics:

- Require the offeror to submit four additional CDRLs (software product specification (SPS), software version description (SVD), database design description (DDD), data accession list (DAL)) as part of its proposed Exhibit A.
- With respect to the offeror's proposed CONOPS that will become a separate Section J attachment:
    - Describe the purpose of the IDE.
    - Define all terms (especially the word "access").
    - Identify the IDE's minimum capabilities.
    - Describe how the offeror will configure the IDE consistent with the relationship between the four CDRLs described above.
    - Identify all types of data that will reside on the IDE.
    - Classify all data that it or its subcontractors will deposit/upload into the IDE as "deliverables" when so deposited/uploaded and that the Government will be notified whenever an item of data has been so deposited/uploaded.
    - Identify what procedures the contractor will develop and maintain to protect all data residing within the IDE from unauthorized release or disclosure, including what procedures the contractor will implement to ensure that restrictive markings affixed to all data will comply with the terms and conditions of the contract.
    - Describe how the offeror will obtain use and non-disclosure agreements from all non-government employees to whom data will be released or disclosed.
    - Identify during what periods authorized users will be able to "access" the data residing on the IDE, under what conditions they will not be able to "access" that data, and the maximum number of authorized users the IDE will be able to support simultaneously.
    - State that the offeror will deliver the SPS, SVD, DDD, and all data listed on DAL CDRLs that constitute the IDE.
    - State that the offeror will image the IDE and deliver that instantiation to the contracting officer upon request.
    - State that the offeror will indemnify the Government against every claim or liability, including costs and expenses resulting from or as a consequence of, an unlawful release or disclosure of any item of data via the IDE.
    - Identify the monetary remedy to which the Government will be entitled to receive should the contractor unilaterally shut off access to the IDE.
    - Identify what restrictive markings shall be affixed to what types of data that will reside within the IDE.
    - Identify what IP rights the Government will acquire to the four CDRLs identified above as well as to all data that will reside within the IDE.
    - Identify and provide copies of all commercial licenses to all commercial data the offeror will use to create the IDE or will reside within the IDE.

Step 5: In Section M, include evaluation criteria that state the Government will evaluate the extent to which the offeror's proposed IDE will permit all personnel assigned to the PMO the ability to securely create, view, manipulate, annotate, deposit/upload, retrieve/download, and exchange all data residing within the IDE during the period of performance of the contract.

Figure 30. Solicitation/Contract Checklist for Integrated Digital Environments

SOLICITATION/CONTRACT CHECKLIST FOR INTEGRATED DIGITAL ENVIRONMENTS*

If a contractor will be providing the Government access to an Integrated Digital Environment ("IDE"), then the following checklist provides a list of talking points for discussion during legal review. When contracting for an IDE, the goal should be to provide an efficient, contractually implementable means for the electronic transfer of digital data between the Government and the contractor, all in a way that supports the Government's needs. Among those needs should be a clear understanding of how the IDE fits into the long term picture and recognition that the IDE is a service available only for the duration of the contract.

ACQUISITION PLANNING	
□	Prepare a Concept of Digital Data Operations ("CONOPS") describing digital data plans over the life cycle (e.g., available resources, users, and relevant data types).[7, 8, 9]
SECTION B, SUPPLIES OR SERVICES AND PRICES	
□	Create a separate contract line item for the IDE's operation, security, and maintenance, to include data maintenance, in support of cost benefit evaluations and other things.[11]
SECTION C, STATEMENT OF WORK	
□	Establish a clear, enforceable requirement for the IDE with reference to the CONOPS.[5, 10]
	- Account for core functions required by the CONOPS.
	- If on-line, remote access to data is desired, so state in the Statement of Work.
	- List availability requirements and the number of Government users.
	- Provide for post-contract data transition planning in view of the CONOPS.
□	To obtain data over the long term, data deliverable requirements should be included. In the end, the IDE is a service available only for the life of the contract.[3, 10]
	- Include data deliverables through appropriate performance-based work statements, various DD Form 1423s, or both.
	- Account for electronic delivery, either in place or through digital exchange with a Government system.
	- Preserve the option of physical delivery.[2]
SECTION E, INSPECTION AND ACCEPTANCE	
□	Describe how IDE services will be reviewed and accepted.[10]
□	Describe how digital data products, as well as physical data products, will be received, inspected, and accepted.[9]
SECTION H, SPECIAL CONTRACT REQUIREMENTS	
□	Establish proper handling procedures to protect from unauthorized disclosure.[2]
	- Obtain necessary non-disclosure agreements when proprietary data is accessible.
	- Account for various types of data that may be accessible.
	- Account for subcontractor interests, such as through an opt-out provision.
	- Markings, markings, markings![12]
□	Protect the Government's interests with relation to the IDE and its data residents.[12]
	- Seek indemnity from IDE provider for liability resulting from data mishandling.[2]
	- List availability requirements as they relate to unilateral access denials.[10, 11, and 12]
	- Beware of embedded licenses, click-wrap licenses, and the like.[12]
	- Clarify the scope of the disputes clause in relation to the IDE.[12]
	- Consider segregating delivered data to preserve its pedigree.[12]

