
EIGHTH EDITION

MAY 2017

PREPARED BY
OFFICE OF THE STAFF JUDGE ADVOCATE
SPACE AND MISSILE SYSTEMS CENTER (SMC)

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.
FOREWORD

Business entities and governments are more cognizant of the value of intellectual property (IP) now than at any time in recorded history. Business entities consider IP their “lifeblood”, which they actively guard and for which they charge a premium. In a similar fashion, the Department of Defense (DoD) considers a certain type of IP—technical data and computer software rights acquired under its contracts—its “lifeblood” because that IP enables the DoD to enhance competition and sustain systems and their subsystems over their life cycle (e.g., development, production, testing, installation, operation, maintenance, upgrades/modifications, interoperability with other systems, transfer of technologies to other programs/systems/platforms).

This Handbook provides a practical “cradle-to-grave” approach to acquiring technical data and computer software rights. It is an extended treatment of that subject which is briefly discussed in Government Contract Law for Engineers (September 2004) issued by SMC/JA. I want to acknowledge Mr. James H. Haag as the driving force and main contributor to this Handbook. Please submit any suggested improvements or corrections to this handbook to the Contract and Patent Law Division, Office of the Staff Judge Advocate, Space and Missile Systems Center, Los Angeles AFB, 483 North Aviation Boulevard, El Segundo, CA 90245 or to james.haag@us.af.mil.

The approach described in this Handbook is agnostic, meaning that program offices have used it in development, production, and sustainment contracts to acquire hardware-intensive systems, software-intensive systems, and services. In that regard, Appendix 1 contains excerpts from a request for proposals (RFP) for a services acquisition; Appendix 2 contains excerpts from an RFP for a software-intensive system; and Appendix 3 contains excerpts from an RFP for a hardware-intensive system. Various program offices carefully tailored those excerpts for each acquisition using the disciplined intellectual framework described in this Handbook to account for the specific needs of their particular acquisition.

Each acquisition has its own unique needs for rights in technical data and computer software. Unfortunately, a one-size-fits-all-panacea-clause does not exist. If it did, the drafters of the Defense Federal Acquisition Regulation Supplement (DFARS) would have included such a clause into that acquisition regulation the last time (i.e., June 28, 1995) they issued a complete rewrite of the regulations applicable to this topic—or the last time they proposed another complete rewrite of those regulations (i.e., September 27, 2010). It would therefore be inadvisable for the reader to conclude that all that is necessary is to select one of the examples included in Appendices 1-3 and copy it over into their RFP. Instead, this office recommends that readers use the disciplined intellectual framework recommended in this Handbook to carefully tailor one of these examples to satisfy the unique needs of their specific program.

The Office of the Staff Judge Advocate, Space and Missile Systems Center (SMC/JA), issued the first edition of this Handbook in June 2009. Since that time, one commentator has described this Handbook as
“[t]he most detailed guidance that we have found [regarding] how does an agency evaluate the life-cycle cost of limited rights technical data (and restricted rights computer software) when it cannot use the bargaining power of the original competition for the development contact to force the contractor to give up the rights[.].”

Since SMC/JA issued that first edition, the DoD Open Systems Architecture Contract Guidebook for Program Managers, MIL-HDBK-502A (“Product Support Analysis”), and a GAO audit report (GAO-11-469) have approvingly cited this Handbook. AFPAM63-128 (“Integrated Life Cycle Management”) has adopted the recommendations contained in Section V.A. of this Handbook. One Defense Acquisition University online training resource (CLM 075) has adopted the techniques described in Section V.C of this Handbook to train over 1200 acquisition professionals from all military departments and defense agencies. In August 2015, the Assistant Secretary of the Army (Acquisition, Logistics and Technology) adopted a modified form of the approach described in Section V.C.5.g. of this Handbook when she issued the 1st Edition of the Army Data and Data Rights (D&DR) Guide and highly encouraged Program Executive Officers, Program Managers, and their support personnel to use that Guide for all Army ACAT programs. In August 2016, the Aerospace Industries Association (AIA) and the American Bar Association’s (ABA) Section of Public Contract Law cited section V.C.1.a of this Handbook in letters sent to a Congressionally-chartered Government-Industry Advisory Panel. (The mission of that Panel is to review 10 U.S.C. §§ 2320 and 2321 and their implementing regulations to ensure those requirements are best structured to serve the interests of the taxpayers and the national defense.) Only time will tell how much further the practical techniques described in this Handbook will spread throughout the DoD.

Due to the size of the appendices to this Handbook, this office has highlighted relevant portions of Appendices 1-3 in yellow in the soft copy so readers can quickly find those excerpts. Readers may wish to print out a double-sided hard copy of this Handbook using a color copier and insert that copy into a three-ring binder, as that approach will facilitate the reader’s ability to find a relevant portion in an appendix the rationale for which this handbook discusses in the narrative portion.

One final observation bears mentioning. The first edition of this Handbook consisted of 151 pages, of which 34 pages consisted of narrative. This edition consists of 516 pages, of which 100 pages are narrative. This increase in the page count is attributable to various factors (e.g., new statutory/regulatory/policy mandates, lessons learned during the intervening years, additional explanations provided in support of recommendations previously provided, new appendices, hyperlinks to relevant resources summarized in the narrative).

But one fact that has remained unchanged since this office issued the first edition of this Handbook is this: the proper acquisition and enforcement of rights in technical data

and computer software under DoD contracts is one of the most complicated subjects in Federal procurement law. It cannot be understood—much less mastered—by skimming through a few cryptic bullets on a PowerPoint® presentation because, as tartly noted by the Secretary of Defense, “PowerPoint makes us stupid.” If members of the DoD acquisition workforce—irrespective of rank or grade—are unwilling to spend the four hours of time needed to carefully read the narrative provided herein and review the examples provided in the appendices, they may very well learn the lesson the Program Executive Officer (Joint Strike Fighter) has learned: There is no fun to be had when cleaning up the mess left by one’s predecessors relative to the acquisition of the most expensive weapon system ever procured in U.S. history.

Put another way, the pithy comment made by a legend in the spacefaring community over half a century ago remains true today:

“. . . It’s not easy for the Government to determine which bid or proposal we receive from industry is best, and how well competing claims and estimates can be substantiated. In order for us to use the very best judgment possible in spending the taxpayer’s money intelligently, we just have to do a certain amount of this research and development work ourselves. We just have to keep our own hands dirty to command the professional respect of the contractor personnel engaged with actual design, shop and testing work.

Otherwise, our own ability to establish standards and to evaluate the proposals—and later the performance—of contractors would not be up to par.

Our Marshall Center engineers operate like doctors: i.e., you take the doctor away from his patients, he soon forgets how to practice medicine and starts writing books or publishing trade journals about it.”

This Handbook is not designed to furnish legal advice to specific problems. Readers should neither cite nor rely upon this Handbook as a substitute for legal advice.

---


YOU ARE ENCOURAGED TO SEEK THE ADVICE OF YOUR PROGRAM ATTORNEY ON SPECIFIC LEGAL PROBLEMS.

PAUL E. CRONIN, Colonel, USAF
Staff Judge Advocate
# Table of Contents

**FOREWORD** ................................................................. i

I. Introduction ........................................................................... 1
   A. Why Be Concerned? ......................................................... 5
   B. Fundamental Concepts .................................................. 7

II. Terminology .......................................................................... 9
   A. “Technical Data” ............................................................ 10
   B. “Computer Software” ...................................................... 10
   C. Noncommercial Rights .................................................. 10
       1. Unlimited Rights ....................................................... 10
       2. Government Purpose Rights .................................... 11
       3. Limited Rights ........................................................ 11
       4. Restricted Rights .................................................... 11
       5. Specifically Negotiated License Rights ....................... 12
       6. SBIR Data Rights ...................................................... 12
   D. Commercial Rights ....................................................... 13

III. Relevant Constraints ....................................................... 17

IV. Modular Open System Approach (MOSA) ............................ 18
   A. Definitions ..................................................................... 19
   B. Relevant Systems Engineering Resources ....................... 21
   C. Results Achieved By Using MOSA ................................. 25

V. The “Cradle-to-Grave” Approach ....................................... 27
   A. Drafting The Capability Development Document (CDD)/Capability Production Document (CPD) ......................................................... 27
   B. Formulating the Acquisition Strategy ................................ 30
       1. Subparagraph 7.6.1 ................................................... 32
       2. Subparagraph 7.6.2 ................................................... 33
       3. Subparagraph 7.6.3 ................................................... 41
       4. Subparagraph 7.6.4 ................................................... 42
       5. Subparagraph 7.6.5 ................................................... 42
   C. Drafting the Request for Proposals (RFP) .......................... 44
       1. Exhibit A (Contract Data Requirements List)(CDRL) ........ 45
       2. Section B (Supplies Or Services And Prices/Costs) ........ 51
       3. Section H (Special Contract Requirements) ................... 52
       4. Section I (Contract Clauses) ....................................... 54
       5. Section J (List of Attachments) .................................... 54
       6. Section K (Representations, Certifications, And Other Statements Of Offerors) .......................... 59
       7. Section L (Instructions, Conditions, And Notices To Offerors Or Respondents) ...................... 59
       8. Section M (Evaluation Factors For Award) .................... 61
I. Introduction

Ultimately, the development and acquisition of IP boils down to one word:

Money.

The reason why is because innovation requires substantial financial investment and effort over a long period, and it uses scarce resources. Where the Government is not subsidizing or outright funding that investment, industry must rely on the IP rights or other resulting competitive advantages as the primary means to make the investment worthwhile. By law, the Government is required to honor any restrictions on its ability to use, release and disclose a corporation’s IP—including technical data and computer software—as reflected by restrictive markings affixed to that IP. Those restrictions exist because the unauthorized or inadvertent disclosure of trade secrets\(^5\) may destroy their commercial value. Although legal remedies for improper disclosure of trade secrets include money damages, injunctions and criminal sanctions, contractual remedies for improper disclosure are often inadequate to preserve the value of the trade secret because it is difficult to prove misappropriation.

Arguably, the proper acquisition of technical data and computer software rights by the Government—a hybrid of the IP concepts of trade secrets and copyrights—is one of the most complicated subjects in Federal procurement law. This dilemma is not necessarily due to any ambiguities that may exist in regulations. Rather, this dilemma is caused in part by (1) their length and format, and (2) their application to specific acquisitions.

As regards their length and format, the regulations take up 118 single-spaced pages in the DFARS. Moreover, to understand how they work one must read those pages and use them multiple times during contract formation and administration—because the regulations are not laid out in chronological order.

With respect to their application to specific acquisitions, rights in technical data and computer software are a function of the technical data and computer software the program office seeks to procure, which in turn is a function of the hardware the program office seeks to procure, which in turn is a function of the mission the requirements

\(^5\) The definition of the term "trade secret" varies depending upon whether one is discussing, e.g., the Trade Secrets Act (18 U.S.C. § 1905), the Freedom of Information Act (5 U.S.C. § 552(b)(4)), or the Uniform Trade Secrets Act codified by most states (e.g., Cal. Civ. Code Ann. § 3426.1(d) (Deering’s 2017)). When using that term in this *Handbook*, the authors are using the definition of "trade secret" in the Economic Espionage Act of 1996, as amended by the Defend Trade Secrets Act of 2016, because that definition is the only one codified in Federal law, *i.e.*, “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if [ ] the owner thereof has taken reasonable measures to keep such information secret[ ] and the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information”. 18 U.S.C. § 1839(3).
community seeks to accomplish by placing that weapon system into the warfighter’s hands. As noted by one commentator in a broader context:

“So how does one determine how to best structure a program? Whether you are a PM, or a chief engineer, or a contracting officer, or a life cycle support manager, you have to start in the same place. You begin with a deep understanding of the nature of the product you intend to acquire. The form of the program has to follow the function the program will perform: developing and acquiring a specific product. The nature of the product should be the most significant determiner of program structure.”

In a similar manner, to understand what rights in technical data and computer software the program office needs to procure, one must have an intimate familiarity with the weapon system—its requirements, its proposed Work Breakdown Structure (WBS) reflecting its level of system decomposition, the program’s System Engineering Plan (SEP) for that system, the system’s proposed software architecture, how the system will be designed/developed/produced, how its design/performance requirements will be validated and verified, where and under what circumstances it is likely to be deployed, and how—as reflected in its Life-Cycle Sustainment Plan (LCSP)—it will be maintained/sustained/disposed throughout its life cycle.

---


To date, no other DoD organization\(^8\) or private publishing company\(^9\) has issued a publication like this one—a user-friendly resource that provides a detailed “cradle-to-grave” approach to acquiring technical data and computer software rights starting from the moment the program office commences drafting the Capability Development Document (CDD)/Capability Production Document (CPD), through drafting the Acquisition Strategy, through properly structuring each section of the Request for Proposals (RFP), through competitive or sole-source negotiations prior to award, through delivery of the technical data and computer software to which those rights pertain, through validating the contractor’s asserted restrictions on the Government’s ability to use, release, or disclose that technical data and computer software outside the Government. That is the purpose of this *Handbook*—to put this topic in chronological order so that program office personnel understand what to acquire, when to acquire, and how to

---


acquire rights in technical data and computer software.10 But before discussing the “what”, “when”, and “how” of acquiring rights in technical data and computer software—much less

10 The Defense Acquisition University (DAU) offers training on this subject via the following courses (to varying levels of specificity depending upon the course in question):

<table>
<thead>
<tr>
<th>Course Number</th>
<th>Course Title</th>
<th>Method of Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACQ 101</td>
<td>Fundamentals of Systems Acquisition Management</td>
<td>Online</td>
</tr>
<tr>
<td>ACQ 202</td>
<td>Intermediate Systems Acquisition, Part A</td>
<td>Online</td>
</tr>
<tr>
<td>ACQ 315</td>
<td>Understanding Industry (Business Acumen)</td>
<td>Resident</td>
</tr>
<tr>
<td>ACQ 370</td>
<td>Acquisition Law</td>
<td>Resident</td>
</tr>
<tr>
<td>CLE 012</td>
<td>DoD Open Systems Architecture (OSA)</td>
<td>Online</td>
</tr>
<tr>
<td>CLE 068</td>
<td>Intellectual Property and Data Rights</td>
<td>Online</td>
</tr>
<tr>
<td>CLM 071</td>
<td>Introduction to Data Management</td>
<td>Online</td>
</tr>
<tr>
<td>CLM 072</td>
<td>Data Management Strategy Development</td>
<td>Online</td>
</tr>
<tr>
<td>CLM 073</td>
<td>Data Management Planning System</td>
<td>Online</td>
</tr>
<tr>
<td>CLM 074</td>
<td>Technical Data and Computer Software Rights</td>
<td>Online</td>
</tr>
<tr>
<td>CLM 075</td>
<td>Data Acquisition</td>
<td>Online</td>
</tr>
<tr>
<td>CLM 076</td>
<td>Data Markings</td>
<td>Online</td>
</tr>
<tr>
<td>CLM 077</td>
<td>Data Management Protection and Storage</td>
<td>Online</td>
</tr>
<tr>
<td>CON 216</td>
<td>Legal Considerations in Contracting</td>
<td>Online</td>
</tr>
<tr>
<td>CON 290</td>
<td>Contract Administration and Negotiation Techniques in a Supply Environment</td>
<td>Resident</td>
</tr>
<tr>
<td>COR 222</td>
<td>Contracting Officer’s Representative Course</td>
<td>Resident</td>
</tr>
<tr>
<td>ENG 301</td>
<td>Leadership in Engineering Defense Systems</td>
<td>Resident</td>
</tr>
<tr>
<td>FE 201</td>
<td>Intermediate Facilities Engineering</td>
<td>Resident</td>
</tr>
<tr>
<td>ISA 201</td>
<td>Intermediate Information Systems Acquisition</td>
<td>Resident</td>
</tr>
<tr>
<td>ISA 301</td>
<td>Advanced Enterprise Information Systems Acquisition</td>
<td>Resident</td>
</tr>
<tr>
<td>ISA 320</td>
<td>Advanced Program Information Systems Acquisition</td>
<td>Resident</td>
</tr>
<tr>
<td>LOG 204</td>
<td>Configuration Management</td>
<td>Online</td>
</tr>
<tr>
<td>LOG 206</td>
<td>Intermediate Systems Sustainment Management</td>
<td>Online</td>
</tr>
<tr>
<td>LOG 215</td>
<td>Technical Data Management</td>
<td>Online</td>
</tr>
<tr>
<td>LOG 465</td>
<td>Executive Product Support Manager (PSM) Course</td>
<td>Resident</td>
</tr>
<tr>
<td>PMT 352</td>
<td>Program Management Office Course, Part A</td>
<td>Online</td>
</tr>
<tr>
<td>PMT 352</td>
<td>Program Management Office Course, Part B</td>
<td>Resident</td>
</tr>
<tr>
<td>PMT 400</td>
<td>Program Manager’s Skills Course</td>
<td>Resident</td>
</tr>
<tr>
<td>PMT 401</td>
<td>Program Manager Course</td>
<td>Resident</td>
</tr>
<tr>
<td>PMT 402</td>
<td>Executive Program Manager’s Course</td>
<td>Resident</td>
</tr>
<tr>
<td>STM 203</td>
<td>Intermediate Science and Technology Management</td>
<td>Resident</td>
</tr>
<tr>
<td>STM 304</td>
<td>Leadership in Science and Technology Management</td>
<td>Resident</td>
</tr>
</tbody>
</table>
describing certain fundamental concepts about those rights—one must answer a fundamental question: “Why should program office personnel be concerned about this topic?”

A. Why Be Concerned?

There are five reasons why program office personnel should be concerned about this topic.

First, law, regulation, and policy require that program office personnel be concerned. Permanent legislation requires the DoD acquire certain types of rights in technical data rights under its contracts. The DFARS implements this statutory mandate not just for technical data but also for computer software. Memoranda issued by USD(AT&L), the DoD Chief Information Officer, the Secretary of the Air Force, the Acting Assistant Secretary of the Air Force, and the Air Force Service Acquisition Executive,

For details, see http://www.dau.mil/training/default.aspx.


as well as various instructions,\textsuperscript{13} reflect senior leadership’s concerns regarding this topic. These concerns are primarily based upon the following reason.


The second reason is that acquiring such rights has a critical impact on the cost and affordability of technology that a program office cannot treat as a separate or distinct issue it can negotiate apart from contract performance requirements or cost/price. Specifically, if program office personnel do not acquire sufficient rights in technical data and computer software prior to award, they may relinquish the opportunity to enhance competition and preserve core logistics capabilities as required by 10 U.S.C. §§ 2464 and 2466. If the Air Force relinquishes that opportunity prior to award, the Air Force will lock itself into a position where the incumbent can force the Air Force to pay an exorbitant price years or decades hence to be able to use, release or disclose that technical data or computer software to individuals outside the Government. Of course, that assumes the incumbent is willing to sell the Air Force a license to use, release or disclose that technical data or computer software to individuals other than Government employees at any price. And once the use of additive (versus subtractive) manufacturing techniques—a process (i.e., vat photopolymerization, material jetting, material extrusion, powder bed fusion, binder jetting, sheet lamination, directed energy deposition) that draws upon a computer-aided design (CAD) file to deposit material, layer upon layer, to construct 3D-printed parts composed of often complex geometries—becomes more widespread, DoD’s need for data and sufficient rights thereto is likely to increase over time.

The third reason is that the unauthorized use, release or disclosure of such trade secrets is a felony under the Trade Secrets and Economic Espionage Acts. The fourth reason is that the unauthorized use, release or disclosure of such trade secrets can subject the Air Force to paying millions of dollars in damages to the owner of that data or software. The fifth reason is that, if a program office does not acquire sufficient technical data or computer software and the rights thereto, the result could be the loss of a weapon system worth over $100 million—and perhaps the death of personnel that just happened to be using that weapon system at the time it experienced a catastrophic failure.14

B. Fundamental Concepts

Before discussing the “what”, “when”, and “how” relative to acquiring rights in technical data and computer software, one also needs to understand certain fundamental concepts about those “rights.” First, there is a difference between the Government owning the delivered physical medium on which the technical data or computer software resides and the Government’s right to use, release and disclose that technical data or computer software to individuals other than Government employees. The Government may own the medium (e.g., book, compact disc, iPhone®) on which the technical data or computer software resides. The Government might not, however, have acquired sufficient rights to use, release or disclose that technical data or computer software to persons that are not Government employees because it has no right to transfer that IP to any contractor. In that case, the Government retains complete ownership of the medium and if the IP can be removed, the Government could transfer the medium to a third party just like the purchaser of a movie on a digital video disc (DVD) could erase the movie and transfer the blank DVD to anyone.

A purchaser of the DVD, however, does not automatically have the right to do anything they want with it (e.g., show the movie to 100 people for a fee). Conversely, the Government could have acquired the “rights” to use, release and disclose IP to individuals that are not Government employees but not own the medium (e.g., the Government could have rights to technical data being developed at Government expense that has never been delivered to the Government). Under those circumstances, the Government would still have to negotiate with the contractor to have the technical data transferred to the medium and pay for the medium. Thus, in general the Government must consider both the acquisition of the medium (i.e., deliverable) and the acquisition of the “rights” to the technical data or computer software residing on that medium.

Second, there is a difference between ownership of the underlying technical data or computer software and the “rights” to use, release or disclose that technical data or computer software to third parties. The owner of technical data or computer software has exclusive control over the use, release and disclosure of that IP (including the right to exclude others from using the technical data or computer software). In contrast, a licensee is limited to using that technical data or computer software in accordance with the terms and conditions of the license the owner has granted the licensee.

Therefore, here is the critical point: Under only unique circumstances (e.g., where the technical data the contractor will deliver to the Government is a “special work” such as audiovisual works, musical compositions, investigative reports, and medical records) does the Government acquire title or ownership to technical data or computer software developed under DoD contracts. This fact remains true even if the Government funded 100% of the development of that technical data or computer software. Instead, the Government almost always acquires a license to use, release or disclose that technical data or computer software to persons who are not Government employees, such as employees of Federally Funded Research and Development Centers (FFRDC) (e.g., The Aerospace Corporation, MITRE), a Systems Engineering and Technical Assistance (SETA) contractor, or a Systems Engineering & Integration (SE&I) contractor. That is why, unless assigned to the Government, the contractor typically owns the copyright in the
technical data and computer software it developed under a Government contract subject to the Government’s license rights (and therefore why copyright markings (“©”) are usually affixed to technical data and computer software delivered to the Government). Under those circumstances, the author of an expression of original thought or work can exclude others from copying, performing, displaying or distributing that IP for the life of the copyright. Accordingly, the DoD will be negotiating over license rights and not ownership in technical data or computer software the contractor will deliver under a contract, and for the reasons stated above it is critical that DoD acquisition professionals understand what license rights the Government will acquire under that contract.

By way of analogy, every driver’s license contains three critical pieces of information:

- the name of the person authorized to drive,
- the type of vehicle that person is authorized to drive (e.g., Commercial Class A, Noncommercial Class A, Commercial Class B, Noncommercial Class B, Commercial Class C, Basic Class C, Motorcycle Class M1, Motorcycle Class M2), and
- an expiration date (i.e., the period during which that person is authorized to drive that type of vehicle).

In a similar fashion, if a program office has not acquired a broad enough license to use, release or disclose a specific item of technical data or computer software to

- specific persons or entities, for
- specifically enumerated purposes, for
- specified periods of time,

the person who releases those items to other than those specified persons/entities or for unauthorized purposes or outside the period permitted by the license may violate two criminal statutes (18 U.S.C. §§ 1832, 1905). With this concept in mind, one can now turn to discussing the “what” (i.e., the terminology) applicable to this subject.

II. Terminology

Experience demonstrates that the DFARS defines various terms (e.g., “computer software”) more broadly in the context of technical data and computer software rights than engineers or computer scientists may have been taught is the case in their undergraduate- or graduate-level computer science courses. The contracting parties may fail to communicate effectively with each other if they use different definitions of the same terms during negotiations prior to award and during contract administration after award. Therefore, understanding the definitions of terms is a prerequisite to properly acquiring and enforcing rights in technical data and computer software.

The following discussion summarizes 10 U.S.C. §§ 2305 and 2320-2321, Federal Acquisition Regulation (FAR) Subparts 2.1, 7.1, 9.5, 15.3, 15.4, 46.3, 46.7, DFARS
Subparts 207.1, 209.5, 215.4, 227.71, 227.72 and 246.7, DFARS Procedures, Guidance, and Information (PGI) Subparts 207.1 and 217.75, the Small Business Innovative Research (SBIR) Program Policy Directive, and SMC Informational Guidance (IG) Subpart 5315.470. Contracts awarded by civilian agencies (e.g., Governmentwide Agency Contracts (GWAC), GSA Federal Supply Schedule (FSS) contracts) contain technical data and computer software clauses required by the FAR that are different from those clauses required by the DFARS. The subject of procuring technical data and computer software via task orders, delivery orders, and Blanket Purchase Agreements issued under GWACs or GSA FSS contracts is beyond the scope of this Handbook. For further details, contact SMC/JAQ.

A. “Technical Data”

“Technical data” is defined by DFARS § 252.227-7013(a)(15) as recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation), excluding computer software or data incidental to contract administration, such as financial and/or management information. Examples of technical data include, but are not limited to, design review data packages, engineering drawings, specifications, interface control documents (ICD), test plans, test procedures, test reports, assessment reports, technical orders, and operations and maintenance manuals.

B. “Computer Software”

“Computer software” is defined by DFARS §§ 252.227-7013(a)(3) and 252.227-7014(a)(4) as computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated or recompiled, but excludes computer databases or computer software documentation. This definition does not expressly mention firmware as being a type of computer software. (SMCI62-109 defines firmware as the “combination of a hardware device and computer instructions or computer data that reside as read only software on the hardware device.”) Nevertheless, the software portion of firmware is encompassed by the broad definition of the term “computer program”, i.e., “a set of instructions, rules, or routines recorded in a form that is capable of causing a computer to perform a specific operation or series of operations.”

C. Noncommercial Rights

A program office may purchase any one of four types of rights associated with noncommercial technical data (i.e., Unlimited Rights, Government Purpose Rights, Limited Rights, Specifically Negotiated License Rights) and any one of four types of rights associated with noncommercial computer software (i.e., Unlimited Rights, Government Purpose Rights, Restricted Rights, Specifically Negotiated License Rights) under DoD contracts.
1. Unlimited Rights

With respect to noncommercial technical data and computer software, Unlimited Rights means the right to use, release, and disclose within and outside the Government without restrictions (DFARS §§ 252.227-7013(a)(16), 252.227-7014(a)(16)).

2. Government Purpose Rights

With respect to noncommercial technical data and computer software, Government Purpose Rights means the right to use, release, and disclose within the Government without restriction and the right to release or disclose outside the Government for U.S. Government purposes. (“Government purpose” includes any activity in which the U.S. Government is a party, including competitive procurements and excluding use, release, or disclosure for commercial purposes.) After five years (or some other period negotiated by the parties), the Government’s rights in that noncommercial technical data or computer software are automatically upgraded to Unlimited Rights. (DFARS §§ 252.227-7013(a)(13), 252.227-7014(a)(12)).

3. Limited Rights

With respect to noncommercial technical data, Limited Rights means the right to use, release and disclose within the Government without restriction and the right to release outside the Government only if all of the following conditions are satisfied:

(1) the recipient requires that data to perform emergency repair and overhaul or the release or disclosure will be to a “covered Government support contractor” in performance of its covered Government support contract for use, modification, reproduction, performance, display, release or disclosure to a person authorized to receive limited rights technical data or (other than detailed manufacturing or process data) will be to a foreign government that is in the interest of the U.S. Government to release and is required for evaluation or informational purposes,

(2) the recipient’s contract contains DFARS § 252.227-7025, and

(3) the Government notifies the owner of that technical data of that reproduction, release, disclosure or use.

If the Government provides Limited Rights technical data to a recipient for purposes of emergency repair or overhaul, the recipient must destroy that technical data and all copies in its possession promptly following completion of the emergency repair/overhaul. (DFARS § 252.227-7013(a)(14)).

4. Restricted Rights

With respect to noncommercial computer software, Restricted Rights means the right to use, copy (solely as a backup) and modify the computer software (generally limited to one computer and not placed upon a shared network) within the Government (if the
contractor is notified that that software will be transferred to another government agency) and the right to disclose that software outside the Government as long as:

(1) the recipient is a contractor/subcontractor performing a services contract to use that computer software to diagnose and correct deficiencies in a computer program, to modify computer software to enable a computer program to be combined with, adapted to, or merged with other computer programs or when necessary to respond to urgent tactical situations, the recipient’s contract contains DFARS § 252.227-7025 or the recipient has signed the Use and Non-Disclosure Agreement found at DFARS § 227.7103-7(c); the Government notifies the owner/licensor that a release or disclosure to the recipient was made; the Government prohibits the recipient from decompiling, disassembling, or reverse-engineering the software or using software decompiled, disassembled, or reverse-engineered by the Government; and the recipient uses the computer program with one computer at one time, or

(2) the recipient is a contractor/subcontractor performing emergency repairs or overhaul of items or components procured under this or a related contract to use the software to perform the repairs or overhaul made or to modify that software to reflect the repairs or overhaul made; the recipient is subject to the Use and Non-Disclosure Agreement found at DFARS § 227.7103-7(c) or is a Government contractor whose contract contains DFARS § 252.227-7025; and the Government prohibits the recipient from decompiling, disassembling or reverse-engineering the software or using software decompiled, disassembled, or reverse-engineered by the Government, or

(3) the recipient is a “covered Government support contractor” performing its covered Government support contract for use, modification, reproduction, performance, display, release or disclosure of that computer software authorized to receive restricted rights computer software provided that the covered Government support contract contains DFARS § 252.227-7025 and the Government prohibits the recipient from decompiling, disassembling or reverse engineering the software or using software decompiled, disassembled or reverse engineered by the Government for any other purpose. (DFARS § 252.227-7014(a)(15)).

5. Specifically Negotiated License Rights

Specifically Negotiated License Rights means the parties can modify the standard license rights granted to the Government or obtain rights under circumstances where the Government would ordinarily not be entitled to specific rights. The Government cannot release noncommercial technical data or computer software marked with Specifically Negotiated License Rights outside the Government unless

(1) the conditions specified in that license—which the Contracting Officer must include into the contract—have been satisfied,

(2) the recipient’s contract contains DFARS § 252.227-7025, and

(3) the recipient has signed the Use and Non-Disclosure Agreement found at DFARS § 227.7103-7(c) as modified by DFARS § 252.227-7025(b)(3). (DFARS §§ 252.227-7013(b)(4), 252.227-7014(b)(4)).
6. SBIR Data Rights

SBIR data rights means the Government acquires Limited Rights in SBIR technical data and Restricted Rights in SBIR computer software during the period commencing with contract award and ending upon the date five years after completion of the project from which that data or software were generated. (DFARS § 252.227-7018(a)(19) & (b)(4)). The SBIR Program Policy Directive states the SBIR program is structured in three phases:

- **Phase I:** Determines the scientific and technical merit and feasibility of the proposed experimental or theoretical research or research and development (R/R&D) related to agency requirements by a small business awardee prior to providing further Federal support in Phase II. SBIR Phase I awards normally do not exceed $150,000 or six months duration.
- **Phase II:** Continues the R/R&D effort from the completed Phase I. Funding is based upon the results of the work performed under a Phase I award and the scientific and technical merit, feasibility, and commercial potential of the Phase II proposal. Only Phase I awardees are eligible for a Phase II award. Phase II contracts cannot exceed $1,500,000 total costs or two years in duration.
- **Phase III:** Completes the work that derives from, extends, or completes an effort made under prior SBIR funding agreements, but is funded by sources other than the SBIR program. Phase III work is typically oriented towards commercialization of SBIR research or technology.

The SBIR Program Policy Directive states that, if an SBIR awardee receives a funding agreement—whether competed, sole-source, or subcontract—for work that derives from, extends, or completes efforts made under prior SBIR funding agreements, then the funding agreement for the new work must have all SBIR Phase III status and data rights. The Directive also emphasizes that a Federal agency may not issue an SBIR award or approve an agreement between an SBIR awardee and a Federal laboratory that violates any SBIR requirement set forth in statute or the Policy Directive, including any SBIR data rights protections. In other words, the Policy Directive takes precedence over any license rights granted to the Government under DFARS § 252.227-7018 except for those license rights described in Section V.C.1.b of this Handbook that are based upon 10 U.S.C. § 2320.

In some cases, the Government may accept less than Unlimited Rights or Government Purpose Rights in noncommercial technical data or computer software—but it cannot accept less than Limited Rights in noncommercial technical data or Restricted Rights in noncommercial computer software. Moreover, if the technical data is of a certain type, the contractor may never restrict the Government from releasing or disclosing that technical data outside the Government—and the law restricts the Government from negotiating away its Unlimited Rights to use, release, or disclose that technical data. See Section V.C.1.b of this Handbook for details.

D. Commercial Rights
Before discussing the types of rights the Government acquires in commercial technical data or computer software, the reader must first understand the definitions of the terms “commercially available off-the-shelf” (COTS) item, “commercial item”, and “commercial computer software.” Program office personnel must understand these terms and apply them correctly to whatever technical data or computer software they seek to acquire because the types of rights the Government acquires in commercial technical data or computer software are different from those rights associated with noncommercial items.

The FAR defines the term “COTS” as any item of supply that (1) is a “commercial item”, (2) is sold in *substantial quantities* in the commercial marketplace and is offered to the Government *without modification* in the same form in which it is sold in the commercial marketplace, and (3) does not include bulk cargo (*e.g.*, agricultural products, petroleum products). The FAR defines the term “commercial item” as any item of a type customarily used by the general public or by non-governmental entities for purposes other than governmental purposes that (1) has been sold, leased or licensed to the general public, (2) has been offered for sale, lease or license to the general public, (3) *evolved* from that item and will be available in the commercial marketplace in time to satisfy the Government’s delivery requirements, or (4) any item described above but for modifications of a type customarily available in the commercial marketplace or *minor* modifications not customarily available in the commercial marketplace made to meet federal Government requirements. The DFARS defines the term “commercial computer software” as software developed or regularly used for non-governmental purposes which (1) has been sold, leased or licensed to the public, (2) has been offered for sale, lease or license to the public, (3) will be available for commercial sale, lease or license in time to satisfy the delivery requirements of the contract, or (4) satisfies any of the criteria specified above and would require only *minor* modifications to meet the requirements of the contract.

Accordingly, when analyzing whether the technical data or computer software should be accepted with a commercial license, the Contracting Officer should use the following decision tree:

- Does the technical data or computer software satisfy the definition of “COTS”? For example, what quantity of those items has the contractor sold in the commercial marketplace that would constitute a “substantial” quantity? What does “without modification” mean when some items are routinely customized in the commercial marketplace? If so, the program office should then perform the analysis described in Section V.F.2.a.(9) of this Handbook.
- If not, has another contracting officer issued a commercial item determination (CID) with respect to the technical data or computer software the offeror asserts is a “commercial item” or “commercial computer software”? If so and the Contracting Officer agrees with the content of that CID, the program office should then perform the analysis described in Section V.F.2.a.(9) of this Handbook.
• If a CID exists, but the Contracting Officer believes it necessary to deviate from the that CID, can the Contracting Officer document a rationale for a different determination sufficient for the Head of the Contracting Activity (HCA) to overturn that CID?

• If no CID exists, does the technical data or computer software meet the “of a type” test? For example, are the essential characteristics—i.e., form (physical characteristics), fit (interface), function (essential purpose)—of the hardware to be acquired to which the technical data pertains substantively similar to COTS hardware? Is the primary purpose of the technical data or computer software to be procured a commercial purpose? Will the “of a type” hardware to which the technical data pertains be manufactured on the same production line as the commercial item?
  o If that technical data or computer software satisfies the “of a type” test, has that “of a type” item been customarily used by the general public or by non-governmental entities for purposes other than governmental purposes, and has it been sold, leased, or licensed to the general public or been offered for sale, lease or license to the general public? If so, the program office should perform the analysis described in Section V.F.2.a.(9) of this Handbook.

• If the technical data or computer software does not meet the “of a type” test, did that technical data or computer software evolve from a “type” of commercial item through advances in technology or performance and that is not available in the commercial marketplace but will be available in the commercial marketplace in time to satisfy the delivery requirements contained in the RFP? For example, is the technical data an updated version of technical data that one can buy in the commercial marketplace—or is the difference between those versions due to some reason other than technology or performance improvements? How far along is the hardware to which the technical data pertains in the development or manufacturing (assembly line established and tested, pieces of equipment remaining to be assembled) process? If this “evolve” test is satisfied, the program office should then perform the analysis described in Section V.F.2.a.(9) of this Handbook.

• If the technical data or computer software would have satisfied either the “of a type” or the “evolved” test but for
  o Modifications “of a type”: For example, how similar is the modified hardware to which the technical data pertains to other modified technical data sold in the commercial marketplace? Does the offeror perform similar modifications for its commercial customers? Are there differences in the manufacturing processes used to perform the modification for the Federal government and commercial customers to the hardware to which the technical data pertains? If this test is satisfied, the program office should then perform the analysis described in Section V.F.2.a.(9) of this Handbook.
  o Minor modifications of a type not customarily available in the commercial marketplace made to meet Federal Government requirements: For example, do the modifications to the hardware to which the technical
data pertains do not significantly alter the nongovernmental function or essential physical characteristics of that hardware or change the purpose of a process described in that technical data? What is the value and size of the modification and the comparative value and size of the final product? The FAR states that modifications of a commercial item are exempt from the requirement for submission of certified cost or pricing data if the total price of those modifications does not exceed the greater of $750,000 or five percent of the total price of the contract. As a result, this standard may serve as a basis for determining whether in this context the proposed modifications to commercial technical data or computer software are “minor”. If this test is satisfied, the program office should then perform the analysis described in Section V.F.2.a.(9) of this Handbook.

As stated above, the types of rights the Government acquires in commercial technical data or computer software are different from those rights associated with noncommercial items. Specifically, the Government will have the “unrestricted” right to use, release, or disclose technical data pertaining to commercial items if the technical data was previously provided without restrictions, is form/fit/function data, is a correction or change to technical data furnished to the contractor by the Government, or is necessary for operation, maintenance, installation or training purposes (other than detailed manufacturing or process data). Outside of those situations the Government may not use, release, or disclose that technical data outside of the Government unless (1) that use, release or disclosure is necessary for emergency repair/overhaul of the commercial items procured, (2) it obtains a license from the licensor to do so, or (3) the recipient is a “covered Government support contractor” performing a Government contract where that contract contains DFARS § 252.227-7025 and the “covered Government support contractor” has entered into a Non-Disclosure Agreement (NDA) with that contractor regarding the use of that data (unless the contractor has waived the requirement for an NDA in writing). (DFARS § 252.227-7015(b)).

There is no standard clause in the DFARS establishing the Government’s rights in commercial computer software, including Open Source Software (OSS). Therefore, that software must be acquired under licenses customarily provided to the public unless provisions in those licenses are inconsistent with Federal procurement law or do not otherwise satisfy user needs. (Section V.F.2.a.(9) of this Handbook provides specific examples of such provisions that the contracting parties must eliminate in the proposed contract prior to award. Appendix 1 (“Relevant Excerpts from SE&I Follow-On RFP”) of this Handbook (at Attachment 10(i)) includes an example of how to eliminate those provisions in the proposed contract.) The Government shall acquire commercial computer

---

software competitively to the maximum extent practicable using firm-fixed-price contracts or firm-fixed-priced orders under available pricing schedules.

III. Relevant Constraints

Apart from the terminology defined above, DoD’s ability to acquire rights in technical data and computer software is constrained by statute, regulation and policy. DoD policy is to acquire only that technical data and computer software, and the rights thereto, necessary to satisfy agency needs and that is consistent with Federal procurement law. (As we will discuss in detail below, one of your most important challenges is to carefully determine what those “agency needs” are.) Once the program office has identified particular items of technical data or computer software it wants to take physical possession of (regardless of what specific license rights it may need), solicitations and contracts must then specify the technical data and computer software the program office expects to be delivered. Solicitations and contracts must also establish procedures for determining the acceptability of that technical data and computer software. They must identify separate Contract Line Item Numbers (CLINs) and Exhibits for that technical data and computer software. They must require offerors to price each item separately. They must also require offerors to identify the technical data or computer software they will furnish with restrictions. Finally, they must require contractors to identify technical data and computer software they will deliver with restrictions prior to delivery.

Even if the DoD wants a contractor to deliver technical data or computer software developed exclusively at private expense, in general DoD is prohibited by statute from requiring the offeror, as a condition of being responsive to an RFP or as a condition for award, to sell or otherwise relinquish to the Government any rights in technical data related to items, components, or processes developed exclusively at private expense unless the technical data is form/fit/function data, data necessary for installation/operation/maintenance/training purposes (which would include computer software documentation)(other than detailed manufacturing process data), data that constitutes a correction or change to data furnished by the Government, data otherwise publicly available, or data that has been released by the contractor without restrictions. Similarly, the Government shall not prohibit or discourage offerors and contractors from furnishing or offering to furnish items, components, or processes developed exclusively at private expense solely because the Government’s rights to use, modify, release, reproduce, perform, display, or disclose technical data pertaining to those items may be restricted.

Regulations also prohibit DoD from requiring offerors, as a condition of being responsive to an RFP or as a condition for award, to sell or otherwise relinquish to the Government any rights in noncommercial computer software developed exclusively at private expense except for certain types of computer software specified in the DFARS. (Those certain types of computer software include corrections/changes to computer software or computer software documentation furnished to the contractor by the Government, computer software or associated documentation that is otherwise publicly available or has been released or disclosed by the contractor or its subcontractor without
restriction on further use, release or disclosure, computer software or associated
documentation obtained with Unlimited Rights under another Government contract or as a
result of negotiations, or computer software and associated documentation furnished
under another Government contract under restrictive conditions that have expired.)
Similarly, the Government shall not prohibit or discourage offerors from furnishing or
offering to furnish noncommercial computer software developed exclusively at private expense solely because the Government’s rights to use, modify, release, reproduce,
perform, display or disclose the software may be restricted.

It is permissible, however, for the program office to evaluate the extent to which an offeror proposes to furnish rights in technical data and computer software, and use the results of that evaluation during source selections provided if the RFP notifies offerors of that fact. In other words, the Source Selection Authority (SSA) may use the Source Selection Evaluation Board’s (SSEB) evaluation of the offeror’s proposal to furnish a certain level of technical data and computer software rights as part of the SSA’s tradeoff analysis to determine which offeror’s proposal provides the “best value” to the Government. However, except for the certain types of technical data identified above, the program office cannot mandate the delivery of technical data or computer software with Government Purpose Rights or Unlimited Rights. Therefore, although the DoD cannot require an offeror to sell or otherwise relinquish to the Government rights in technical data or computer software previously developed at private expense except for certain types of technical data and computer software specified above, the law does not prohibit the DoD from negotiating with offerors to purchase those rights.

A common misconception is that the Government only acquires rights in technical data or computer software if it has funded, in whole or in part, the creation of that data or software. That is not always the case. Under certain circumstances the program office may—and in some cases must—obtain Unlimited Rights even if an offeror or contractor developed the technical data or computer software exclusively at private expense.

The above discussion answers the “why” and “what” questions pertaining to the acquisition of technical data and computer software rights. But before one can turn to answering the “when” and “how” questions applicable to this subject, it is necessary to provide a brief explanation of a related systems engineering topic; namely, Modular Open Systems Approach.

IV. Modular Open System Approach (MOSA)

Over the past two decades, the DoD has become aware that the design of a weapon system’s architecture can significantly enhance the DoD’s ability to achieve agility, rapid capability enhancement, interoperability, increase competition, and lower costs over the life cycle of the program. As a result, DoDD 5000.02 mandates that a program’s systems engineering approach shall employ a MOSA where feasible. Specifically, DoDI 5000.02 Change 2 and AFI63-101/20-201 now require program managers to apply a MOSA to design development to the maximum extent feasible and cost effective 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 proprietary data. In a similar manner, DoD 5000.02 Change 2 also states that program managers must allocate cybersecurity and related system security requirements to the system architecture and design by structuring the proposed architecture so as to protect and preserve system functions or resources (e.g., through segmentation, separation, isolation, or partitioning).

A. Definitions

Recently, Congress enacted 10 U.S.C. § 2446a, which requires that all ACAT I programs that will receive Milestone A or Milestone B approval after January 1, 2019, shall be designed and developed to the maximum extent practicable with a MOSA to enable incremental development and enhance competition, innovation, and interoperability. That statute defines a MOSA as an integrated business and technical strategy employing a modular design that

- uses major system interfaces between major system components, or between major system platforms,
- is subjected to verification to ensure major system interfaces comply with—if available and suitable—widely supported and consensus-based standards,
- uses a system architecture that allows severable major system components at the appropriate level to be incrementally added, removed, or replaced throughout the life cycle of a major system platform to afford opportunities for enhanced competition and innovation while yielding (1) significant cost savings or avoidance, (2) schedule reduction, (3) opportunities for technical upgrades, (4) increased interoperability, including system of systems interoperability and mission integration, or (5) other benefits during the sustainment phase of a major weapon system, and

10 U.S.C. § 2446a defines a “major system platform” as the highest-level structure of an ACAT I 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. That statute also defines a “major system component” as 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, and
- includes a subsystem or assembly that is likely to have additional capability requirements, is likely to change because of evolving technology or threat, is needed for interoperability, facilitates incremental deployment of capabilities, or is expected to be replaced by another major system component.