SECTION I, CONTRACT CLAUSES	
□	FAR Case 2011-020, Safeguarding of Contractor Information Systems (Forthcoming)
□	DFARS 252.204-7012, Safeguarding of Unclassified Controlled Technical Information
□	DFARS 252.227-7013, 7014, 7015, 7018 (Rights allocation clauses)
SECTION J, LIST OF DOCUMENTS, EXHIBITS, AND OTHER ATTACHMENTS	
□	Include the Government's CONOPS as Government Furnished Information.[10]
□	Include Contract Data Requirements Lists (DD Form 1423) in response to various data needs.
SECTION L, INSTRUCTIONS, CONDITIONS, AND NOTICES TO BIDDERS	
□	Describe how any contractor-provided solutions will support all life cycle activities, including interfacing with Government systems, in response to the CONOPS. [11]
SECTION M, EVALUATION FACTORS FOR AWARD	
□	Insofar as IDEs are to leverage a contractor's existing infrastructure, evaluation factors should focus on the contractor's ability to support the Government's digital data operations strategy as reflected in the CONOPS.[3]
OTHER	
□	Pursue IDEs in conjunction with deferred data acquisition techniques, such as priced contract options and the deferred ordering and delivery clauses.[12]

RESOURCES

LAWS
[1] 10 U.S.C. § 2320 (2006).

REGULATIONS
[2] 48 C.F.R. § 227.7108 (2011).

ACQUISITION GUIDANCE DOCUMENTS
[3] Defense Acquisition Guidebook, § 2.3.14.2; § 4.2.3.1.7; § 5.1.6.5, and § 11.12.

[4] AFPAM 63-128, Guide to Acquisition and Sustainment Life Cycle Management (Oct. 5, 2009).

[5] MIL-HDBK-245D, Handbook for Preparation of Statement of Work (SOW) (Dept. of Defense April 3, 1996).

[6] Dept. of Defense Open Systems Architecture Contract Guidebook for Program Managers, (Dept. of Defense Dec. 15, 2011).

DATA MANAGEMENT GUIDANCE DOCUMENTS
[7] ANSI/GEIA-859-2009, Data Management (2009).
[8] ANSI/GEIA-HB-859, Data Management (Jan. 2006).
[9] MIL-HDBK-X132, Acquisition Data Management, (Dept. of Defense Dec. 12, 2008) (draft).
[10] MIL-HDBK-59B, Continuous Acquisition and Life-Cycle Support Implementation Guide, (Dept. of Defense June 10, 1994) (cancelled).
[11] MIL-STD-974, Contractor Integrated Technical Information Service (CITIS), (Dept. of Defense Aug. 20, 1993) (cancelled).
[12] SAF/GCQ Lessons Learned and Best Practices.

Appendix A – FAR/ DFARS Patent, Technical Data, and Computer Software Clauses

TD = Technical Data; CS = Computer Software; ICP = Item, Component, or process; CSD = Computer Software Documentation

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

Specific Clauses and 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 and construction with many prohibitions on use.
52.227-10: All that 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 is 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.

Source: DISA, https://disa.mil/About/Legal-and-Regulatory/DataRights-IP/DataRights#10

Appendix B – Guidebook Contributors

The following personnel are all subject matter experts on data and data rights. Their contributions to this Guidebook have been invaluable.

Kanna Annamalai-Brown (SAF/AQC)
Susan Bergeron (AFLCMC/AZA)
Mark Borowski (SAF/GCQ)
Ken Branham (AFMC/A4)
Stephanie Burris (AFMC/JAQ)
Steve Clark (SAF/AQX)
Ryan Eatough (AFLCMC/ISR)
Bob Flagg (AFLCMC/LG)
Katherine Frotten (AFLCMC/PZ)
Jacqueline Gall (AFMC/JA)
Chris Garrett (AFLCMC/EZ)
Jim Gravely (AFLCMC/LG)
Jim Haag (SMC/JAQ)
Dora Hancock (SAF/AQC),
Howard Harris (DAU)
Curtis Jefferson (AFMC/EN)
Mike Jennings (AFLCMC/LG)
Elizabeth Kent (AFLCMC/HN)
Rob Klauzinski (66th ABG/JA)
Nancy Kremers (SAF/GCQ)
Racheal Lienhard (AFLCMC/AZA)
Tim Livingston (AFSC/EN)
Chris Monsey (NWSC-Crane)
Kraig Neer (AFMC/PK)
Mike Oar (SAF/AQD)
Bruce Page (AFMC/JAQ)
Jeremy Peters (OC-ALC)
Col Christine Piper (SAF/JA)
Beth Rogers (AFLCMC/AZA)
Dave Ruddy (SAF/GCQ)
Billy Sandridge (AFMC/PK)
Marc Shaver (AFMC/EN)
Porter Smith (WR-ALC)
Sarah Stanton (SAF/JA)
Dave Stark (AFLOA/JA)
Jeff Watson (AFLCMC/BES)
Mike Wills (WR-ALC)
Amanda Woodruff (AFLCMC/LG)
Chris Young (AFLCMC/AZA)