10 U.S.C. § 2446a also defines a “major system interface” as
• 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 (e.g., electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software elements), and
• 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.

Publications issued by USD(AT&L) use similar terminology to describe the concepts defined in 10 U.S.C. § 2446a. Specifically, the Implementation Directive for Better Buying Power 3.0—Achieving Dominant Capabilities through Technical Excellence and Innovation, Guidelines for Creating and Maintaining a Competitive Environment for Supplies and Services in the Department of Defense and the DoD Open Systems Architecture Contract Guidebook for Program Managers, state that an open architecture is one that adopts open standards supporting a modular, loosely coupled and highly cohesive system structure that includes publishing of key interfaces within the system and full design disclosure. This architecture is based upon the following five principles:

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

The term “modular” in the first bullet is comprised of two concepts: Module Coupling and Module Cohesion. Module Coupling means that the contractor’s design will result in the creation of software items that have minimal dependencies on other items (loose coupling) to ensure that any changes to one module will not require extensive changes to other modules. Module Cohesion means that the contractor’s design will result in modules each of which feature an identifiable and discrete functionality (high cohesion). The purpose of Module Cohesion is to ensure that all that is necessary to change the performance of the system is to replace a minimum number of software items within the system that feature the increased functionality desired by the customer (“plug-and-play”).

Having described the concept of MOSA, the question then becomes to what extent that concept must be implemented in the CDD/CPD, acquisition strategy, and resulting RFP? Before answering that question, however, the program office must first create—or if they have already been created—carefully review the four resources listed below. The
reason why will become clearer to the reader after they have finished reading Sections V.A, V.B.1.b, V.B.3, V.C.1, V.C.5.b-c, V.C.7, V.C.8, V.F.2.a, V.F.2.a.(1), (2), and (8), and—last but not least—V.G.2 of this Handbook.16

For the moment, however, it will suffice to say that in some cases IP rights are allocated between the Department of Defense and its industry partners is based upon who funded the development of a particular item or component. But unless the program office understands what document memorializes the technical baseline associated with an item or component that was developed exclusively at private expense consistent with MOSA principles, it will be difficult at best for the program office to correctly analyze what level of license rights it may be able to acquire to that technical baseline—and whether the scope of the license to that technical baseline will suffice to achieve the program’s manufacturing/reproduction/maintenance/sustainment/disposal strategy for each major system component.

B. Relevant Systems Engineering Resources

The purpose of this Handbook is not to provide the reader with a graduate-level understanding of systems engineering documentation as they apply to a MOSA. Nevertheless, due to the statutory mandate in 10 U.S.C. § 2446a described above, it is critical that the reader of this Handbook have a basic familiarity with various documents so the reader will understand how they relate to the proper acquisition of IP under DoD contracts. Accordingly, the following discussion of four resources is necessarily brief. Whereas the first three resources apply to all weapons systems, the last resource applies only to software-intensive systems. These four resources are:

The program’s Systems Engineering Plan (SEP). DoDI 5000.02 Change 2 requires that program managers for all ACAT programs prepare a SEP as a management tool to guide the systems engineering activities on the program. The SEP must be submitted for approval for each milestone review. DoDI 5000.02 Change 2 states that at each milestone and at the development RFP release decision point, the SEP will support the acquisition strategy, including the program interdependencies, and communicate the overall technical approach to balance system performance, life cycle cost, and risk in addressing warfighter needs. Amongst other things, DoDI 5000.02 Change 2 states that the SEP will document “interface requirements and interface products to track interdependent touch points.”

To that end, the program manager must discuss the applicability of MOSA principles to their major system platform using DASD(SE)’s *Systems Engineering Plan (SEP) Outline Version 2.0* (June 2, 2015). In particular, paragraph 2.1 (“Architecture and Interface Control”) of that *Outline* requires that the program office list the architecture products that will be developed (including system-level physical and software architectures and Department of Defense Architecture Framework (DODAF) architectures). The expectation is that

“Architectures are generated to better describe and understand the system and how the subsystems join together, to include internal and external interfaces, to form the system. Plans to develop architecture products to support requirements and specification development are understood.”

Likewise, paragraph 4.5 (“Configuration and Change Management”) of that *Outline* requires that the program office will list and describe the planned or established technical baseline artifacts upon approval of various design reviews; *i.e.*,

- **System Functional Review = Functional Baseline =** Artifacts containing the system’s performance (functional, interoperability, and interface characteristics) and the verification required to demonstrate the achievement of those specified characteristics.
- **Preliminary Design Review = Allocated Baseline =** Artifacts containing the functional and interface characteristics for all system elements (allocated and derived from the higher-level product structure hierarchy) and the verification required to demonstrate achievement of those specified characteristics.
- **Critical Design Review = Initial Product Baseline =** Artifacts containing necessary physical (form, fit, and function) characteristics and selected functional characteristics designated for production acceptance testing and production test requirements, including “build-to” specifications for hardware (product, process, material specifications, engineering drawings, and other related data) and software (software module design – “code-to” specifications).

The expectation is that

“Programs should understand which artifacts make up each technical baseline and manage changes appropriately. At completion of the system-level Critical Design Review, the Program Manager will assume control of the initial product baseline, to the extent that the competitive environment permits (DoDI 5000.02, Enclosure 3, Para.8, page 84). Exceptions are explained.”

That paragraph also states that the program’s SEP must describe the program’s process for maintaining configuration management and control of its baselines. With
respect to the program’s configuration change process, the SEP must, amongst other things, “[d]escribe how the Intellectual Property Strategy affects and influences the planned configuration control processes.” The expectation is that

“Programs control their baselines. Configuration Management planning is consistent with the Intellectual Property Strategy.”

Finally, paragraph 4.6 (“Design Considerations”) of that Outline requires that the program office include a table that identifies fourteen different design considerations critical to the achievement of the program’s technical requirements. The description shall include the name of the design consideration, the cognizant program management organization, certification requirements, the documentation that memorializes that design consideration, how those documents are included into the contract (e.g., “CDRL #”), and a description of how the program office will address that design consideration. One of those design descriptions the table requires program offices provide is a description of

“how open systems architecture design principles support an open business model, and are incorporated into the program’s design to enable affordable change, evolutionary acquisition, and interoperability. Provide rationale if it is not feasible or cost effective to apply an open systems approach.”

The program’s WBS. MIL-STD-881C (“Department of Defense Standard Practice: Work Breakdown Structures for Defense Materiel Items”)(October 3, 2011) states that the foundation for a WBS is DoDD 5000.1 and DoDI 5000.02. According to MIL-STD-881C, the purpose of a WBS is to define the logical relationship among all program elements (e.g., hardware, software, services, data, facilities) to a specific level of indenture that does not constrain the contractor’s ability to define or manage the program and resources. (The contractor should then extend all other elements to the level and form based upon the way the system is developed, produced, or managed.) A secondary goal is to provide a systematic and standardized method for gathering cost data so that both the Government and the contractor can track the cost to develop and produce a specific item or component that resides within a specific level of the WBS so that work progress is documented as resources are allocated and expended.

Amongst other things, the WBS segregates a defense materiel item into its component parts, clarifies the relationship among the parts, and clarifies the relationship of the tasks to be completed both to each other and to the end item (weapon system). In other words, the WBS is an organized method to break down a product into sub-products at lower levels of detail (e.g., Level 1 = Space System, Level 2 = Space Vehicle 1, Level 3 = Bus, Level 4 = Bus Flight Software, Level 5 = a Computer Software Configuration Item (CSCI) (e.g., software item, software subroutine) that provides a specific functionality). When appropriately structured and used in conjunction with systems engineering principles, cost estimating, Earned Value Management (EVM), integrated scheduling, and risk management, the WBS allows for program status to be continuously
visible so the program manager and the contractor can identify, coordinate, and implement changes necessary for desired results. Since the WBS evolves during the Engineering and Manufacturing Development (EMD) phase of a program, by the end of that phase, the WBS is defined at its lowest levels, which best represents the entire system.

The program’s spare parts Acquisition Method Code/Acquisition Method Suffix Code (AMC/AMSC) assignment codes. DFARS PGI 217.7506 describes the Department of Defense’s spare parts breakout program. That program includes procedures for screening and coding parts in order to provide contracting officers with summary information regarding technical data and sources of supply to meet the Government’s minimum requirements. An AMC is a single digit numeric code assigned by a DoD activity to describe to the contracting officer and other Government personnel the results of a technical review of a part and its suitability for breakout. An AMCS is a single digit alpha code assigned by a DoD activity that provides the contracting officer and other Government personnel with engineering, manufacturing, and technical information.

In brief, the assignment of those codes assists the contracting officer in selecting the method of contracting (competitive, sole-source), identifying sources of supply (e.g., knowledge of manufacturing sources, additional operations performed after manufacture of parts possessing safety or other critical characteristics), and the availability of technical data (i.e., the adequacy of the technical data package for that spare part and the Government’s IP rights to use that technical data for acquisition purposes). As it relates to the topics discussed in this Handbook, Section 3-303.2 (“Data Evaluation Phase”) of DFARS PGI 217.7506 provides a 13-step process for determining the adequacy of that technical data, and Section 3-303.3 (“Data Completion Phase”) provides a six-step process for determining the adequacy of the IP rights retained by the contractor to that technical data.

The program’s Software Architecture Description (SAD), SMCI63-104 (“Software Acquisition Instruction”)(May 26, 2009) states that one of the 17 Contract Data Requirements Lists (CDRLs) all programs must acquire from contractors developing and delivering software-intensive systems to SMC is a SAD. Aerospace Report No. TOR-2011(8506)-117 (“Integrating Software Topics into the Request for Proposal”)(July 19, 2012) states that a SAD contains at minimum the following information:

- Diagrams indicating the software architectural components and subcomponents, and their internal and external interfaces.
- A flowdown of the system architecture to the software architecture.
- A description of the architecture modeling tool and methodologies used, e.g., DODAF, UML (OMG 2011).
- Multiple software architectural perspectives, including both models and detailed textual descriptions of the logical organization, dynamic behavior, process decomposition, and organization of the software system.
In other words, a SAD identifies the purposes (functionality) for software items used in that major system platform’s software architecture (e.g., during development, in delivered code, and for use on which systems and in which geographic locations).

C. Results Achieved By Using MOSA

If program office personnel understand what these four documents say about the systems’ architecture, they will then have a common understanding of the technical baseline and the system’s decomposition down to the lowest practicable level that can be used for their specific needs: systems engineering, cost estimating, scheduling, EVM, IP, logistics, etc. With respect to IP, armed with these four resources the program office can then determine what IP rights the Government can—if not should—acquire to the technical baseline that describes a specific major system component in order to foster competition and reduce the total life cycle cost of the major system platform. As a result, the primary deliverables the Government would acquire from a contractor whose contract required the major system platform to be developed using MOSA principles are:

- System/subsystem specifications that (1) specify the requirements (including functionality and associated test requirements) for each major system component and the major system platform that is comprised of all such components in objective, quantifiable terms, so anyone can design/develop/produce/integrate that component into that platform, and (2) require that platform be designed consistent with MOSA principles,
- System/subsystem design descriptions that describe each major system component and the major system platform that is comprised of all such components and the architectural design of each component and the platform,
- Major system interfaces between each major system component and between each major system component and the major system platform that is comprised of major system components to the appropriate level of indenture in the WBS consistent with the program’s minimum needs (e.g., its maintenance philosophy, its SEP),
- A WBS, and
- For software-intensive systems, a SAD.

Given the existence of that technical baseline, the Government would not necessarily need to acquire Government Purpose Rights to detailed manufacturing process data for the hardware or the source code residing within the major system component identified in the major system platform’s WBS/SAD. Instead, consistent with 10 U.S.C. § 2320, the Government would only need to acquire Government Purpose Rights to the deliverables listed above in order to use, release or disclose those items to sources other than the original equipment manufacturer (OEM). The Government’s disclosure of that technical baseline to alternate sources will foster competition at the major system component (in the case of software, module) level thereby precluding “vendor lock” by encouraging those sources to develop, maintain and sustain components featuring equivalent or improved functionality as the component(s) the Government seeks to replace.
The reason why is because those alternate sources will retain the right to restrict the Government’s ability to use, release, or disclose detailed manufacturing process data for the hardware or the source code residing within the major system component identified in the major system platform’s WBS/SAD to competitors in the same manner that the OEM retained the right to restrict the Government’s ability to use, release, or disclose detailed manufacturing process data for the hardware or the source code residing within the major system component identified in the major system platform’s WBS/SAD the OEM created to those alternate sources. Ultimately, both the OEM and the alternate sources—the OEM’s competitors—will be incentivized to develop, maintain and sustain equivalent or improved functionality major-system-component-by-major-system-component at a cheaper price.

Of course, the Government would still need to acquire at minimum, e.g., Limited Rights to technical data that describes, and Restricted Rights to computer software—in this case, source code—residing within, the major system component developed by either the OEM or an alternate source so the program office can complete the risk management framework process mandated by DoDI 8510.01 (“Risk Management Framework (RFM) for DoD Information Technology”) (March 12, 2014). The reason why is because, as stated in DoDI 5000.02 Change 2, undiscovered weaknesses or flaws in system elements containing software or microelectronics, including spares, can provide the foundation for threat actors to defeat fielded systems through cyber-attacks. As a result, it is imperative that the Department be able to identify and eliminate those weaknesses and flaws (1) before it places the major system platform into the warfighter’s hands, and (2) discovered after the system is fielded.

In order to properly incorporate MOSA principles into the major system platform the program office seeks to acquire, the program office must include those concepts into the CDD/CPD, the acquisition strategy, and the RFP. And the program office must analyze the extent to which offerors propose a MOSA during source selection—especially the means they intend to use to satisfy MOSA principles after award. For ease of understanding, implementation of this concept at each of those stages is discussed at the appropriate locations in the text that follows consistent with the statutory mandates that now apply to each of those documents.

We emphasize, however, that an essential condition precedent to the successful implementation of MOSA is that systems engineers, product support managers, logisticians, contracting officers, and program attorneys not only need to talk to each other earlier than may have occurred in the past—they also need to have a basic understanding of the tools and lexicon used by their colleagues’ respective professions to perform their respective jobs. The reason why is because systems engineers need to take into consideration what major system components logisticians and product support managers believe would be appropriate to repair or replace consistent with the program’s maintenance philosophy, thereby ensuring that the resulting contract requires the awardee to create components featuring minimal dependencies on other components (Module Coupling) and that that functionality is confined to a specific component (Module
Cohesion). Likewise, it is now incumbent upon contracting officers and program attorneys to understand the major system platform’s WBS and SAD.

Put another way, those communities must agree with each other regarding the expected content of system/subsystem specifications, system/subsystem design descriptions, and what major system interfaces the contract will require the contractor to create that will define the interfaces between major system components, between a major system platform and its major system components, and between major system platforms, to be repaired/replaced at the appropriate level of indenture in the WBS consistent with the program’s minimum needs as reflected in, e.g., its maintenance philosophy, its SEP. As a consequence, during development and production, the contractor will decompose the major system platform to identify where the functionality to be provided by a specific major system component will reside in the system’s architecture—the results of which will be found in the contractor’s WBS (and for software-intensive systems) and SAD.

V. The “Cradle-to-Grave” Approach

Having answered the “why” and “what” questions pertaining to the acquisition of technical data and computer software rights—and having taken a temporary detour to discuss MOSA principles and related programmatic documentation—the following pages answer the “when” and “how” questions by describing a cradle-to-grave approach to acquiring sufficient rights in technical data and computer software to permit the program office to successfully execute a program. This approach begins with the program office’s formulation of the CDD/CPD, through drafting the acquisition strategy, through drafting provisions of the RFP, through competitive or sole-source negotiations, through the ultimate use, release and disclosure of those deliverables to non-Government employees after award of the resulting contract.

A. Drafting The Capability Development Document (CDD)/Capability Production Document (CPD)

Sustainment planning early during design and procurement enables the requirements and acquisition communities to provide a system with optimal availability and reliability to the warfighter at an affordable life cycle cost. That is why the Manual for the Operation of the Joint Capabilities Integration and Development Systems (JCIDS) (February 12, 2015, including errata as of December 18, 2015) requires that (1) all CDDs/CPDs contain a Sustainment Key Performance Parameter (KPP) consisting of Materiel Availability and Operational Availability components—including supporting Reliability and Operations and Support (O&S) Cost Key System Attributes (KSA)—and (2) all other system attributes not identified elsewhere in CDDs/CPDs that tend to affect life cycle cost should be identified in CDDs/CPDs. Neither that publication nor AFI10-601 (“Operational Capability Requirements Development”) (November 6, 2013), however, requires that those critical documents identify what technical data and computer software and their associated license rights the program office must acquire to successfully execute the program from development through disposal. That fact is surprising given that acquisition of technical data and computer software (and their associated rights) can
be a critical factor in reducing the program’s total life cycle cost. Fortunately, however, AFPAM63-128 (“Integrated Life Cycle Management”)(July 10, 2014) now summarizes the concepts discussed below.

Although there are different ways of analyzing what rights the program office should acquire, as explained below, it all starts with the program office determining what critical technical data or computer software the contractor must delivered to the program office. Next, the program office must determine, consistent with 10 U.S.C. §§ 2320-2321, which specific persons or entities will need to use those critical items for which specific purposes (e.g., depot level maintenance, follow-on competitive acquisitions) for specified periods in order to identify what rights need to be acquired for those deliverables. Ideally, the program manager should be able to summarize the results of this analysis in no more than a paragraph of text in the CDD/CPD—clearly identified in the table of contents under the heading “Rights in Technical Data and Computer Software”—that identifies those items and their associated license rights. That paragraph should also explain why the requirements community needs those items and their associated license rights to enable the system’s materiel and operational availability.

And now, thanks to 10 U.S.C. § 2446b, the CDD/CPD must also identify and characterize

- the extent to which requirements for system performance are likely to evolve during the life cycle of the system because of evolving technology, threat, or interoperability needs, and
- for requirements that are expected to evolve, the minimum acceptable capability that is necessary for initial operating capability of the ACAT I program.

In other words, CDD/CPDs must now address the applicability of MOSA principles to the major system platform being procured under that program.

We have identified five reasons why it is imperative that this summary of the Government’s needs for critical technical data or computer software and the rights thereto, along with a discussion of the applicability of MOSA principles to the major system platform being procured under the program, into those critical requirements documents, be included in CDDs/CPDs. First, AFI63-101/20-101 states that all acquisition programs will coordinate the requirements document (e.g., Systems Requirements Document) used in conjunction with an RFP with the requiring Lead Command prior to the release of the final RFP and directs the reader’s attention to MIL-HDBK-520A (“Systems Requirements Document Guidance”)(December 19, 2011) for additional information on preparation of requirements documents. In turn, MIL-HDBK-520A indicates that requirements documents must specify technical data and computer software requirements. Thus, inclusion of those requirements into the CDD/CPD will increase consistency between the RFP and the CDD/CPD insofar as identification of critical technical data and computer software and associated license rights are concerned.
Second, AFI63-101/20-101 states that the Commander, Air Force Space Command, will, along with the Service Acquisition Executive (SAF/AQ), certify to the SECAF that the requirements as described in the CDD for ACAT I, ACAT IA and non-delegated ACAT II space programs can, amongst other things, be translated for evaluation in a source selection in a clear and ambiguous way. That instruction also requires that source selections consider Government rights to data. Accordingly, inclusion of requirements for the acquisition of technical data and computer software (and their associated rights) into the CDD/CPD will ensure that, once the RFP is finalized, the latter mandate can be executed consistent with the former mandate.

Third, the Competition In Contracting Act (CICA) requires that the program office demonstrate that the requirements it ultimately included in a RFP are reasonably necessary for the Air Force to meet its minimum needs. In theory, a bid protester can challenge any requirement as unduly restrictive of competition. If, however, the CDD/CPD contains the information described above, it is likely that a bid protest forum (e.g., Government Accountability Office (GAO), U.S. Court of Federal Claims (COFC), U.S. Court of Appeals for the Federal Circuit (CAFC)) will give the determination made by the Vice Chairman of the Joint Chiefs of Staff in the CDD/CPD regarding what rights in technical data and computer software they need to accomplish the mission great weight—especially if the reasonable explanation for needing that technical data and computer software and their associated license rights is included into the CDD/CPD.

Fourth, if the requirements community includes its summary of its minimum needs and their rationale into the CDD/CPD, any successor program manager will find it difficult to relax those requirements after the Government has awarded the contract. Situations where a relaxation of requirements might be contemplated would include the program manager erroneously assuming that that relaxation will reduce the total ownership cost of the program or the contractor experiencing “seller’s remorse” (described in Section V.H.1 below) with respect to the rights it agreed prior to award to deliver to the program office after award.) The reason why is because that program manager will be unable to relax those contract requirements unless and until those requirements are deleted from the CDD/CPD by the Vice Chairman of the Joint Chiefs of Staff. In other words, including those requirements in the CDD/CPD puts the program manager in a strong position to resist pressure originating from any source to relax them.

Finally, the Government can maximize the materiel and operational availability of that system by requiring the contractor to deliver critical technical data and computer software needed to maintain that system within an area of operation overseas by either government personnel or support services contractors, and the associated license rights needed to provide those items to those personnel or contractors. If, however, the Government never required the delivery of those critical items or failed to acquire the appropriate license rights to use, release and disclose those items to those government personnel or contractors, when that system breaks down, the user will have no choice but to ship it back to the OEM in the United States. The user must then wait the weeks (if not
months) it will take that manufacturer to repair that system and return it to that area of operation.

B. Formulating the Acquisition Strategy

Recently, Congress mandated that acquisition strategies for ACAT I/II programs shall consider the IP strategy in accordance with 10 U.S.C. § 2320 (10 U.S.C. § 2431a). This mandate is implemented by DoDI 5000.02 Change 2.

Specifically, DoDI 5000.02 Change 2 states that every acquisition strategy must address how program management will create and sustain a competitive environment throughout the program's life cycle. With respect to IP rights, that regulation requires program management establish and maintain an IP strategy to 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. (In this regard, DoDI 5000.02 Change 2 states that a life cycle affordability analysis should nominally cover 30-40 years into the future. Of course, certain weapons systems in DoD's inventory (e.g., B-52, U-2, CVN-68) have been in operational use longer than 40 years.) The IP Strategy must describe, at a minimum, how program management will assess program needs for, and acquire competitively whenever possible, the IP deliverables and associated license rights necessary for competitive and affordable acquisition and sustainment over the entire product life cycle, including by integrating, for all systems, the IP planning elements required by DFARS § 207.106 (S-70) for ACAT I and II programs and subsystems thereof. (That subsection of the DFARS requires that acquisition strategies assess the long-term technical data and software needs for those programs and subsystems prior to issuing an RFP for that system or subsystem, address the merits of including a priced option for the future delivery of technical data, computer software and associated license rights that were not acquired upon initial contract award, and address the potential for changes in the sustainment plan over the life cycle of that system or subsystem.) The program manager must update the IP Strategy throughout the entire product life cycle, summarize it in the acquisition strategy, and present that document along with the LCSP during the Operations and Support Phase.

Along the same lines, AFI63-101/20-101 states that the IP Strategy describing the acquisition of technical data and associated rights for the system’s total life cycle sustainment must be addressed and documented at Acquisition Strategy Panels, reviews, and in associated data planning documents. Specifically, AFI63-101/20-101 states that data rights requirements and corresponding acquisition strategies must ensure they provide for rights or delivery of data the Government requires for systems sustainment and to maintain competition throughout the life cycle (e.g., organic source of repair and/or supply decisions, Government Core depot maintenance capability requirements, expeditionary logistics footprint requirements, engineering data requirements needed for OSSE&E assurance, integrity programs, sustaining engineering, reliability management and configuration management, technical orders, reprocurement/modification/upgrade, demilitarization/disposal, MOSA, cybersecurity strategies, technology refreshment or
enhancement, training and training program information, spare parts procurement, testing and evaluation, intelligence mission data production, contractor logistics support, supply chain management, depot-level repairable and consumables procurement, support equipment procurement and maintenance, special tools/tooling, diminishing manufacturing sources and material shortages). Conversely, the MDA must approve the business case analysis justifying the decision not to acquire licenses or associated IP rights necessary for organic support. The program manager must also ensure that the program acquires computer software as executable code and source code unless the MDA documents and approves the rationale for not doing so.

For services acquisitions, DoDI 5000.74 states that acquisition strategies for those acquisitions will provide appropriate mechanisms to identify and manage intellectual property issues to allow industry a fair and reasonable return on investment while avoiding vendor lock, and enable the competitive and cost-effective transition to follow-on service providers. Where competition is determined not to be feasible or practical, acquisition strategies and plans will incorporate processes to generate improved performance or cost savings with the sole source vendor, such as incentives and performance metrics.

For business systems—i.e., information systems operated by, for, or on behalf of the DoD (e.g., financial systems, financial data feeder systems, contracting systems, logistics systems, planning and budgeting systems, installation management systems, human resources management systems, and training systems) that are not national security systems or information systems used exclusively by and within the defense commissary system or the exchange system or other instrumentality of the DoD conducted for the morale, welfare, and recreation of members of the armed forces using non-appropriated funds—DoDI 5000.75 states that the tailored acquisition strategy shall include a description of the program approach to leverage competition to acquire the required capability at reduced cost and risk. As a result, the approach for acquiring those business systems must describe the business strategy that includes an intellectual property strategy.

Before the program office begins to implement those statutory and regulatory mandates by drafting the acquisition strategy for a specific program, however, all personnel who will be assigned to the resulting source selection or sole-source acquisition who will evaluate an offeror’s proposal relative to technical data and computer software rights should first read DFARS Subparts 227.71 and 227.72 and the related clauses for themselves so they will possess an intimate familiarity with pertinent terminology. (A copy of the DFARS is available on-line at http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html.) Second, those personnel should address the topics discussed below. Although some of these topics are not discussed anywhere in the DFARS, resolving them when drafting the acquisition strategy is critical to minimizing disagreements between the contracting parties after award and increasing the probability the program office will achieve the objectives of the acquisition. These topics are discussed in the context of what information should be included into the program office’s acquisition strategy to comply with paragraph 7.6 of PDUSD(AT&L)’s
You may notice that some of these topics relate to how the program office should structure various sections of the RFP. The reason why these topics are discussed in this section is because PDUSD(AT&L)’s memorandum of June 23, 2011 states that prior to Milestones B and C the program office must submit their acquisition strategy accompanied by the RFP for all ACAT I-IV programs. In a similar manner, USD(AT&L) memorandum of May 7, 2015 requires that a development RFP review be conducted prior to that RFP’s release decision point and as otherwise directed for programs for which the Defense Acquisition Executive is the Milestone Decision Authority. As a result, program offices seeking approval of their acquisition strategy should commence drafting that document at the same time they are drafting their RFP. With that caution in mind, the following text describes what information the program office should insert into the pertinent subparagraphs of paragraph 7.6 of its acquisition strategy—and what analysis the program office will need to perform to complete that task.

1. Subparagraph 7.6.1

This subparagraph of the program’s acquisition strategy must include an analysis of the data required to design, manufacture and sustain the system as well as to support re-competition for production, sustainment, or upgrade and consider baseline documentation data, analysis data, cost data, test data, results of reviews, engineering data, drawings, models, and Bills of Materials.

To comply with this mandate, in accordance with the DFARS, the acquisition strategy should identify the long-term technical data, computer software, and cost/financial/schedule data needs of the program to achieve the program’s objectives (and identify those objectives) and how those needs were assessed. It should consider the needs of the entire life cycle, including potential competition/re-competition for procurement of the system, subsystems, components, and logistics support (including spare and repair parts), e.g., the potential for changes in the sustainment plan over the life cycle of the weapon system or subsystem. Put another way, the program office should assume that the OEM will not maintain or sustain the system.

To complete this task, the program office must identify in the acquisition strategy what deliverables (Contract Data Requirements List (CDRLs)) will be included into the RFP. The most efficient way to do so is to initiate the data call required by DoD 5010.12-M (“Procedures for the Acquisition and Management of Technical Data”)(May 1993). The purpose of that data call is to solicit answers from systems and software engineers, logisticians, cost analysts, and requirements personnel internal and external to the program office to the following questions based upon the unique nature of the supplies or services being acquired and how those supplies or services will be used:

a. What critical technical data and computer software—if any—does the CDD/CPD require the program office to acquire from the contractor? Although not all
CDDs or CPDs may contain such requirements, the program office should not assume that those documents omit mention of that topic. Those requirements may be buried on some obscure page, the existence of which is not explicitly stated in the table of contents underneath a heading (e.g., “Software Engineering”) that does not contain helpful terminology like “technical data and computer software.” Accordingly, the program office must carefully scrutinize each page of the CDD or CPD for those requirements.

b. Based upon its review of the program’s SEP, WBS, and spare parts AMC/AMSC assignment codes (if already issued), what technical data that describes the technical baseline for each major system component, the major system interfaces between major system components, between the major system platform and its major system components, and between that platform and other major system platforms, will the program office need for the total life cycle of the program?

c. What data (including technical data and computer software) will the program office need to acquire to develop and produce the weapon system? For example, consistent with SMCl63-104, systems and software engineers will recommend acquiring deliverables like engineering change proposals, system/subsystem specifications, system/subsystem design descriptions, WBSs, design review data packages, test plans, test procedures, test reports, software development plans, software product specifications, SADs, system safety program plans, environmental analysis data reports, and Integrated Master Schedules (IMS). Cost analysts will recommend acquiring Cost Performance Reports, Design-to-Cost/Life-Cycle Cost and Variance Analysis Reports, and Functional Cost-Hour and Progress Curve Reports.

d. What technical data and computer software will the program office need to maintain, sustain, and dispose of the weapon system? For example, logisticians will recommend acquiring ICDs, technical orders, training manuals, and product drawings/models and associated lists.

Based upon the answers to these questions, the program office should include a comprehensive list of proposed CDRLs into this subparagraph of the acquisition strategy. Next, as required by the FAR, the program office should identify the estimated cost of those CDRLs and their delivery schedules. Finally, the program office should describe how it will store, manage, and review those CDRLs for technical accuracy and completeness—and who (e.g., the program’s Engineering Data Manager) will be responsible for ensuring those activities are performed.

2. Subparagraph 7.6.2

This subparagraph of the program’s acquisition strategy must explain how the program will provide for rights and delivery of technical data the program office requires for the system’s total life cycle sustainment (e.g., material management, training, cybersecurity, cataloging, open architecture, configuration management, engineering,
technology refreshment, maintenance/repair within the technical order (TO) limits and specifically engineered outside of TO limits, reliability management).

To address this mandate, the acquisition strategy must identify the rights the program office will acquire to the CDRLs—including the extent to which those rights will support future competition—described in subparagraph 7.6.1 of the acquisition strategy. In other words, it should address the potential for changes in the sustainment plan over the life cycle of the weapon system or subsystem. Put another way, the program office should acquire sufficient rights so it will not need the OEM to maintain or sustain the system. To do so, the program office should address the following issues:

a. The program office must procure those rights the Government is required to acquire by 10 U.S.C. § 2320, DFARS Subparts 227.71 and 227.72, DoDI 5000.02 Change 2, AFI63-101/20-101, and SMCI63-104. Section V.C.1.b below provides further details regarding the rights 10 U.S.C. § 2320, DFARS Subparts 227.71 and 227.72 require the Government to procure. The rights the other resources cited in the preceding sentence require the program office to procure are discussed in the following paragraphs.

b. To comply with DoDI 5000.02 Change 2/AFI63-101 for hardware-/software-intensive systems, DoDI 5000.74 for services acquisitions, and DoDI 5000.75 for business systems, the program office must take into consideration the unique nature of the goods or services it seeks to acquire. In this regard, it is worth noting that some program offices attempt to solve this problem by having their development/production contractors agree to so-called “enabling” provisions in Statements of Work/Performance Work Statements (SOW/PWS). Such “enabling” provisions require those contractors provide a program office’s support services contractors “access” to various types of technical, financial and schedule data. Although this is a type of license (since it attempts to identify who can have “access” for what purposes for a specified period), such provisions are a questionable solution to the problem of properly acquiring rights in technical data and computer software for two reasons.

First, the license rights used by the DFARS clauses described above do not use the term “access”—they are phrased in terms of “use”, “release” and “disclosure” restrictions associated with deliverables. It is unclear why a program office would want to become embroiled in litigation regarding whether the vague term “access” is synonymous with those terms—or whether, according to Webster’s Dictionary, that term should be interpreted to mean anything from “an attack or onset of illness or disease”, to “a fit or spell of intense feeling”, “permission, liberty, or ability to enter, approach, communicate with, or pass to and from”, etc. Second, if a development/production contractor is providing those support services contractors “access”, then the contractor is providing that “access” directly to a support services contractor. In other words, use of those agreements may erode the program office’s control of the program since it takes the program office “out-of-the-loop” because the program office is no longer the sole conduit of that technical data and computer software between that contractor and its support services contractor. And if the recipient provides comments on that technical data or computer software to which it has had “access” back to the contractor, those comments
may not have been approved by the program office—but nevertheless might be construed by the contractor as a constructive change to its contract. (For further details regarding the concept of a constructive change, please see Government Contract Law for Engineers.)

The preceding examples demonstrate why the program office must determine what technical data and computer software rights are needed to sustain the system and its subsystems over their life cycle (e.g., development, production, testing, installation, operation, maintenance, upgrade/modification, interoperability with other systems, transfer of technologies to other programs/systems/platforms) when drafting the acquisition strategy for that system. In order to make this determination, the program office must analyze to whom does the program office want to release or disclose specific items of technical data and computer software (i.e., CDRLs) listed in paragraph 7.6.1 of its draft acquisition strategy, for what purposes, and for what specified period.

For example, does the weapon system’s maintenance/sustainment philosophy as reflected in the system’s LCSP state the program office plans to competitively procure additional quantities of the system, spare parts, or future system upgrades/modifications? Does the LCSP state the program office will have services contractors perform organic sustainment of the system? Does the LCSP state the Government will compete on-orbit anomaly resolution of bus flight software? Is the current producer unable to satisfy surge requirements? If so, the program office should acquire Government Purpose Rights to that technical data or computer software.

In contrast, does the program office want to use, release or disclose that technical data to only Government employees for organic sustainment? In the alternative, does the program office need that technical data to perform only emergency repair and overhaul (as opposed to routine repair and overhaul) of the system? If so, the program office should acquire Limited Rights.

Do contractors performing services (not supply) contracts need that computer software to diagnose and correct deficiencies in a computer program or to modify computer software to enable a computer program to be combined with, adapted to, or merged with other computer programs or when necessary to respond to urgent (as opposed to routine) tactical situations if additional restrictions are satisfied? Or do contractors need that computer software to perform only emergency— as opposed to routine—repairs or overhaul of items or components thereof to use that software when necessary to perform the repairs or overhaul or modify the software to reflect the repairs or overhaul if additional restrictions are satisfied? If either is the case, the program office should acquire Restricted Rights.

Does the program office want to modify the standard license rights granted to the Government, need additional rights in technical data or computer software acquired with Government Purpose, Limited or Restricted Rights, or does the program office want to obtain rights in technical data or computer software in which it does not have rights? If so, it will need to acquire a Specifically Negotiated License.
c. The program office must attempt to procure the rights required by the program’s CDD or CPD. Although not all CDDs or CPDs may contain such requirements, the program office should not assume that those documents omit mention of that topic. As suggested above, those requirements may be buried on some obscure page, the existence of which is not explicitly stated in the table of contents underneath a heading (e.g., “Software Engineering”) that does not contain helpful terminology like “Data Rights.” Accordingly, the program office must carefully scrutinize each page of the CDD or CPD for those requirements.

d. The program office must ultimately structure RFP provisions in a manner that will make it extremely difficult for a contractor to change the basis of the parties’ bargain after award. By way of explanation, DFARS clauses in the contract permit the contractor to assert after award additional use, release or disclosure restrictions when those restrictions are based upon “new information” or “inadvertent omissions” “unless the inadvertent omissions would have materially affected the source selection decision.” If the program office structured the RFP in the manner recommended in Section V.C. below, it will be difficult for a contractor to make those assertions after award. The reason why is that the program office will be able prove the negative: It will be able to point to contemporaneous records proving that, had the program office known of those additional restrictions prior to award, those omissions would have materially affected the source selection decision. (Those records would include, but not be limited to, admissions by the awardee contained in its responses to Evaluation Notices the Contracting Officer issued to the offeror during discussions, videotaped discussion sessions, and specific language in the SSEB Report, Source Selection Advisory Council (SSAC) Report, or Source Selection Decision Document (SSDD) that supported the award of the contract in question.) Conversely, if the program office fails to carefully structure the RFP in that manner, the contractor can (and may) drive the proverbial truck through this exception.

e. The provisions the program office ultimately includes in the RFP must be unambiguous and therefore enforceable. To that end, the program office must ensure that those provisions precisely identify what specific CDRLs the Government may use, release or disclose to which specific persons/entities who are not Government employees, for which specific purposes, and for which specific period—otherwise known as “mapping” various licenses to applicable CDRLs. The reason why is because if the program office does not “map” licenses to specific CDRLs in the RFP, the program office will have difficulty analyzing whether the proposed licenses satisfy its minimum needs prior to award. Moreover, for the reasons discussed below, if licenses are not “mapped” to specific CDRLs in the resulting contract the program office will find it virtually impossible to successfully complete that “mapping” exercise after contract award.

f. The program could experience adverse consequences if the program office uses some novel approach to acquire technical data and computer software rights for an ACAT I program (i.e., any program that will require an eventual total expenditure for RTD&E of more than $365 million in FY00 constant dollars or more than $2.19 billion in FY00 constant dollars of procurement appropriations). It is therefore preferable for a
program office to include provisions in the RFP that have been battle-tested in a program of similar magnitude. For example, when considering that program of similar magnitude, the evidence demonstrates that those provisions minimized if not eliminated disagreements between the parties during contract administration. That is not to say, however, that a “one-size-fits-all” approach is appropriate. Each program has unique characteristics that the program office must take into consideration when it is formulating its acquisition strategy and the resulting RFP.

g. DoDI 5000.02 Change 2 states that a program manager will ensure ergonomics, human factors engineering, and cognitive engineering are employed during systems engineering over the life of the program to provide for effective human-machine interfaces and to meet human systems integration requirements. That publication also states that systems designs will minimize or eliminate system characteristics that require excessive cognitive, physical, or sensory skills, entail extensive training or workload-intensive tasks, result in mission-critical errors, or produce safety or health hazards.

We submit this principle applies equally to structuring data rights provisions in RFPs. For decades, some program offices and their contractors have repeatedly violated this fundamental principle of systems engineering by including cumbersome and confusing data rights provisions into RFPs and contracts—when they should have instead included provisions that are as user-friendly as an Apple© iPhone used by a teenager (or an AK-47 wielded by (regrettably) a child soldier). In other words, when drafting those provisions the program office should consider the following “human [data rights] integration” requirements:

1. They must be structured to permit the SSEB to quickly identify potential licensing problems associated with a specific CDRL contained in an offeror’s proposal.

2. They must take into consideration the program office’s personnel constraints (i.e., the lack of specialized training provided to program office personnel on this subject). In other words, upon receipt of a CDRL deliverable after award, a Second Lieutenant or a support services contractor employee should be able to compare the restrictive marking to the contract requirements and provide his/her assessment to the Contracting Officer regarding whether the marking is consistent with contract requirements within 30 seconds. In contrast, a program office violates a fundamental principle of error-free design when it awards a contract which establishes numerous types of Specifically Negotiated License Rights, each of which grant 20+ categories of entities/personnel (“communities of interest”) differing levels of use, release, or disclosure rights to vaguely-identified items of technical data or computer software that are not expressly “mapped” to specific CDRL deliverables: “Simplify where you can, and build in constraints to block errors.”

resulting contract will obscure what rights the Government actually acquired and thus exponentially increase the risk of unauthorized releases of trade secrets. Similarly, licensing approaches that make it impossible for program attorneys to figure out what rights were acquired for any item of technical data or computer software (i.e., CDRL)—unless a great deal of technical assistance is provided by program office engineers—are a waste of resources. In short, the program office should baseline all contents of a specific CDRL to a single level of license rights to the maximum extent practicable in the RFP.

(3). They must not require audit assistance to resolve disputes between the contractor and the program office regarding what rights the program office acquired under a particular contract. By way of background, except as indicated below, the DFARS states that the level of rights the Government acquires depends upon the source of the funding used to develop the noncommercial technical data or computer software in question (otherwise known as the “doctrine of segregability”). This “source of funding” test means that the Government acquires

- Unlimited Rights to noncommercial technical data pertaining to an item, component, or process or computer software that has been or will be developed exclusively with Government funds,
- Government Purpose Rights to noncommercial technical data pertaining to an item, component, or process or computer software developed with mixed funding,
- Limited Rights to noncommercial technical data pertaining to an item, component, or process developed exclusively at private expense, and
- Restricted Rights to noncommercial computer software developed exclusively at private expense.

The DFARS permits “segregation” in a contractor’s accounting system of the cost to develop technical data pertaining to items, components or processes to any practicable sub-item or sub-component level of the WBS, or any segregable portion of a process. For computer software, “segregation” would apply to a software item that performs a specific function. Therefore, if the program office merely includes the standard DFARS clauses into the contract and a dispute arises between the parties after award regarding what type of rights the Government acquired to a particular item, component or process, or a software item that performs a specific function, the program office will need to request audit assistance.

During the audit, the auditor will need to analyze the extent to which the contractor (1) developed an accounting system capable of tracking the allocation of private and government funds to the developmental work accomplished with those funds, (2) identified technologies that offered long-term competitive advantages worthy of the initial investment to develop them, and (3) broke or separated the accounting trail for development of those technologies to indirect cost pools (e.g., Independent Research and Development (IR&D)), costs not allocated to a government contract, or any combination thereof. If the contractor properly implemented these steps, the contractor can demonstrate that it developed a particular item, component or process (or all items,
components or processes) described in a particular CDRL exclusively at private expense.\textsuperscript{18} The program office would have to obtain an estimate from the auditor regarding when the program office should expect to receive that incurred cost audit report. Only upon receipt of that audit report might the program office receive a nasty surprise: The contractor’s position is unassailable—and therefore the program office will not receive the rights in technical data and computer software it assumed would be the case.

Complicating the matter further would be if the audit report concludes that the contractor developed some noncommercial items, components or processes described in that CDRL exclusively at private expense (\textit{e.g.}, IR&D), it developed other noncommercial items, components or processes with both contractor and Government funding (“mixed funding”), and it developed yet other noncommercial items, components or processes exclusively with Government funds. Accordingly, differing levels of license rights would apply to various portions of a particular CDRL—which means that only certain individuals could see certain portions of that CDRL. (That situation would violate the pragmatic rule described above: To the maximum extent practicable, the program office should ensure that all content of a specific CDRL is governed by a single level of license rights.) In contrast, if the program office uses the framework discussed below, the issue of the source of funding used to develop a particular item, component or process becomes completely irrelevant. The reason why is because all that matters is the content of the license(s) (otherwise known as Specifically Negotiated License Rights) attached to the contract which the parties agreed prior to award would apply to that specific CDRL.

One final point bears mentioning before leaving this discussion regarding the doctrine of segregability. The reader may have noticed the preceding discussion omits any reference to obtaining audit assistance from the Defense Contract Audit Agency (DCAA). The reason why is because that agency’s \textit{Contract Audit Manual} states that, although its auditors can verify that the amount claimed by the contractor as the cost of developing the proposed technical data, and can evaluate information regarding sales of the technical data to other parties if those sales have occurred, the auditor cannot determine if the costs incurred under a claimed project or account relate only to the proposed data. Nor can the auditor determine if there were other costs related to the data that were incurred under additional projects or accounts, or be reasonably certain regarding whether any specific contract required development of some or all of the proposed data. As a result, the auditor will be unable to render an informed opinion regarding the reasonableness of the contractor’s proposed price for data rights.

\textsuperscript{4} If feasible, the program office should include provisions in the RFP that obtain an express waiver from the contractor for “covered Government support contractors” to enter into any non-disclosure agreements (NDA) between the contractor and the program office’s “covered Government support contractor” relating to any Limited/Restricted Rights noncommercial technical data or computer software and commercial technical data and computer software the contractor will deliver under the resulting contract. If that is not feasible, those provisions should ensure that any NDA

does not impose impermissible terms and conditions upon those “covered Government support contractors.” (A “covered Government support contractor” is a contractor (other than a litigation support contractor covered by DFARS § 252.204-7014) under a contract the primary purpose of which is to furnish independent and impartial advice or technical assistance directly to the Government in support of the Government’s management and oversight of a program or effort, so long as the contractor is not affiliated with the prime contractor, a first-tier subcontractor on the program or effort, or any direct competitor of that prime contractor or any first-tier subcontractor, and receives access to technical data or computer software for performance of a Government contract that includes DFARS § 252.227-7025.)

For example, they should not prescribe the use of terms (i.e., restrictive markings) on technical data or computer software CDRL deliverables sent from the contractor to the program office’s “covered Government support contractors” that are different from those terms described above. Moreover, they should not require the transfer of technical data and computer software directly from the contractor to the program office’s “covered Government support contractors.” The reason why is because if they do, those NDAs may erode the program office’s control of the program since it takes the program office “out-of-the-loop” because the program office is no longer the sole conduit of that technical data and computer software between that contractor and its support services contractor—potentially resulting in the adverse consequences described above. Furthermore, they should not be so restrictive as to prevent that “covered Government support contractor” from warning other programs about systemic problems of which it is aware associated with the contractor’s performance (of the subject contract) that might arise on those other programs—such text might violate FAR § 52.203-19 (“Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements”).

After the program office has used the criteria described above, it should summarize in subparagraph 7.6.2 of its acquisition strategy the level(s) of rights it believes it must acquire to the CDRLs listed in subparagraph 7.6.1 along with the logic it used to select the level(s) of rights it did and the alternative solutions considered. Subparagraph 7.6.2 should also list or summarize the DFARS clauses that will be included into the resulting contract(s) (including the Deferred Ordering and Deferred Delivery clauses), and identify the estimated cost of the rights to those CDRLs as required by the FAR. That subparagraph should also describe the overall approach to managing data the program office will acquire with less than unlimited rights and how data deliverables will be reviewed for unjustified or nonconforming markings. It should describe the process the program will follow to question or challenge contractor assertions or markings, and the approach for maintaining the software and its related documentation once software maintenance is transferred from the original equipment manufacturer (including contract provisions that will allow for a cost-effective migration). It should describe the use of withholding or incentives specific to performance in the area of data management (e.g., heavily-weighted award fee plan subjective evaluation criteria to incentivize the contractor to deliver CDRLs with conforming and justified restrictive markings, withholding payment of up to 10% of the total contract price if technical data is not delivered in a timely manner or is deficient upon delivery). It should describe how the use of an Integrated Data/Digital
Environment (IDE) (see Section V.D below) factors into the IP Strategy, any required interfaces to government data systems or repositories, how those requirements will be satisfied, and the digital format standards to be used and why they were selected.

3. Subparagraph 7.6.3

This subparagraph of the program’s acquisition strategy must include a business case analysis calculation, conducted in concert with the engineering tradeoff analysis, which outlines the approach for using MOSA and acquiring technical data rights. This calculation must analyze alternative acquisition decisions to provide evidence that justifies an investment decision to implement (or not implement) an MOSA or acquiring (or not acquiring) rights in technical data and computer software for the program. It must take into consideration the contractor’s economic interest in technical data and computer software pertaining to items, components or processes that potential offerors have developed at private expense. It must also consider the Government’s costs to acquire, maintain, store, retrieve and protect the data, as well as procurement needs, repair/maintenance/overhaul philosophies, spare/repair part considerations, and whether procurement of the items, components or processes can be accomplished on a form, fit or function basis.

As best as can be determined—given the lack of detailed guidance that exists on this topic—this analysis consists of four parts:

a. Using the program’s SEP, WBS, SAD, and spare parts AMC/AMSC assignment codes, decompose the major system platform down to its major system components. Then, as required by 10 U.S.C. § 2446b, to the maximum extent practicable,

- clearly describe the MOSA to be used for the program,
- differentiate between the major system platform and major system components being developed under the program, as well as major system components developed outside the program that will be integrated into the ACAT I program,
- clearly describe the evolution of major system components the program office anticipates will be added, removed, or replaced in subsequent increments,
- identify additional major system components that may be added later in the life cycle of the major system platform,
- clearly describe how IP and related issues—e.g., technical data deliverables—that are necessary to support a MOSA will be addressed, and
- clearly describe the approach to systems integration and systems-level configuration management to ensure mission and information assurance.

b. Analyze the contractor’s economic interest in the technical data that describes the technical baseline for those major system components that potential offerors developed exclusively at private expense. Specifically, the program office should perform market research by, e.g., issuing presolicitation notices requesting potential offerors identify what technical data or computer software they have developed exclusively at private expense would be contained in a CDRL deliverable, what license
rights they contemplate delivering to the Government, and what would be the price they might charge to deliver a higher level of license rights than that which they contemplate delivering to the Government.

c. Analyze the Government’s costs to acquire, maintain, store, retrieve and protect the data, repair/maintenance/overhaul philosophies, spare/repair parts considerations, and whether procurement of major system components can be accomplished by acquiring the system/subsystem specifications to those components and to the major system platform, and related major system interfaces. In other words, the program office must analyze the basis of its maintenance philosophy and what is the potential that philosophy may change. If, for example, the program’s Source of Repair Assignment Process (SORAP) determines that various major system components residing within the major system platform cannot be repaired but instead must be replaced for the foreseeable future, it is unlikely the program office could justify acquiring Government Purpose Rights to a full design disclosure technical data package for those components as its minimum need. In contrast, the program office will need to acquire Limited Rights to the Critical Design Review data package for those components so the program office and its covered government support contractors can analyze the design details and manufacturing processes for that component for, e.g., single-point failures.

d. Compare the results of item b. to item c. to justify an investment decision to implement (or not implement) an MOSA or acquire (or not acquire) rights in technical data and computer software for the program.

4. Subparagraph 7.6.4

This subparagraph of the program’s acquisition strategy must include a cost-benefit analysis of including a priced contract option for the future delivery of technical data and IP rights not acquired upon initial contract award. For example:

- Based upon its technology readiness assessment, the program office determines whether critical technology elements will mature to the extent that a component that cannot be repaired at present can be repaired by a depot-level maintenance facility in the future.
- The requirements community can be convinced over time that a company other than the software developer can deliver software patches/updates of equivalent quality at a cheaper price.
- The program office will acquire Unlimited/Unrestricted Rights to all technical data and computer software needed for the life cycle of the weapon system as part of the basic contract.

5. Subparagraph 7.6.5

This subparagraph of the program’s acquisition strategy must include an analysis of the risk that the contractor may assert limitations on the government’s use and release of data, including IR&D-funded data (e.g., require the contractor to declare IR&D up front
and establish a review process for proprietary data). In other words, the program office should analyze the difference ("gap") between those minimum needs it has identified for the contemplated acquisition in subparagraphs 7.6.1 and 7.6.2 of its draft acquisition strategy and those rights in technical data and computer software associated with items, components or processes for any components or subsystems of that weapon system the Government already acquired under existing contracts. Note that the level of system decomposition used in performing this analysis should be consistent with the program’s SEP, WBS and LCSP for the contemplated acquisition.

To determine what rights the Government currently possesses, the program office should carefully review the following six sources of information:

- Copies of all relevant contracts.
- Copies of FAR/DFARS standard clauses incorporated by reference into those contracts. Note that by the time that analysis commences, the program office might have difficulty obtaining a copy of those clauses if those regulations have been revised to include a more current version of those clauses or those clauses have been deleted from the FAR/DFARS. The law library of the Office of the Staff Judge Advocate contains hard copies of superseded versions of those clauses.
- Copies of any asserted rights restrictions made by the contractor prior to award in its completed DFARS § 252.227-7017 certification/representation.
- Copies of technical data/computer software (i.e., CDRLs) delivered under predecessor contracts, as the restrictive marking on the cover page of those CDRLs should indicate what use, release and disclosure restrictions apply to those CDRLs.
- If the CDRLs did not contain technical data which by law the Government was entitled to receive Unlimited Rights, the program office should request the contractor provide its accounting records that identifies the sources of funding used to develop the items, components, or processes associated with the technical data or computer software delivered via those CDRLs. For further details, see Section V.G.4.c.(1) below.
- Copies of any Contract Performance Reports (CPR) submitted to the Government under any Government contract that may identify the sources of funding used to develop the items, components or processes associated with the technical data or computer software delivered via those CDRLs. The relevance of those CPRs will be directly proportional to the level of detail contained in the WBS appended to that Government contract. For example, the contract’s WBS extended down to the level of the item/component described in that CDRL so that the information contained in those CPRs proves that data was in reality developed exclusively at Government expense.

The results of this analysis will lead the program office to one of three conclusions:

- The contractor will not assert any limitations.
- The contractor will assert limitations that are unjustified.
• The contractor will assert limitations that are valid.

In the first situation, the program office would summarize its analysis in subparagraph 7.6.5 of its acquisition strategy. In the second situation, the program office should formally challenge those limitations as described in Section V.H.3 below. In the third situation, the program office should summarize its analysis in subparagraph 7.6.5 of its acquisition strategy—and in its sole-source justification and approval (J&A) document as described in Section V.G.3 below.

C. Drafting the Request for Proposals (RFP)

As stated above, AFI63-101/20-101 requires that source selections consider Government rights to data and include priced options that correspond to the data and data rights recommended as part of the IP Strategy. That instruction, however, does not provide detailed guidance on how to structure an RFP in order to implement that mandate. Experience has demonstrated that merely incorporating by reference standard DFARS clauses will not suffice to identify and resolve critical technical data and computer software rights issues prior to and after award. For example, the DFARS requires that program offices include into their RFPs a provision that offerors use to identify use, release and disclosure restrictions (DFARS § 252.227-7017). That provision, however, does not require that the offeror "map" those restrictions to specific CDRLs. If the program office does not correct this omission prior to award, the program office may not have a defensible position regarding whether the restrictive markings the contractor affixed to a particular CDRL prior to delivery are consistent with contract requirements.

Similarly, as stated above, even though military departments encourage contractors to deliver COTS software, no clauses establish the Government’s rights in that commercial computer software. If a program office encourages the delivery of that COTS software but fails to read and incorporate the relevant license agreement(s) into the contract prior to award, it may be in for an unpleasant surprise after award. Specifically, it may realize the license(s) prevent(s) the use, release or disclosure of that software to certain entities to which it must release that software in order to execute successfully the program.

Accordingly, what follows is a structured approach for drafting the relevant sections of the RFP consistent with the Uniform Contract Format (UCF) contained in the FAR that, if implemented, should minimize the probability that the program office will acquire insufficient rights in technical data and computer software to execute successfully an acquisition program. This approach is not the only manner in which a program office could structure an RFP to achieve that objective. (Note, however, that various program offices have successfully used the framework described below on a Navy ACAT I program and multiple Air Force ACAT I programs. For further details, see Appendices 2 and 3.) Any other approach that satisfies all objectives described above in Section V.B. would be equally acceptable. Again, however, experience demonstrates that unless the program office implements an approach similar to that described above from the outset, it may be forced into having protracted discussion sessions with offerors that take much more time.
than would otherwise have been the case had the RFP been properly structured in the first place (not to mention multiple RFP amendments). That situation, of course, will cause delays in award of the resulting contract.

1. **Exhibit A (Contract Data Requirements List)(CDRL)**

   **a. The “acquisition reform” experiment—and its offspring**

   One school of thought which held court during the “acquisition reform” heyday of the 1990s—and which may be reemerging from the Sebonian Bog—asserts that a reduction in the number of CDRLs will dramatically reduce the (initial) cost of the weapon system. In retrospect, the consequences of implementing that approach should have come as no surprise: the contractors wrote few documents; they did not provide those documents in a timely manner; and the Government had much less authority to require improved documentation when the products omitted necessary content. Deficient documentation then resulted in late, inadequate weapon systems needing rework to improve them so the Air Force could field those weapon systems. Contracts awarded based in part upon that school of thought experienced substantial cost overruns in the years that followed—including, in some cases, multiple Nunn-McCurdy breaches. Moreover, in some cases, the Air Force could not perform anomaly resolution activities and resolve pertinent issues during Safety Investigation Boards (SIB) in order to determine the most probable root cause of an on-orbit failure of a satellite. In sum, the offspring of that school of thought was that the Government lacked necessary insight into the weapon system, its quality, and overall progress.

   That school of thought failed then—and fails now—to consider a basic principle of systems engineering: No weapon system ever magically appeared on-demand in the warfighter’s hands as an Immaculate Conception. Before the developer can manufacture any component of any of the subsystems of that weapon system, the developer must create documentation that accurately describes the product baseline. And during the manufacture of that weapon system, the developer must create documentation that accurately describes the product (as-built) baseline and the final (as-built) configuration. That is why Aerospace Report No. TOR-2006(8506)-5738 (“Recommended Software-Related Contract Deliverables for National Security Space System Programs”)(February 14, 2008) states that successful (software) development depends upon having the necessary system, segment, subsystem, and element CDRLs items in place.

   Like nature, competent accountants cannot be fooled. Even if the regulatory mandates described below did not exist, a program office must still spend money having the contractor create documentation that accurately describes the product (as-built) baseline and the final (as-built) configuration in order to successfully design, develop, manufacture, deploy, sustain/maintain and dispose of a weapon system.

---

19 Report to the President by the Presidential Commission on the Space Shuttle Challenger Accident, Appendix F (“Personal Observations on Reliability of Shuttle” by R.P. Feynman) p. F-5 (June 6, 1987) (“[f]or a successful technology, reality must take precedence over public relations, for nature cannot be fooled”), available at [http://history.nasa.gov/rogersrep/v2appf.htm](http://history.nasa.gov/rogersrep/v2appf.htm).
In other words, the free lunch does not exist. The lunch must be prepared and served. The only question is who will pick up the tab.

During the “acquisition reform” heyday of the 1990s, program offices also attempted to convey the impression to senior leadership that they had managed to square the circle. They would still acquire the technical data and computer software necessary to successfully execute the program while at the same time dramatically reducing the number of CDRLs. How did they do that? They started using the Data Accession List (DAL) CDRL as the proverbial “kitchen sink” into which all of their known requirements for technical data or computer software could be poured. In doing so, they disregarded two facts.

First, the very text of the Data Item Description (DID) for a DAL (DI-MGMT-81453A) warns that a program office is not authorized to use the DAL in that manner: The DAL “is not a substitute for standard data requirements that are contractually applied.” The reason why the DoD does not authorize misusing the DAL in that manner is because the DAL is nothing more than a list of technical data and computer software the contractor decided to and ultimately created during contract performance. The DAL does not describe in detail the content of any technical data or computer software the program office will require the contractor to deliver after award that is listed on the DAL.

A fundamental principle of government contracting is that in a competitive environment an RFP must provide for the submission of proposals based upon a common understanding of the agency’s requirements. Since the DAL does not accurately describe the content of each item of technical data or computer software the program office expects the contractor will deliver to it after contract award, it is impossible for a common understanding to exist between all offerors and the Government as to that content. As a result, the Government will be unable to negotiate a fair and reasonable price for that data. Some offerors may underbid not realizing what the Government’s content needs are. Other offerors may overprice assuming that the Government will require delivery of all items the contractor will eventually list on the DAL.

Second, the DAL states that the list “shall also identify the Government Rights to the data using the following codes: ‘GPR’ = Government Purpose Rights[;] ‘UR’ = Unlimited Rights[;] ‘LR’ = Limited Rights[;] ‘RR’ = Restricted Rights (Computer Software only).” This language basically permits a contractor to unilaterally determine what license rights the Government will acquire to those items listed on the DAL after award—as opposed to the Government knowing prior to award what rights it will acquire to each item of technical data or computer software that is the subject of its own DD Form 1423. In short, a program office that seeks to use the DAL in that manner is like a real estate developer whose standard practice is to use the butt-end of a screwdriver to hammer nails to build commercial and residential properties: It is possible—but the adverse consequences could be catastrophic.
b. The “back-to-basics” approach

After having read the above discussion you should now understand why program offices should reject the “acquisition reform” approach and get “back-to-basics” by strictly complying with official DoD mandates that have existed for decades. Specifically, DoD 5010.12-M, the DFARS, and the SMC IG require that program offices acquire technical data under DoD contracts via a DD Form 1423 (CDRL). Similarly, the military departments acquire computer software and cost/financial/schedule information via DD Form 1423. (The DoD uses DD Form 1423 to assist in defining delivery obligations, not to establish the Government’s rights to use, release or disclose the delivered IP outside the Government.) This approach properly bounds the scope of the technical data and computer software that the contractor will deliver to the program office. Moreover, the Warranty of Data clause in the resulting contract (DFARS § 252.246-7001) states that the warranty period extends for three years after completion of the delivery of the line item of data “as identified in DD Form 1423, Contract Data Requirements List. . . .” As a result, if the program office did not acquire a particular item of technical data “identified in [a] DD Form 1423” it is doubtful whether the program office acquired a warranty to that data.

Accordingly, the first step the program office should take when drafting the RFP so that it will properly acquire rights in technical data and computer software is to create the appropriate CDRLs. (As explained in Sections IV and V.C.5.b below, CDRLs in Exhibit A would include the WBS and WBS dictionary, system/subsystem specifications (DI-IPSC-81431A), system/subsystem design descriptions (DI-IPSC-81432A), and—for software-intensive systems—the SAD. Appendix D of Aerospace Report No. TOR-2011(8506)-117 provides the recommended content and format of a SAD. The program office would copy that text into the CDRL for that deliverable incorporated by reference into Exhibit A of the RFP.) Creating the appropriate CDRLs includes ensuring the content of those CDRLs—including any tailoring of referenced Data Item Descriptions (DIDs)—encompasses the universe of all technical data, computer software, or both, that the program office desires the contractor to deliver after award. And where the ACAT I program will implement MOSA principles, 10 U.S.C. § 2320 states that major system interfaces—i.e., between a major system platform and a major system component, between major system components, or between major system platforms—must be expressly identified in the RFP (i.e., as DD Form 1423 CDRLs).

To that end, the content of a CDRL could—and may very well need to be—component-specific. For example, if the WBS for a major system platform is written to the

---

20 A DID is a form that defines the intended use, preparation instructions and content and format requirements for a specific data product. The ASSIST database (https://assist.dla.mil/online/login/mainframe.cfm) is the official source for DoD specifications and standards (e.g., DIDs). If one does not know the Document ID number for a DID (e.g., “DI-IPSC-81441A”) or the words in the title of the DID (e.g., “Software Product Specification”), we recommend the reader consult the DID Selector in the ASSIST database. That resource helps users locate active DIDs that have been identified for priority consideration by subject matter experts within each Military Department. Users may search for DIDs that will require the delivery of data or computer software to efficiently and cost effectively operate and support weapons systems throughout their acquisition and logistics life cycle by Product Support Elements, by common WBS elements, or by Standardization Areas.
fifth level of indenture, the DD Form 1423 could require the contractor to deliver a separate Design Review Data Package (DI-ILSS-81335) CDRL for each major system component at that level of indenture residing within the system. Similarly, to implement MOSA principles, the DD Form 1423 could require the contractor to deliver separate Interface Control Document (ICD) (DI-SESS-81248B), Interface Requirements Specification (DI-IPSC-81434A), and Interface Design Description (DI-IPSC-81436A) CDRLs that describe the interfaces between

- each major system component and all other major system components, and
- the interface between each major system component and the major system platform in which that component resides.

As indicated in Sections V.B.2.e., V.B.2.g.(2), and V.C.5.g., this approach would facilitate “mapping” of licenses to each deliverable and baselining license rights to a single level per CDRL.

We hasten to add that one should not read the phrase “high-level” as that phrase is used in the definition of “major system component” in 10 U.S.C. § 2446a as meaning the program office may only acquire major system interfaces between items at the third level of indenture of the WBS (e.g., an interface between a satellite bus and a payload). Instead, the primary consideration that should govern what major system interface CDRLs between major system components residing within the major system platform the program office will require the contractor to deliver via Exhibit A—irrespective of the level of indenture of the WBS at which those major system components will reside—are the program’s minimum needs as reflected in, e.g., its maintenance philosophy, its SEP.

The best way to complete the task of creating appropriate CDRLs is to convene the Data Requirements Review Board (DRRB) described in DoD 5010.12-M (“Procedures for Acquisition and Management of Technical Data”) (May 14, 1993). The co-chairs of the DRRB should be the program manager and the Contracting Officer. Attendees should include all CDRL authors (e.g., business financial managers, engineers, logisticians). During the DRRB, the author of the CDRL should explain:

- Why the program office needs that CDRL.
- Why delivery of the proposed content is required (e.g., the tailoring of that CDRL is consistent with the DID invoked by that CDRL, the author used the Queen’s English properly).
- Where in the SOW/PWS is the tasking statement that requires the development/production and delivery to the Government of that CDRL.
- Why “approval” (vice “review”) of that CDRL is required.

In other words, if the program office fails to describe in a particular CDRL that item of technical data or computer software, that item may not be a deliverable. As a result, the program office may not acquire any license to use, release or disclose that item to non-Government employees for any purpose whatsoever.
We note in-house counsel for some defense contractors cannot even agree amongst themselves whether the Government acquires rights to various items of technical data—that the contract did not classify as a “deliverable” via a DD Form 1423—where the Government only acquired electronic “access” via some type of IDE. In other words, neither in-house counsel—nor, for that matter, academia—agree whether delivery must occur before the DoD acquires IP rights to the content of that technical data or computer software. These facts strongly counsel in favor of a program office making every scrap of technical data, computer software, and cost/financial/schedule data the program office needs to successfully execute the program throughout its life cycle the subject of a DD Form 1423—thereby neatly circumventing the need for the program office to extricate itself from this legal quagmire after award. The program office should also include a sentence at the beginning of Block 16 of the DD Form 1423 that states whether the CDRL requires the delivery of technical data, computer software, both technical data and computer software, or neither technical data nor computer software.

Next, the program office should review the content of the SOW paragraph, the tailored DID, and any compliance documents invoked by each CDRL and then answer the following questions to determine the technical data/computer software rights associated with that CDRL to which the Government may be entitled. (Thus, if Exhibit A of Section J of the RFP contains 120 CDRLs, the program office must repeat the following analysis 120 times.)

If those sources describe noncommercial technical data, is it (1) form/fit/function data, (2) data necessary for installation/operation/maintenance/training purposes (which would include computer software documentation)(other than detailed manufacturing process data), (3) data that constitutes a correction or change to data furnished by the Government, or (4) data otherwise publicly available or has been released by the contractor without restrictions? If that technical data fits within any of those categories, the program office should acquire Unlimited Rights in that technical data unless the program office determines that its minimum needs may be satisfied by acquiring a level of license rights (i.e., Specifically Negotiated License Rights) no lower than Limited Rights. In making this determination, the program office must remember that, when agreeing to a lower level of license rights, it cannot surrender rights below the level of Government Purpose Rights if relinquishment would unduly restrict future competition.

To reiterate, with respect to one type of form/fit/function data—major system interfaces between an item or process and other items or processes necessary for the segregation of an item or process from, or the reintegration of that item or process (or a physically or functionally equivalent item or process) with, other items or processes in a MOSA—10 U.S.C. § 2320 states that the Government shall have Government Purpose Rights in that type of technical data developed exclusively at private expense or with mixed funding except where negotiation of different rights in that technical data would be in the best interest of the Government. And if that type of technical data was developed exclusively at private expense, the program office must negotiate with the contractor the appropriate and reasonable compensation for that technical data. For details in this regard, see Section V.G.4 below.
If not, does that noncommercial technical data pertain to (1) studies, analyses, test data or similar data produced in the performance of a contract where that study, analysis, test data or similar work was specified as an element of performance, (2) data that the Government has obtained Unlimited Rights under another Government contract or as a result of negotiations, or (3) data furnished under another Government contract with Government Purpose Rights or Limited Rights and the restrictive condition(s) has/have expired? If that technical data fits within any of those categories, the program office should acquire Unlimited Rights in that technical data unless the program office determines that its minimum needs may be satisfied by acquiring a level of license rights (i.e., Specifically Negotiated License Rights) no lower than Limited Rights.

If those sources describe noncommercial technical data that does not fit within the enumerated categories listed above, will the contractor develop that item exclusively with Government funds? If so, the program office should acquire Unlimited Rights in that technical data unless it has determined that its minimum needs will be satisfied by acquiring a level of license rights (i.e., Specifically Negotiated License Rights) no lower than Limited Rights. If not, will the contractor develop that item in part with Government funds? If so, the program office should acquire Government Purpose Rights in that technical data unless it has determined that its minimum needs may be satisfied by acquiring a level of license rights (i.e., Specifically Negotiated License Rights) no lower than Limited Rights. In making this determination, the program office must remember that, when agreeing to a lower level of license rights, it cannot surrender rights below the level of Government Purpose Rights if relinquishment would unduly restrict future competition.

If those sources describe commercial technical data, is it (1) form/fit/function data, (2) data necessary for installation/operation/maintenance/training purposes (which would include computer software documentation)(other than detailed manufacturing process data), (3) data that constitutes a correction or change to data furnished by the Government, or (4) data otherwise publicly available or has been released by the contractor without restrictions? If so, consistent with 10 U.S.C. § 2320, the program office should acquire Unrestricted Rights in that technical data unless it has determined that its minimum needs may be satisfied by acquiring a lower level of license rights. In making this determination, the program office must remember that, when agreeing to a lower level of license rights, it cannot surrender rights below the level that is equivalent to Government Purpose Rights if relinquishment would unduly restrict future competition.

If those sources describe noncommercial computer software, is it (1) corrections/changes to computer software furnished to the contractor by the Government, (2) computer software that is otherwise publicly available or has been released or disclosed by the contractor or its subcontractor without restriction on further use, release or disclosure, (3) computer software obtained with Unlimited Rights under another Government contract or as a result of negotiations, or (4) computer software furnished under another Government contract under restrictive conditions that have expired? If so, the program office should acquire Unlimited Rights in that noncommercial computer software unless it has determined that its minimum needs may be satisfied by acquiring
a lower level of license rights. If not, will the contractor develop that item in part with Government funds? If so, the program office should acquire Government Purpose Rights in that noncommercial computer software unless it has determined that its minimum needs may be satisfied by acquiring a level of license rights (i.e., Specifically Negotiated License Rights) no lower than Restricted Rights.

If those sources describe noncommercial computer software that does not fit within the enumerated categories above, will the contractor develop that item exclusively with Government funds? If so, the program office should acquire Government Purpose Rights in that noncommercial computer software unless it has determined that its minimum needs may be satisfied by acquiring a level of license rights (i.e., Specifically Negotiated License Rights) no lower than Restricted Rights. If not, will the contractor develop that item in part with Government funds? If so, the program office should acquire Government Purpose Rights unless it has determined that its minimum needs will be satisfied by acquiring a level of license rights (i.e., Specifically Negotiated License Rights) no lower than Restricted Rights.

If those sources describe commercial computer software, what rights to use, release, or disclose that software outside the Government does the program office need to acquire? Irrespective of the answer to that question, are the proposed rights inconsistent with Federal procurement law?

2. Section B (Supplies Or Services And Prices/Costs)

When the Government awards a contract that includes the appropriate DFARS clauses, the contract price should include the price for the allocation of rights specified by those clauses (irrespective of whether the rights the contractor proposes to grant to the Government are based upon which entity funded the development of a particular item, component or process). For the reasons stated above, however, it is prudent to structure the contract to require the offeror to expressly identify the cost/price the Government will have to pay to acquire those rights and let competition (if competition exists) encourage the offeror to propose to deliver those rights at no additional cost/price.

Accordingly, the contractor should identify the cost/price for the delivery of the technical data or computer software (e.g., the work involved in copying the data to a compact disc and mailing that disc to the Government) under a CLIN other than the CLIN it uses to identify the cost/price for the rights to use, release or disclose that technical data or computer software. The DFARS states that acquisition plans should address the merits of including a priced contract option for the future delivery of rights in technical data and computer software that the program office will not acquire upon initial contract award. Similarly, the instructions provided on the back of the DD Form 1423 for filling out Block 18 (“Estimated Total Price”) state that the cost/price for data itself is different from the cost/price associated with the rights to use, release or disclose that data outside the Government:

“[f]or each data item, enter an amount equal to that portion of the total price which is estimated to be attributable to the
production or development for the Government of that item of data. These estimated data prices shall be developed only from those costs which will be incurred as a direct result of the requirement to supply the data, over and above those costs which would otherwise be incurred in performance of the contract if no data were required. The estimated data prices shall not include any amount for rights in data. The Government’s right to use the data shall be governed by the pertinent provisions of the contract [emphasis added].”

In certain cases, the Government may be already paying for the development of the technical data or computer software but not have determined whether it needs that IP delivered to it. Accordingly, Contracting Officers should include the appropriate DFARS clause into Section I regarding future ordering of that technical data and create an additional firm-fixed-price option CLIN for delivery of technical data and computer software that addresses potential delivery costs (i.e., the cost of reproduction and delivery).

In contrast, the Government may be requiring delivery of that technical data or computer software via CDRLs. For example, SMC RFPs usually allocate the cost of creating that technical data and computer software to “Not Separately Priced” “Data and Reports” CLINs associated with various hardware CLINs. The Government’s assumption that the contractor will develop and deliver certain items of technical data or computer software as part of a CDRL exclusively at its expense—and therefore the Government will receive a certain level of rights to use that CDRL—may be incorrect. Conversely, its assumption that the contractor will develop and deliver certain items of technical data or computer software as part of a CDRL exclusively at private expense—and therefore it will receive a different level of rights to use that CDRL—may likewise be incorrect.

Accordingly, to assist the SSEB in determining which assumption is correct, the Contracting Officer should consider creating an additional firm-fixed-price option CLIN entitled “Rights in Data (Including Technical Data, Computer Software, and Computer Software Documentation).” That option CLIN will in turn reference pricing tables contained in a Section J attachment of the RFP entitled “Rights in Data (Including Technical Data, Computer Software, and Computer Software Documentation)” (hereinafter “Data Rights Attachment”). Although at first blush creating a separately-priced option for those rights would appear to result in the Government paying twice for that IP—once under the CLIN under which that IP was developed, and a second time upon exercising the option for the rights in that IP—that is not necessarily the case given competitive constraints. In other words, a properly structured RFP will incentivize offerors to not put themselves at a competitive disadvantage. In any case, the SSEB should be sensitive to this issue and be prepared to address it through discussions should this situation arise.

3. Section H (Special Contract Requirements)
a. If the contractor is delivering computer software under a fixed-price CLIN, the program office should consider acquiring a warranty for that software. In contrast, if the contractor will be delivering the computer software under a cost-reimbursable CLIN, the Government may not obtain a warranty for that software.

b. If the program office has included a fixed-price Option CLIN into Section B for Rights in Data (Including Technical Data, Computer Software, and Computer Software Documentation), it must include an option exercise clause that states the Government may exercise the option in whole or in part from the date of contract award through the end of the period of performance of the contract. In other words, the program office can exercise an option for a certain level of rights associated with a specific CDRL upon obligation of the amount indicated in Table 1 of the Data Rights Attachment (described below).

AFI65-601V1 ("Budget Guidance and Procedures") (August 16, 2012) states that the source of funds to procure and print technical data depends upon the appropriation that funded the acquisition of the end item of equipment or systems to which the technical data is applicable. We can therefore logically conclude that the appropriation used to acquire the rights in technical data or software should be the same as the appropriation used to fund the creation of that technical data or software. Accordingly, the option exercise clause should state that the Contracting Officer will obligate the same type of appropriations onto that CLIN to procure rights in technical data, computer software or computer software documentation to be delivered as part of a CDRL as that appropriation they obligated to procure that item and that is current in the year an option is exercised for the rights in that item.

c. Many DoD contracts incorporate by reference all Section K certifications/representations the offeror completed via a Section I clause (i.e., FAR § 52.204-19 ("Incorporation by Reference of Representations and Certifications"), including those completed electronically via the System for Award Management. FAR § 52.204-7 ("System for Award Management") (SAM) requires offerors to complete certifications/representations in the SAM database. FAR § 52.204-13 ("System for Award Management Maintenance") requires contractors to update that information on an annual basis to ensure it is current, accurate, and complete. One of the provisions in the SAM database is FAR § 52.227-15 ("Representation of Limited Rights Data and Restricted Computer Software").

The FAR and the DFARS state that FAR data rights clauses do not apply to DoD contracts. Moreover, FAR § 52.204-13 states that updating information in the SAM database does not alter the terms and conditions of the contract. But that language would not appear to affect any restrictions the offeror submitted to that database prior to award. Accordingly, the Contracting Officer should include language into a Section H clause stating that none of the restrictions an offeror may have submitted into the SAM database in response to FAR § 52.227-15 will apply to the acquisition in question.
4. Section I (Contract Clauses)

Incorporate by reference all technical data and computer software clauses required by the DFARS, including DFARS § 252.246-7001 ("Warranty of Data").

5. Section J (List of Attachments)

a. Indicate that the offeror’s completed DFARS § 252.227-7017 certification/representation (see below) will be an attachment to the resulting contract.

b. Exhibit A. Include all CDRLs. The CDRLs should include a WBS/WBS dictionary, system/subsystem specifications, system/subsystem design descriptions, and (for software-intensive systems) a SAD. In accordance with 10 U.S.C. § 2446b, Exhibit A should also include ICD CDRLs between the major system platform and its components, between all major system components, and between major system platforms to the appropriate level of indenture in the WBS consistent with the program’s minimum needs (e.g., the program’s maintenance philosophy).

c. WBS. In accordance with 10 U.S.C. § 2446b, the WBS must identify the minimum set of major system components that must be included in the design of that program.

d. SOW (MIL-HDBK-245D)/PWS.

(1). As required by SMC IG5315.470-90, the SOW/PWS should contain tasking statements that require the development/production and delivery of CDRLs contained in Exhibit A. If a program office fails to do so, the development costs for the relevant technology can be shifted to an indirect cost pool, and by being so shifted, can leave the Government with fewer rights than otherwise expected. This risk is particularly relevant in light of a recent judicial interpretation of a sentence buried in a cost principle—the Independent Research and Development and Bid and Proposal (IR&D/B&P) Costs cost principle (FAR § 31.205-18) that governs the allowability of costs incurred under Government contracts. The sentence in question defines what IR&D is—and what it is not. Specifically, that cost principle states that “[t]he term does not include the costs of effort sponsored by a grant or required in the performance of a contract.”

Based upon its review of the nearly 40-year-long disagreement between the DoD and its industry partners, the CAFC decided that “required in the performance of a contract” means “specifically required” by that contract. (In contrast, the DCAA’s Selected Area of Cost Guidebook: FAR 31.205 Cost Principles states that auditors must ensure that contractors do not include costs in the IR&D cost pools for developmental efforts “that are specifically required in the performance of a contract or those efforts that are not explicitly stated in the contract, but are necessary to perform the contract.”) Therefore, unless the contract specifically requires development or production of a specific item of noncommercial technical data or computer software in the performance of the contract, the cost for those items could be allocated to an indirect cost pool (e.g., IR&D) so that—
based upon the funding rules described above—the Government acquired only Limited or Restricted Rights, respectively to that technical data or computer software.

Given this judicial interpretation of the IR&D cost principle, program offices would be well-advised to include tasking statements required by SMC IG5315.470-90 into the SOW/PWS that clarify that the development or production of that item of noncommercial technical data or computer software was specifically required in the performance of the contract. For example, depending upon the type of appropriation used to fund the development or production of that item, a tasking statement would be phrased as follows: “The contractor shall develop and deliver a Critical Design Review data package (CDRL A0XX)”, or “The contractor shall produce and deliver a Systems Engineering Management Plan (CDRL A0XX)”.

One additional benefit of this approach is that, consistent with SMC IG5315.470-90(e), a CDRL will exist in Exhibit A associated with every such tasking statement contained in the SOW/PWS. As a result, the program office will have built bi-directional traceability into its contract, thereby easing the burden of contract administration. The reason why is that the instructions for filling-in BLK 5 of the DD Form 1423 require the author identify what SOW/PWS paragraph requires the creation of that item of technical data, computer software, or cost/schedule/financial data—thereby making it easier for the reader to quickly find that paragraph in the SOW/PWS. In a similar fashion, adding the parenthetical proposed above just after the tasking statement in the SOW/PWS makes it easier for the reader to quickly find in Exhibit A the DD Form 1423 that describes the content of the deliverable mentioned in that SOW paragraph.

(2). In order to diagnose on-orbit anomalies on the ground, it is essential that the software portion of firmware delivered as part of the end item be identical to that contained in a CDRL. Accordingly, the program office should include a sentence into the SOW/PWS that states the software portion of firmware delivered as part of an end item (e.g., space vehicle, launch vehicle) must be identical to that contained in a CDRL.

(3). Include a sentence into the SOW/PWS that requires the contractor ensure that there is no functionality in the reusable software that would inhibit operation unless explicitly specified and approved by the Government (e.g., the periodic need to enter in a license code, the presence of a physical key or similar device to enforce licensing limitations).

e. Performance specification (MIL-STD-961E Change 3)/System requirements document (MIL-HDBK-520A). Where the ACAT I program will implement MOSA principles, to implement 10 U.S.C. § 2446b the performance specification/system requirements document shall describe the MOSA to which the contractor's design must comply.

f. Compliance and Reference Document List. The purpose of this document is to identify all documents the contractor must comply with during performance of the contract, as well as all documents that the contractor may use as guidance for which the
primary audience is the program office. In this case, the list of reference documents should include the SEP for the reasons described in Section IV.B above.

9. Include a Data Rights Attachment (see Appendix 1 (“Relevant Excerpts from SEI Follow-On RFP”) Attachment 10). Within this attachment resides the heart of the program office’s approach to acquiring rights in technical data and computer software. Specifically, this attachment contains three tables that separate the rights the program office will acquire to (1) noncommercial technical data and computer software, (2) commercial technical data and computer software, and (3) cost/financial/schedule data from each other.

In negotiated procurements, clearly stated solicitation requirements are considered material to the needs of the Government. Thus the primary purpose of this attachment is to make it clear to all offerors that the program office’s need to acquire certain types of rights to specific deliverables is a material term and condition of the solicitation. As a result, the failure of an offeror’s proposal to conform to those terms and conditions is unacceptable and cannot form the basis for award. (Material terms of a solicitation are those that affect the price, quantity, quality, or delivery of the supplies or services being provided.) More specifically, the primary purpose of these tables is—as stated in Section V.B.2.e & g.(2) of this Handbook—to identify what license rights the program office will acquire to each CDRL (“mapping”) and to baseline all contents of a specific CDRL to a single level of license rights to the maximum extent practicable. This attachment also contains other conditions that apply to this subject as follows:

(1). Table 1 consists of four columns (i.e., “CDRL Number,” “Data Item Title (Subtitle),” “Asserted Rights Category”, “Price” or “Estimated Cost”) and a quantity of rows equal to the number of CDRLs. The program office must fill-in the first and second columns using the information in Exhibit A. Based upon the answers provided to the questions listed in Section V.B.2 and V.C.1. of this Handbook, the program office must fill-in the third column with either “Unlimited” or “Offeror to Complete.” (If a Specifically Negotiated License will satisfy the program office’s needs, then the program office should instead identify that concept in the table.) The offeror will fill-in the third column for each level of rights associated with each CDRL. If a Specifically Negotiated License will satisfy the program office’s needs, the program office—with the program attorney’s assistance—must clearly specify the scope of that license (i.e., identify specific persons/entities to whom that CDRL may be released or disclosed to for what specific purposes and for what specified period). In other words, the program office must fill-in the third column based upon a careful analysis of its minimum license requirements for a specific CDRL.

(2). Table 2 identifies any commercial technical data and computer software the contractor will deliver to the program office. It presupposes that, although the end item being procured is not itself a commercial item (e.g., F-35), and many items included in that end item are likewise not commercial items, various commercial items will be included in that end item delivered to the Government that in and of themselves satisfy the legal definition of a commercial item. This table will contain five columns (i.e., “CDRL Number” (or, for firmware delivered as part of a hardware item, “CLIN Number”), “Data Item Title
(Subtitle)” (or, for firmware delivered as part of a hardware item, “CLIN Noun Description”), "Vendor Name, Technical Data/Software Application Name, License No.", “Quantity” of licenses (if applicable), “Price” or “Estimated Cost”)) and rows equal to the number of CDRLs and CLINs that will contain that commercial technical data and computer software. It is unlikely the program office will know under what CDRL or CLIN the offeror will deliver each item of commercial technical data associated with each commercial hardware component, and under what CDRL or CLIN the offeror will deliver each commercial software item or subroutine to the program office. Therefore—in contrast to Table 1—the offeror will fill-in all five columns.

(3). Military departments invariably acquire other types of data via CDRLs that do not fall within the definition of “technical data” or “computer software” described above (e.g., Design-to-Cost/Life Cycle Cost and Variance Analysis Report, Cost Data Summary Report, IMS). As a result, the program office acquires no rights to use, release or disclose that data outside the Government to support service contractors because the licensing provisions in the DFARS discussed above do not apply to that data. Accordingly, if that data must be used, released or disclosed to those contractors so the program office can successfully execute the program, the attachment should describe the license the program office will acquire to use, release or disclose that data to those contractors for enumerated purposes for what specified period. To that end, Table 3 identifies any cost/financial/schedule data the contractor will deliver to the program office. This table should contain three columns (i.e., “CDRL Number”, “Data Item Title (Subtitle)”, “Price” or “Estimated Cost”) and rows equal to the number of CDRLs that will contain that data. The program office must fill-in the first and second columns and the offeror will fill-in the third column.

(4). Many program offices procure systems via contracts that contain both fixed-price and cost-reimbursable CLINs. To prevent cost migration between various cost-reimbursable CLINs and between cost-reimbursable and firm-fixed price CLINs, the attachment should mandate how the contractor must allocate costs for various licenses procured under various CLINs in reasonable proportion to the benefits received by each CLIN.

(5). In many cases, the contractor will deliver firmware as a part of an end item (e.g., space vehicle, launch vehicle) under the resulting contract. Accordingly, the attachment should state that all licenses to be furnished by the contractor associated with any computer programs (inclusive of firmware) shall be identical to those associated with any computer programs (inclusive of firmware) the contractor will deliver under a specific CDRL.

(6). The attachment should state that the price (or estimated cost) for any level of rights to a specific CDRL granted by the Contractor includes the same level of rights to any updates, software maintenance patches, minor version changes, and substitutions, at no additional cost to the Government. The purpose of this provision is to facilitate accurate submission of future years’ budget requests requesting funding to acquire those rights. In other words, this approach will reduce the probability that the
contractor can “nickel-and-dime-to-death” the program office for the rights to use, release and disclose to non-Government employees each time the contractor or its subcontractors release any update, patch, minor version change, etc., in the future.

(7). The attachment should state that any licenses must transfer to the Government upon exercise of the option by, and delivery of that CDRL or CLIN to, the Government.

(8). The attachment should specify what restrictive markings the contractor must affix to which CDRLs, and require that the contractor physically attach a copy of the attachment and all applicable commercial licenses to the CDRL prior to delivery to the Government. The purpose of this requirement is so that the recipient can quickly determine what use, release and disclosure restrictions apply to which specific items of commercial technical data located in which specific portions of the CDRL—versus having to hunt around for a hard or soft copy of the contract in order to make that determination.

(9). The attachment should prohibit the contractor from including impermissible terms and conditions described above into any NDAs between it and the program office’s “covered Government support contractors” relative to the use, release or disclosure of technical data or computer software to which Limited/Restricted Rights markings are affixed. Better yet, for the reasons discussed in Section V.B.2.g.(4) above, the attachment should request the contractor waive the requirement that the program office’s “covered Government support contractors” enter into NDAs with the contractor relative to the use, release or disclosure of that technical data or computer software.

(10). The attachment should require the contractor to, whenever it proposes changes to, e.g., existing CDRLs, to propose the appropriate changes to the attachment as well.

(11). To prevent the contractor from abandoning fundamental principles of configuration control, the attachment should prohibit the contractor from adding, deleting, or replacing any commercial item technical data, computer software, or computer software documentation listed in Table 2 from any CLIN or CDRL under which that technical data, computer software or computer software documentation will be delivered to the Government unless the Government has approved that addition, deletion or replacement and the contract has been modified to add, delete or replace that item from that table and deleted or replaced the applicable license(s). The purpose of this prohibition is three-fold: First, to ensure at all times that the paper (the contract) reflects reality (the system’s architecture). Second, presumably the program office does not want to learn for the first time ever as the weapon system undergoes the RMF process that the contractor inserted that software into that system. Third, to give the program office the opportunity to determine whether the license(s) associated with that replacement software are consistent with Federal procurement law and satisfies the program office’s needs.
In many cases, subcontractor commercial technical data and computer software licenses contain provisions that violate Federal procurement law. Examples of such provisions include, but are not limited to, disputes provisions, choice of law provisions, attorneys’ fees, automatic renewal provisions that violate the Anti-Deficiency Act, and provisions that prohibit disclosure of license terms/conditions. Therefore, the attachment should include an order of precedence clause that nullifies provisions that violate Federal procurement law.

If standard provisions in those licenses do not satisfy user needs (e.g., they are inconsistent with requirements specified in the CDD/CPD), the order of precedence clause should expressly nullify those provisions.

6. Section K (Representations, Certifications, And Other Statements Of Offerors)

Insert DFARS § 252.227-7017 (“Identification and Assertion of Use, Release, or Disclosure Restrictions”). That provision—which is not included in the SAM database—requires offerors to identify any technical data or computer software it proposes to deliver to the Government after award with less than Unlimited Rights.

7. Section L (Instructions, Conditions, And Notices To Offerors Or Respondents)

Under the GAO’s Bid Protest Regulations and bid protest decisions issued by the U.S. Court of Appeals for the Federal Circuit, protests based upon alleged solicitation improprieties which are apparent prior to the time set for receipt of initial proposals must be filed prior to the time set for receipt of initial proposals. The importance of this fact is that a protester could file a bid protest with either of those forums claiming that the contents of the RFP exceed the program office’s minimum needs for rights in technical data and computer software rights.

Accordingly, the program office should explain in Section L its minimum needs for rights in technical data and computer software and the pedigree of those needs so that if a protest results, the program office will be able to establish that rationale existed prior to release of the RFP—it is not some after-the-fact rationale the program office created after the protester filed its protest. By “pedigree”, we mean that Section L should state, e.g.,

- The statutory/regulatory basis for requiring offerors to deliver certain types of technical data with unlimited rights.
- What type of noncommercial or commercial license rights the CDD/CPD or acquisition strategy indicates are needed to satisfy the total life cycle needs of the program.
- The rationale for requiring offerors to negotiate with their commercial software vendors modifications to those vendors’ standard commercial software licenses to meet the Government’s minimum needs or to be consistent with Federal procurement law.
• The extent to which the weapon system’s maintenance/sustainment philosophy dictates that the Government must acquire a certain type of license rights—e.g., the maintenance philosophy will be that the Government will compete on-orbit anomaly resolution of a specific major system component (i.e., software item) of bus flight software identified at the fifth level of indenture of the WBS and in the SAD—including the extent to which that maintenance philosophy as described in the program’s LCSP will change at some point. Of course, if the Government never represents to offerors what is its maintenance philosophy—or the offeror’s assumption that it would be performing maintenance of that component or major system platform for the life cycle of that platform is not expressly incorporated into the contract prior to award—it would be unreasonable for the offeror to base its decision (in whole or in part) whether to submit a proposal for development/production of that platform upon a belief that the Government will award it follow-on maintenance contracts sole-source for the life cycle of that platform (whatever the duration of that life cycle may be).

Immediately after describing this pedigree of the program office’s minimum needs, Section L should emphasize that the technical data and computer software rights described in the DFARS clauses listed in Section I of the RFP are the rights the program office expects to receive in exchange for paying for development of the technical data or computer software. The purpose of this information is to warn offerors they should not propose the Government have to pay an additional cost for acquiring those rights.

Section L should then require that offeror’s Technical Volume in its Contracts Volume explain how its Data Rights Attachment in its Contracts Volume will meet the Government’s minimum needs and will result in an executable program underneath the appropriate subfactor(s). Section L should also describe how the offeror must propose prices or estimated costs for licenses in its Cost/Price Volume.

Next, Section L should provide instructions to offerors (1) describing how they must fill-in their Data Rights Attachment described above, and (2) requiring them to complete their DFARS § 252.227-7017 certification/representation consistent with the manner in which offerors have filled-in the tables in their Data Rights Attachment. Section L should also require offerors to provide copies of all licenses associated with all commercial technical data and computer software the offeror proposes to deliver to the Government. The program office should also insert DFARS § 252.227-7028 (“Technical Data or Computer Software Previously Delivered to the Government”) into Section L.

Finally, for the reasons mentioned in Section V.C.5.b-c above, Section L should require the offeror to include into Section J of its proposed Contract Volume a WBS and WBS dictionary as a Section J attachment and instruct the offeror to further extend each WBS element as necessary to define the complete contract scope, consistent with its proposed approach for executing the program. Section L should also require that the offeror describe how its proposed WBS supports the program’s delivery schedule, the extent to which its MOSA approach will define all major system interfaces consistent with
the program’s performance specification/system requirements document—because as stated in DoDI 5000.02 Change 2, poorly configured, inadequately maintained, undocumented, or unprotected network and system interfaces create cybersecurity vulnerabilities—and how its approach for conducting systems engineering will be consistent with the program’s SEP. For software-intensive systems, Section L should also require the offeror submit a SAD as part of its Technical Volume, and include the SAD CDRL into Exhibit A of its proposed Model Contract. The proposed SAD should identify precisely where all noncommercial and commercial software applications will reside in the offeror’s proposed architecture.

8. Section M (Evaluation Factors For Award)

The GAO has held that the Government must evaluate proposals in accordance with the terms of the solicitation, and that an agency may properly consider specific, albeit not expressly identified, matters that are logically encompassed by, rationally related to, or intrinsic to, expressly stated evaluation criteria. The COFC has enunciated a similar standard: A solicitation need not identify each element to be considered by the agency during the course of the evaluation as long as such element is intrinsic to the stated factors.

This does not mean, however, that an agency may evaluate whatever it wants to under any particular evaluation criteria, as there must be a clear nexus between the stated evaluation criteria and the unstated criteria. Given this legal principle—and the fact that the subject of acquiring IP rights is in a class by itself—it is highly inadvisable for any program office to assume that it will be able to prove its evaluation of the offeror’s proposal to furnish rights in technical data and computer software was logically encompassed by and rationally related to whatever expressly stated technical evaluation criteria was in Section M. Accordingly, and for the reasons described in Section V.B.2.d above, Section M must include evaluation criteria within the appropriate Technical subfactor that expressly state the Government will evaluate the extent to which the offeror’s proposed rights as reflected in its Data Rights Attachment (including the content of any commercial licenses) and its completed DFARS § 252.227-7017 certification/representation satisfies the Government’s minimum needs and does not inhibit the Government’s ability to execute successfully the program throughout its life cycle.

Section M should also explain how the Government will use the prices the offeror proposes for the rights in technical data and computer software it proposes to deliver to the Government after award as part of the Government’s cost/price evaluation. In this regard, if the Government will permit offerors to propose more than one type of license rights (and therefore a different price for each type), it should identify what price for what type of license rights it will use as part of its Most Probable Cost (MPC) calculation for each offeror. Caution is advised when making this identification—as an improper selection could widen the MPC differential between offerors to such an extent as to make it difficult if not impossible for an SSA to make award to a technically superior offeror.
Finally, for the reasons mentioned in Section IV above, Section M must state the Government will evaluate the extent to which the offeror’s proposed architecture will implement MOSA principles consistent with the program’s SEP, the offeror’s proposed WBS as contained in Section J of its Contract Volume, and (for software-intensive systems) its proposed SAD as reflected in the offeror’s Technical Volume.

D. Integrated Data/Digital Environments (IDE)

1. The Concept

Over the past two decades, program offices have used IDEs to execute their acquisition programs. Unfortunately, in some cases they have realized too late that they unconsciously inserted into their program management structure something they would rarely—if ever—permit a contractor to intentionally insert into the design of the weapon system to be provided to the warfighter: a single-point failure just waiting to happen. The single-point failure is because for administrative convenience, the program office decided that an IDE would reside on the prime contractor’s servers. What that means is that the program office will not have physical custody or control of any data residing within that IDE. The single-point failure occurs when the prime contractor unilaterally decides to electronically shut off “access” to its servers for any reason (or no reason at all), thereby preventing the program office from using, releasing or disclosing that technical data or computer software outside the Government—irrespective of whatever restrictive markings (if any) the contractor affixed to that CDRL.

The consequences of this unilateral decision is that program execution comes to a screeching halt when those personnel the program office intended to have “access” cannot “access” that technical data and computer software anymore to execute the program. Only then does the program manager realize that the parties “made this IDE up as they went along”—because prior to contract award and during contract performance, they never memorialized that concept in enforceable language and included that language into the RFP and resulting contract as required by AFI63-101/20-101 and AFPM63-128. With those catastrophic consequences in mind, the stage is now set for a discussion regarding what IDEs are and how the parties should memorialize that concept in the request for proposals and the resulting contract. That discussion begins with defining what is an “IDE”.

An IDE is a data storage and information management system. Its purpose is to create an environment of connected knowledge workers, in which the preferred approach to performing work involves instantaneously accessing data (including work-in-process data) required to accomplish the necessary tasks and then outputting the results into an instantaneously accessible form. It is the infrastructure that permits implementation of Product Life Cycle Management as it integrates the people, processes, business systems, and information associated with the design, development, production, deployment, maintenance, sustainment, and disposal of a weapon system over its entire life cycle. Under this construct, information sharing is rewarded and redundant data development, transmission or storage is frowned upon.
The IDE can either be a program-unique repository run by Government personnel on a Government server, a program-unique repository run by a contractor on its own servers, or an existing Government enterprise repository on a Government server (e.g., Military Engineering Data Asset Locator System (MEDALS), Joint Engineering Data Management Information and Control System (JEDMICS)). Key functions of IDE support include:

- Product data management: Storing and managing all information about the weapon system throughout its life cycle.
- Configuration management: Tracking and managing all configuration changes.
- Collaboration: Supporting virtual teaming and common access to team work products.
- Design analysis and tradeoff studies: Evaluation of different design concepts and decisions made on selected designs.
- Requirements traceability: Relationship between user requirements, weapon system technical requirements, design capabilities, and test results.
- Logistics support analysis and planning: Leveraging design information to perform logistics analysis and planning activities that will positively influence weapon system reliability, maintainability, and supportability.
- Long-term data access and controls.

The Defense Acquisition Guidebook states that to the greatest practical extent, programs should use existing Government enterprise IDEs; program-unique IDEs are disfavored due to high infrastructure cost and because multiple program-unique IDEs inhibit access, sharing and reuse of data across programs. Program-unique IDEs may violate 40 U.S.C. § 11312, which requires that the heads of executive agencies identify information system investments that would result in shared benefits or costs for other federal agencies for “national security systems” to the extent practicable. Program-unique IDEs may also violate Section 2867 of the National Defense Authorization Act for Fiscal Year 2012 (Pub.L. No. 112-81), that prohibits the obligation of funding for a “data server farm” or “data center” unless approved by the Chief Information Officer of the Department of Defense. In contrast, program-unique IDEs are encouraged by the DoD Open Systems Architecture Contract Guidebook for Program Managers.

If after analyzing the statutory restrictions summarized in the preceding paragraph the program office concludes that neither restriction precludes the creation of a program-unique repository run by a contractor on its own servers, the program office must carefully determine what will be its Concept of Operations for that IDE. Like Julius Caesar’s Gaul, the IDE will consist of three parts:

- The environment consisting of a web-based platform.
- The data residing within that environment.
- The licenses the contractor will grant to the program office to the environment as well as to the data that will reside within that environment.
2. How To Properly Implement That Concept In An RFP

Although the parties may allocate the terms and conditions in a contract that must memorialize each of the parts of an IDE to different sections of the RFP consistent with the UCF, that approach is not particularly user-friendly. The reason why is because it assumes that a user of the contract years hence will be able to find all those proverbial “needles-in-the-haystack” scattered throughout the contract and be able to put them together in an integrated—pun intended—fashion in order to understand how all those terms and conditions relate to each other.

Therefore, a program office should only use that approach if each section of the contract that discusses a topic relating to the IDE will cross-reference all other relevant sections of the contract. In the alternative, most of those terms and conditions may be located in a single location in the contract. That approach has the benefit of making it easier for any user of the contract years hence to find quickly those terms and conditions years hence. That approach is discussed below.

Invariably, each offeror will have their own unique proposed IDE that it believes will best satisfy the program office’s needs, and one offeror’s proposed IDE may be technically superior to another offeror’s proposed IDE. It is therefore inadvisable for program offices to include into Section L of the RFP a requirement that offerors submit proposals against a “cookie-cutter” IDE. Conversely, the program office needs to accurately identify its IDE requirements in order to comply with a fundamental principle of government contracting stated above: In a competitive environment an RFP must provide for the submission of proposals based upon a common understanding of the agency’s requirements.

Accordingly, the program office must identify in Section L of the RFP what additional CDRLs the offeror must deliver to implement its proposed IDE and what IDE-related topics the offeror must address in an Appendix to the Section J Data Rights Attachment to its Model Contract. The program office must also identify in Section M of the RFP what evaluation criteria it will use to determine the technical acceptability of each offeror’s unique proposed IDE relative to the three concepts described above.

Therefore, Section L should require offerors to submit as part of their proposed Model Contracts the following documents:

a. Exhibit A.

Offerors should be required to submit the following four CDRLs, tailored consistent with their unique solution:

(1). A Software Product Specification (DI-IPSC-81441A). The purpose of this CDRL is to require the offeror to deliver the computer software needed to instantiate the “environment”. It should require delivery of the source code to any modifications the offeror intends to make to any commercial computer software (e.g., Microsoft SharePoint)
to create the IDE. If the program office will not be procuring those commercial computer software applications under separate contracts, this CDRL should also require the delivery of the executable code to those commercial computer software applications.

(2). A Software Version Description (DI-IPSC-81442A). The purpose of this CDRL is to release, track and control software versions for configuration control purposes. In other words, it identifies all versions of commercial computer software the offeror intends to use to create the IDE, as well as all modifications the offeror intends to make to those software applications to customize the IDE for that specific acquisition program.

(3). A Database Design Description (DI-IPSC-81437A). The purpose of this CDRL is to describe the design of the database that comprises the IDE. In other words, it provides the Government with a textual description of the IDE instantiation (i.e., the file folder structure/hierarchy, levels of access rights and privileges specified at the user level (e.g., administrator, guest, super-user) and at the data/deliverable level (e.g., ability to allow access to specific data/deliverables to selected users only based upon the classification level and level of license rights associated with that data) into which the “data” will be deposited, search functions). The program office will then be in a position to carefully review and approve that structure to ensure that authorized users who will create the data deposited into that IDE will know precisely in which sub-sub-sub-subfolder they should deposit that specific document and so that authorized users can quickly find that proverbial “needle in the haystack”. If the program office does not mandate that disciplined approach from the date of contract award, during contract performance authorized users will create their own sub-sub-sub-subfolders and deposit data into those locations—making it virtually impossible for many other authorized users to find a specific document, and thereby defeating the purpose for which the IDE was created in the first place.

(4). A Data Accession List (DI-MGMT-81453A). The purpose of this CDRL is to list all data the offeror will create during contract performance, including all “work-in-progress” data that will reside on the IDE.

b. Appendix A to Section J Data Rights Attachment.

Section L should require the offerors discuss the following topics in their proposed Appendix A:

(1). Purpose. In this subsection, the offeror should insert a short statement that describes the purpose of the IDE.

(2). Definitions. In this subsection, the offeror should define all terms used in this Appendix to the Section J Data Rights Attachment. Next, the offeror should describe the software architecture of the “environment” into which the “data” will reside in both a narrative manner as well as in a pictorial depiction so that the reader can understand the relationship between the Software Product Specification, Software
Version Description, Database Design Description, and Data Accession List CDRLs. As stated in Section V.B.2.b of this Handbook, the term “access” is vague. Accordingly, the offeror should define that term in this subsection (e.g., the ability to view, print, download, annotate, and interact with all modified or archived versions of any data residing on the IDE), along with all other relevant terms (e.g., “IDE”, “authorized user”).

(3). Requirements. In this subsection, the offeror should discuss the following topics:

(i). What the minimum capabilities of the IDE will be (e.g., internet accessible by using a standard web browser application, navigation, data exchange, data interaction, error-checking protocols, archive library).

(ii). How the offeror will configure the IDE consistent with the relationship between the four CDRLs described above.

(iii). How the costs the offeror will incur to develop and maintain the “environment”—including the costs incurred to acquire the commercial software licenses and modify that software to create the “environment”—will be allocable to the contract. If, for example, the IDE will be supporting a single program, Section B of the offeror’s Model Contract should include a separate CLIN so that the program office will have visibility into how much it will be paying the offeror to develop and maintain that IDE for the entire period of performance of the contract. In contrast, if the IDE will be implemented via an advisory and assistance services contract supporting multiple ACAT I/II/III programs, it will probably be too unwieldy to acquire funding from those programs and then obligate that funding onto that CLIN on a regular basis. Accordingly, the offeror should be required to allocate the costs of developing and maintaining the IDE on an equitable basis to the CLINs under which the services are being provided to support the multiple programs in question.

(iv). As stated in the DoD Open Systems Architecture Contract Guidebook for Program Managers, “a requirement for an IDE is not a substitute for having formal technical data and software delivery requirements.” Accordingly, in this subsection the offeror should state that all data listed on the Data Accession List will reside on the IDE—as will all data delivered under other CDRLs—and that all that data will be considered “deliverables”.

(v). In this subsection, the offeror should explain what procedures it will develop and maintain to protect data delivered to or stored in the environment from unauthorized release or disclosure and to control the release of data from the environment to authorized users consistent with DFARS § 252.204-7012 (“Safeguarding Covered Defense Information and Cyber Incident Reporting”), the program’s Security Classification Guide, and the Government’s IP rights in that data. Those procedures would include an identification of who will be authorized to “access” the data residing on the IDE consistent with the contractor’s proposed Database Design Description CDRL—including any authentication procedures the contractor will implement to control “access”
— and how those authorized users will obtain “access”. This subsection should also state
that the contracting officer will provide the contractor with the names of authorized users
and the level of access authorized for each user.

(vi). If necessary, this subsection should describe how the offeror will
obtain use and non-disclosure agreements from all non-government employees to whom
data will be released or disclosed if that data will be delivered with less than Unlimited
Rights if the recipients’ contracts do not contain DFARS § 252.227-7025.

(vii). In this subsection, the offeror should identify during what periods
authorized users will be able to “access” the data residing on the IDE—with occasional
periods of unavailability for maintenance purposes assuming the contractor gives
authorized users advance notice of any regular or extended periods of unavailability—
and the minimum number of authorized users the IDE will be able to support
simultaneously.

(viii). In this subsection, the offeror should state that it will deliver the
Software Product Specification, Software Version Description, Database Design
Description, and all data listed on Data Accession List CDRLs that comprise the IDE.

(ix). In this subsection, the offeror should state that, pursuant to
DFARS § 252.227-7027, it will image the IDE—both the “environment” as well as the
“data” residing within that “environment”—and deliver that instantiation to the Contracting
Officer upon request. The purpose of this section is to ensure that, well prior to contract
closeout, the program office receives a copy of the IDE. The program office will then be
able to include that IDE into the Bidders’ Library for the follow-on competitive acquisition,
and provide that IDE to the awardee of that follow-on contract to sustain the weapon
system(s) for which the IDE was established in the first place.

(x). In this subsection, the offeror should indemnify the Government
from any liability to any data owners or licensors resulting from or as a consequence of a
release or disclosure of data made by the contractor or its officers, employees, agents, or
representatives.

(xi). If the offeror will be depositing into the IDE final versions of data
the contract requires to be delivered as CDRLs, in this subsection the offeror should
describe how that data will be received, inspected and accepted by the program office.

(xii). In this subsection, the offeror shall identify what training (e.g.,
classroom, on-line) and help desk support it will provide to authorized users of the IDE.

(4). Remedies. Congress has not granted any court the power to order a
contractor to reinstate “access” to authorized users of the IDE where, e.g., the contractor
has unilaterally shut off access. Nor can the parties to a government contract confer that
power upon any court. Since such an agreement between the parties would be illusory,
the program office should instead require the offeror propose a monetary remedy. This
section should also identify any circumstances under which the offeror will not be liable to the Government if unauthorized users are unable to “access” the “data” residing within the “environment”.

(5) IP Rights. The preceding discussion has described how to memorialize in enforceable contract language two of the three essential parts of an IDE: The environment (i.e., the contractor data repository itself) and the data that will reside within that electronic repository. Accordingly, this subsection should identify the third part of an IDE, namely, what license rights the offeror will grant to the program office to all data that will reside within that environment. In other words, the offeror should “map” what license rights it will grant to the:

- Software Product Specification CDRL that requires the delivery of the software applications that comprise the integrated digital/data environment.
- Software Version Description CDRL that identifies all versions of that software that create that environment.
- Database Design Description CDRL that identifies the file folder structure/hierarchy of the IDE.
- Those items the offeror will list in the Data Accession List CDRL.

This subsection should also identify what restrictive markings the offeror must affix to that “data”.

In sum, the program office must memorialize the IDE product baseline in an Appendix to the Section J Data Rights Attachment that describes the environment, the data that will reside within that environment, and the licenses that the Government will acquire to the data that will reside within that environment. To achieve this objective—and to evaluate during source selection offerors’ proposed CDRLs and Section J Data Rights Attachment Appendix—the Contracting Officer will need the assistance of three types of acquisition professionals:

- Program office personnel who will be using the IDE (e.g., program managers, engineers, product support personnel, supply chain personnel, quality assurance personnel, life cycle logisticians, engineering data managers).
- Information technology professionals familiar with the capabilities of the software applications that will constitute the IDE.
- Program attorneys possessing extensive government contract transactional and trial experience who can memorialize the environment, the data that will reside within that environment, and the licenses to the data that will reside within that environment in enforceable contract language understandable by those possessing only a high school degree.

As suggested by the complexity of the above discussion, this is not a job for amateurs.

E. Prior to RFP Release
In order to foster transparency with its industry partners, after it issues the draft RFP the program office should highlight the existence of the provisions described above. The program office should also describe how the Government arrived at its minimum needs, and invite potential offerors to comment on the proposed terms and conditions to address potential offerors’ legitimate concerns while at the same time educating potential offerors as to the program office’s requirements. The purpose of this approach is to reduce the potential for bid protests relating to the provisions described above and to ensure the program office has conducted appropriate market research.

For example, the program office may have indicated that its minimum needs include acquiring Unlimited Rights to a particular CDRL that contains form, fit and function data as required by law—but that CDRL also requires the delivery of detailed manufacturing process data. A potential offeror may be understandably reluctant to sell at any price Unlimited Rights to detailed manufacturing process data. Conversely, the program office may not have intended to request Unlimited Rights to that technical data. Therefore, the program office may decide to solve this problem by first modifying the content of the offending CDRL by deleting the requirement for such technical data (while retaining the form, fit and function information in that CDRL and its associated Unlimited Rights license). Next, the program office would move the requirement to deliver detailed manufacturing process data to a second CDRL—and then describe the scope of a Specifically Negotiated License associated with that second CDRL that accommodated potential offerors’ reasonable concerns while at the same time satisfying the Government’s (revised) minimum needs.

In a similar manner, a program office could split up technical data contained within a particular CDRL that describes multiple subsystems into multiple CDRLs based upon the weapon system’s Work Breakdown Structure (WBS), so that each CDRL describes only that technical data associated with a particular major system, subsystem, or component. In either case, the result will be the same in that one of the steps described in Section V.B.2.g.(2) above will still be satisfied: The program office will have baselined all contents of a specific CDRL to a single level of license rights to the maximum extent practicable.

F. During Source Selection

1. General Guidance

Upon receipt of offerors’ proposals, the SSEB should evaluate those proposals in accordance with the Sections B/I/J/K/L/M/Exhibit A provisions described above. If the SSA establishes a competitive range and opens discussions, the SSEB should have discussions with offerors regarding any weaknesses, significant weaknesses, or deficiencies in their proposal regarding this matter. If an offeror asserts that it will be delivering a particular CDRL with less than the minimum level of rights specified in Section L, the SSEB may need to request that the offeror provide support for its position, amend the RFP to change the Government’s minimum needs, or notify the offeror that its proposal is technically unacceptable consistent with 10 U.S.C. § 2320 and the CICA.
the Government decides that its needs are different from those rights described in the RFP, the Contracting Officer must amend the RFP consistent with its revised requirements.

Occasionally, an offeror may “overachieve”. Specifically, the offeror may propose to deliver more content in a CDRL deliverable than is required by the DD Form 1423—but in so doing “underachieve” by proposing a lower level of rights in technical data and computer software than is required by the RFP because the offeror wants to restrict the use, release or disclosure of that additional content. The offeror, however, may not realize that by attempting to obtain a strength assessment under a particular Technical subfactor for proposing that additional content, it may very well have injected a feature into its proposal the program office would assess as a deficiency under a different Technical subfactor. The reason why is because the offeror is now proposing to deliver a lower level of rights in technical data or computer software than the RFP indicates are the program office’s minimum needs. There are at least two ways to fix this problem. First, during discussions, the Contracting Officer can suggest to the offeror that it delete that additional proposed content and propose to deliver technical data and computer software rights consistent with the program office’s minimum needs specified in the RFP. In the alternative, if the program office believes that additional content is necessary, the Contracting Officer must amend the RFP to require delivery of that additional CDRL content and if necessary modify the level of technical data and computer software rights identified as the Government’s minimum needs for that CDRL.

2. Specific Guidance

According to the FAR, the SSA must base the award decision on a comparative assessment of proposals against all source selection criteria in the RFP. Since this general principle applies to the acquisition of technical data and computer software rights, the SSEB must analyze whether all portions of the offeror’s proposal are consistent with each other insofar as the level of rights in technical data and computer software proposed are concerned. Assuming the SSEB has structured its RFP in a manner similar to that described above, the following decision tree will assist the program office in completing an integrated assessment of an offeror’s proposal technical data and computer software rights offering:

a. Evaluating the Offeror’s Technical Approach

(1). To determine the extent to which the offeror’s technical approach is based upon MOSA principles, for all supply and services acquisitions, the SSEB should carefully review the offeror’s proposed WBS in its Contract Volume to identify what major system components are identified in that proposed WBS and the extent to which the offeror’s technical approach as described in its Technical Volume is consistent with the program’s SEP. Next, the SSEB should determine what major system interfaces—between the major system platform and a major system component, between major system components, and between major system platforms—the offeror identifies in its Contracts Volume and discusses in its Technical Volume to determine the extent to which
those interfaces will contain physical, logical, and functional characteristics sufficient for a competitor to be able to incrementally add, remove, or replace major system components throughout the life cycle of that major system platform.

(2). For software-intensive supply acquisitions, carefully review the offeror’s SAD contained in the *Technical Volume* of its proposal. Understand which major system components (in this case, software items/software subroutines)—including OSS—reside in which locations of the offeror’s proposed architecture and the purposes (functionality) for which those components are being used in that architecture (e.g., during development, in delivered code, and for use on which systems and in which geographic locations). Create a list of those components for use when completing step (9) below.

(3). Verify that all text in the offeror’s Data Rights Attachment (see Appendix 1 (“Relevant Excerpts from SE&I Follow-On RFP”) Attachment 10) contained in the *Contracts Volume* of its proposal is identical to that contained in the Data Rights Attachment in the RFP.

(4). Verify that the offeror has properly filled-in all cells in Tables 1 and 3 in its Data Rights Attachment and determine whether the noncommercial rights proposed in Table 1 satisfy the program office’s minimum needs as specified in Section L of the RFP.

The following explanation of how the Government would determine whether the offeror’s proposal satisfies the Government’s minimum needs is based upon the provisions in Appendix 1 of this *Handbook*. In that case, Section M-4.2.1.1.b of the RFP included in Appendix 1 states the Government will evaluate the extent to which the offeror’s proposed data rights meet the Government’s minimum needs as specified in the RFP. Accordingly, offerors should first carefully read Section L-7.3.11.a-b of that RFP, which stated the pedigree of the Government’s minimum needs and directed the offeror’s attention to the Data Rights Attachment of that RFP in Section J (i.e., Attachment 10). In turn, Table 1 of Attachment 10—when read in conjunction with Section L-7.3.11.d.i—states the Government’s minimum license needs for, e.g., CDRL A004 (Interface Control Documents/Interface Specifications) are Unlimited Rights.

The GAO has held that clearly delineated solicitation requirements constitute a minimum need of the Government. Section M-4.2.b.ii of the RFP in Appendix 1 of this *Handbook* restates the definition of a “deficiency” lifted from the FAR: A material failure of the proposal to meet a Government requirement. In other words, the provisions in that RFP have put all offerors on express notice of precisely what will happen if an offeror proposes to deliver a lower level of license rights than Unlimited Rights to CDRL A004 to the Government: The Government will assess that feature of the offeror’s proposal associated with Section M-4.2.1.1.b evaluation criteria as a deficiency.

Section M-4.1 Table 1 of that RFP states that any deficiency in the offeror’s proposal will result in the Government assigning a “Red/Unacceptable” rating to that aspect of the offeror’s proposal under the Technical Capability/Technical Risk Subfactor in which various evaluation criteria is located (in this case, Subfactor 1 (Systems
Engineering and Integration)), thereby rendering that proposal unwawardable. (The same result would ensue under the current version of the Department of Defense Source Selection Procedures, which prescribes the use of an “Unacceptable” Technical Risk Rating—the definition of which is that the proposal contains a material failure or a combination of significant weaknesses that increases the risk of unsuccessful performance to an unacceptable level—in conjunction with the use of a “Red/Unacceptable” Technical Rating.) Accordingly, the offeror’s business decision to propose to deliver to the Government anything less than Unlimited Rights to CDRL A004 will render that offeror’s proposal unwawardable on that basis alone irrespective of whether the SSA’s tradeoff analysis would have resulted in that offeror becoming the awardee based upon its (1) otherwise technically superior approach or (2) its comparatively lower MPC.

In short, these provisions of the RFP contained in Appendix 1 foster transparency between the program office and its industry partners regarding precisely what will be the ramifications of the offeror’s decision to propose less than Unlimited Rights to CDRL A004. This assumes, of course, that the offeror has asked their in-house counsel to review those provisions prior to drafting their proposal—and that in-house counsel has carefully reviewed those provisions.

(5). Evaluate whether the proposed license rights contain any flaws.

Even if the offeror’s proposed licenses satisfy the Government’s minimum needs—i.e., they do not contain any deficiencies similar to that described above—those licenses may contain various flaws that increase the risk of unsuccessful contract performance. In general, there are two types of flaws: (1) weaknesses, defined as a flaw in the proposal that increases the risk of unsuccessful contract performance, and (2) significant weaknesses, defined as a flaw in the proposal that appreciably increases the risk of unsuccessful contract performance. (Section V.F.2.a.(9) of this Handbook provides examples of such flaws.) The FAR requires that the Government identify such flaws in an offeror’s proposal and then—if the SSA decides to establish a competitive range and conduct discussions—bring the existence of significant weaknesses (and deficiencies) to the offeror’s attention during discussions.

(6). Verify that the licenses for all commercial item or COTS software applications described in the offeror’s proposed SAD are included in the appendix to the offeror’s Data Rights Attachment.

(7). Verify that the offeror has mapped all commercial item or COTS licenses to the proper CDRLs and CLINs in Table 2 of that Attachment.

(8). Analyze whether the proposed “commercial item” or COTS” is truly a “commercial item” or “COTS.” The Government is required to acquire commercial items or COTS items if those items satisfy its needs. As a result, some offerors may claim that a certain item of technical data or computer software it proposes to deliver as part of a CDRL is a “COTS” item, a “commercial item”, or “commercial computer software” such
that the program office should accept the terms and conditions of the proposed commercial license. Before agreeing with the offeror, the SSEB should carefully determine whether the technical data or computer software the offeror proposes to deliver with various use, release disclosure restrictions in the proposed license is in fact a “COTS” item, a “commercial item”, or “commercial computer software” by using the definitions of those terms and the questions provided in Section II.D of this Handbook. The danger of the SSEB agreeing with the offeror’s determination that the technical data or computer software is in fact a “COTS” item, a “commercial item”, or “commercial computer software” without carefully analyzing the pedigree of that determination is that the program office may agree to commercial license restrictions when in fact it should have agreed to a noncommercial license (e.g., Unlimited Rights).

If after performing the analysis described in Section II.D of this Handbook the SSEB concludes that portions of the technical data or computer software in the deliverable do not satisfy the definition of a “COTS” item, a “commercial item”, or “commercial computer software”, consistent with MOSA principles, the SSEB should then ask the offeror whether the major system components (in this case software items/software subroutines) that will contain those portions are physically separable from those portions that do satisfy any of those definitions. If so, the program office should acquire the standard commercial license to those portions that satisfy any of those definitions and an appropriate noncommercial license (e.g., Unlimited) to the major system components that do not satisfy any of those definitions. To ensure releasability of all portions of the major system component to the same entities for the same purposes for the same period, the scope of those licenses must be identical to each other. If, however—in contravention of MOSA principles—the offeror failed to physically segregate major system components that satisfy any of those definitions from major system components that do not satisfy any of those definitions, the program office should acquire a license (or licenses) to all portions of the deliverable the scope of which are identical to each other in order to satisfy its minimum use, release and disclosure needs.

(9) Carefully read each COTS license to determine whether it will satisfy the program office’s needs and whether any terms or conditions in the license are inconsistent with Federal procurement law. If they are not, the SSEB must point out that fact to the offeror during discussions and modify the order of precedence clause in the Data Rights Attachment accordingly.

To assist the reader in understanding how this concept applies, consider the following examples. A license provision that would violate federal criminal laws—e.g., those that apply to the dissemination of classified information—would be one that states that foreign persons will perform software maintenance of a commercial software application. The reason why that provision would violate Federal procurement law would be because, according to the offeror’s proposed SAD, that software application will reside in a classified facility—which therefore means the resulting contract will contain a patent (obvious) ambiguity because the DD Form 254 will prohibit foreign persons from entering that facility.
One license provision that would be incompatible with user needs would be one that states that the customer may only use the commercial software application in the country where purchased when, *according to the offeror’s proposed SAD*, that application will be embedded into a weapon system that will be installed in countries other than the U.S. Another license provision that would be incompatible with user needs would be one that requires the customer to remove, uninstall, and return software to the contractor if the program office breaches the terms of the license. Compliance with those provisions could very well require the Air Force to declare a space vehicle non-operational so that the Air Force will be in substantial compliance with those terms/conditions since it may not be physically possible to uninstall and return that software to the contractor given the orbits within which those space vehicles reside. With respect to a control segment, since removal is physically possible the Air Force would have to declare that system non-operational until the situation is resolved either by (1) obtaining the contractor’s permission to continue using the software, or (2) requiring the contractor to replace that software application with another one along with an appropriate license for that application.

The national security implications these situations would create demonstrate the need to nullify such provisions contained in proposed commercial licenses in the resulting contract prior to award. As a result, the contractor’s and—if the software application was licensed from a subcontractor—its subcontractor’s remedy for that breach will be limited to monetary damages (versus retaining language in a license that states a court could issue an injunction against the Air Force ordering it to uninstall the software and return that software to the contractor).

Yet a third provision that might be incompatible with user needs is one that states the commercial software application is not designed or intended for use in weapon systems, for aircraft navigation purposes or safety-of-life applications. Such a disclaimer may be nothing more than another example of our litigious society. On the other hand, it could be a warning to the program office that the developer has little faith in the stability and integrity of that software—in which case, why would the program office want to purchase it for use in those critical applications? The only way for an SSEB to determine whether that provision in the proposed license should be classified as a deficiency, weakness or significant weakness would be to ask the following questions:

- *According to the offeror’s proposed SAD*, at which locations in the contractor’s architecture will that software reside—on the periphery or at its heart?
- Does the history of that software indicate it is sufficiently robust to satisfy the requirements in the performance specification/system requirements document and related compliance/reference documents?
- If the SSEB initially determines the software is sufficiently robust prior to award, but after award the Government later determines that was not the case, how difficult will it be for the contractor to switch-out that software with a replacement or develop source code from scratch to overcome those inadequacies?
An offeror’s proposed use of OSS poses additional licensing issues that the SSEB must carefully analyze during source selection. For example, some OSS licenses (e.g., earlier versions of the GNU General Public License) require distribution of modifications to that OSS under the same terms as the license of the original software. If the program office wants the offeror to modify that software to perform successfully the contract, it would not be possible to comply with those license terms for failure to do so might violate Federal procurement law (e.g., export control laws, the program’s Security Classification Guide).

(10). Evaluate the offeror’s DFARS § 252.227-7017 certification/representation.

In many cases, an offeror will not understand how to properly fill-out the DFARS § 252.227-7017 certification/representation. Amongst other things, that provision requires the offeror to identify which noncommercial technical data pertaining to items, components or processes and which noncommercial computer software or computer software documentation will be delivered with less than Unlimited Rights. Unfortunately, many offerors fill-in that provision by identifying various hardware items (e.g., “Digital receiver”) notwithstanding that hardware is not “technical data.” Accordingly, during discussions the SSEB should ensure the offeror revises its certification/representation to identify the specific items of technical data (e.g., “Drawing No. 12756 Rev. B (Digital Receiver) dated June 21, 2006, contained in CDRL A037”) and computer software (software application name, version, release data, which CDRL will contain that software) to be furnished with restrictions. The SSEB should also analyze whether the assertions made in that certification/representation are consistent with those stated in the offeror’s Data Rights Attachment.

b. Evaluating the Offeror’s Proposed Costs/Prices

As stated at the beginning of this Handbook, the development and acquisition of IP requires money—which brings us to the subject of how the SSEB should evaluate an offeror’s Cost/Price Volume relative to the program office’s acquisition of rights in technical data and computer software. The extent of this evaluation depends in great part upon whether the RFP required offerors to propose licenses under cost-reimbursable CLINs or firm-fixed-price CLINs.

If the RFP required the offeror to propose prices for licenses under a fixed-price CLIN, the SSEB must verify that the offeror has done so in its Data Rights Attachment. In contrast, if the RFP requires the offeror propose the costs of licenses under a cost-reimbursable CLIN (or CLINs), the SSEB must verify that the offeror has proposed costs in the Basis of Estimates (BOE) the offeror proposed in its Cost/Price Volume for all licenses listed in its Data Rights Attachment—which presumably are associated with the identical software applications described in its SAD. The SSEB must then perform a cost realism analysis of the offeror’s proposed license costs and make upward adjustments to the offeror’s proposed costs, if appropriate. The SSEB should also verify that the costs proposed in the offeror’s Cost/Price Volume are identical to those proposed in its Data Rights Attachment.
In addition, the SSEB should determine the fairness and reasonableness (and if necessary, the price/cost realism) of the proposed cost of the data itself in addition to the cost/price of the rights to that data. Accordingly, the offeror must fill-in Block 18 of each DD Form 1423 ("Estimated Total Price") contained in Exhibit A of its Contracts Volume with the amount equal to that portion of the total price estimated to be attributable to the production or development for the Government of that item of data. The Armed Services Pricing Manual explains the purpose for which the SSEB will obtain that information from the offeror:

The [program office] will use the submitted prices in deciding whether its needs for the data are worth the dollars they will cost. If the [program office] concludes that the benefits are commensurate with the cost, the data requirement stays on the list; if the [program office] concludes that the data are not worth what they will cost, it modifies or deletes the requirement. The amended list is made a part of the contract. The prices on that list, how they are derived, and what they mean are the subject of this section.\(^{21}\)

In other words, if after receipt of initial proposals the program office realizes that a particular CDRL will be expensive and in retrospect does not need that CDRL, after the SSA establishes the competitive range the Contracting Officer can amend the RFP to delete that CDRL from Exhibit A. In a similar fashion, if after award the program office decides it made a mistake and no longer needs the CDRL, it can request a deductive change proposal from the contractor to delete that CDRL from the contract. To be sure, negotiations between the parties must commence with the current estimates of what the cost would have to produce that CDRL—not the original proposal estimates the contractor typed into BLK 18 prior to award. Nevertheless, a contractor's deductive change proposal that asserts the current cost of that CDRL is far less than what it proposed—especially if only a short period has elapsed between the date of award and the date the Government receives the contractor's deductive change proposal—would arguably lack credibility.

This final part of the SSEB's evaluation is not complete, however. The reason why is because the GAO has repeatedly held that an evaluation of an offeror's technical approach must be consistent with its cost/price evaluation. What that means in this case is that the SSEB must ensure that its evaluation of the offeror's proposed licenses described in its Technical and Contracts Volumes is consistent with its evaluation of the offeror's proposed costs/prices in its Cost/Price Volume.

\(^{21}\) Armed Services Pricing Manual (ASPM) § 9.5 (p. 9-29)(1986)(emphasis added), available at http://www.library.dau.mil/ASPM_v1_1986.pdf. In 1996, the FAR replaced the ASPM with the Contract Pricing Reference Guides (see FAR 15.404-1(a)(7)). Since, however, those Guides no longer include the detailed information found in the ASPM, the ASPM remains a useful reference for SSEBs to use when analyzing whether an offeror's estimated total price for a proposed CDRL is fair and reasonable (and if necessary, realistic).
Accordingly, after assigning a weakness or significant weakness to that aspect of an offeror’s proposal associated with a proposed license the SSEB concludes contains flaws that increase or appreciably increase the risk of contract performance, the SSEB may need to—in the case of cost-reimbursement contracts—“dollarize” those weaknesses or significant weaknesses and then adjust upward that offeror’s proposed cost to account for the risk of unsuccessful contract performance. Those restrictions impose on the Government’s ability to use, release, or disclose that technical data and computer software outside the Government. SSAs would then use those discriminating assessments and resulting adjectival ratings, along with (if applicable) the SSEB’s MPC resulting from upward adjustments to offeror’s proposed costs contained in the offeror’s Cost/Price Volume to complete their tradeoff analysis consistent with the relative ranking of evaluation factors in Section M of the RFP to decide which offeror’s proposal represents the “best value” to the Government. (In contrast, if an RFP requires the agency to perform a price realism analysis in order to award a fixed-price-type contract, the FAR prohibits the agency from “dollarizing” weaknesses and significant weaknesses and adjusting upward offerors’ proposed prices.) Given these GAO bid protest decisions, it would be inappropriate to contend that “dollarizing” weaknesses or significant weaknesses in such a manner and then adding the results of those upward adjustments to the SSEB’s most probable cost calculations constitutes improper “double-counting”—for an agency is not precluded from considering an element of a proposal under more than one evaluation criterion where the element is relevant and reasonably related to each criterion under which it is considered.

G. Sole Source Contracts

1. Establish Data and Data Rights Requirements

Two of the steps described above to acquiring rights in technical data and computer software in a competitive environment apply equally to situations where the program office seeks to acquire supplies and services sole source. In other words, in order to establish its data and data rights requirements, the program office should first use the same disciplined approach to drafting an acquisition strategy and the RFP described in Sections V.B-D.

2. Understand The Offeror’s Proposed System and Software Architecture

Irrespective of whether the offeror proposes to deliver noncommercial or commercial technical data or computer software, the program office should require the offeror to identify where—consistent with MOSA principles—each major system component to be delivered as part of the major system platform will reside as depicted in its proposed SAD and WBS. The reason why is two-fold. First, to facilitate mapping of licenses to deliverables for the reasons described above, if the offeror can prove it developed a particular major system component exclusively at private expense, the Government may need to (1) create a new CDRL requiring the delivery of items developed exclusively at private expense separate from the existing CDRL that requires the delivery of all remaining components to be delivered as part of the major system.
platform, and (2) modify the Section J Data Rights Attachment so that it is clear what license(s) will apply to which software items delivered under which CDRL.

Second, the Government must ensure the offeror’s implementation of the funding rules was consistent with its proposed architecture. The reason why is because, if the offeror established an internal project charge code to allocate the cost of developing a particular item to an IR&D project but failed to use MOSA principles to segregate that item from all other items developed with mixed funding or developed exclusively at government expense in its architecture, it will be impossible for the offeror to partition all items delivered as part of the major system platform from each other as separate CDRL deliverables so that the appropriate markings are affixed to the appropriate parts of each deliverable. And if the offeror failed to develop its architecture using MOSA principles, the Government should take the position that in the aggregate the components to be delivered as part of the major system platform were developed with mixed funding—and therefore, the Government is entitled to receive government purpose rights to all noncommercial technical data associated with those hardware components and all noncommercial computer software components that reside within that platform.

3. Justify The Award Of A Sole Source Contract

The Air Force Federal Acquisition Regulation Supplement (AFFARS) states that the contracting officer cannot issue an RFP to a sole-source offeror unless the appropriate official has approved a Justification & Approval (J&A) authorizing the acquisition of supplies, services, or both, sole source. Although seven exceptions exist to the requirement to obtain full and open competition under the Competition in Contracting Act, only one of those exceptions relates to the topic of rights in technical data and computer software. That exception applies when the DoD demonstrates the supplies or services required are available from only one or a limited number of responsible sources when it is likely that award to any other source would result in substantial duplication of cost to the Government that is not expected to be recovered through competition or unacceptable delays in fulfilling the agency’s requirements (FAR § 6.302-1).

When attempting to rely upon that exception, some program offices assume that inclusion of a conclusory statement into their J&A such as “the data rights are too expensive” will suffice to convince the approving official to sign that document. For various reasons, that assumption is incorrect. First, those statements are usually not supported by any rigorous analysis regarding (1) what specific items of technical data and computer software the program office is referring to, (2) what specific rights to those specific items of technical data and computer software the program office is referring to, or (3) the manner in which the program office calculated the value of those rights to those items of technical data or computer software. Second, the FAR cautions that, although the existence of limited rights in data may make the supplies and services available from only one source, the mere existence of those rights does not in and of itself justify use of this exception.

In the alternative, some program offices assume that including other types of conclusory statements into their J&A like “the contractor refuses to sell rights to various
items of technical data or computer software” will suffice. Given the holding in a recent COFC decision that is currently on appeal to the CAFC, that would be an unwise assumption. Based upon the cautionary statement from the FAR mentioned above, the COFC held that the Government’s decision in 2006 to procure a weapon system that “locked in” the Government to the contractor’s technical data package (TDP) for the next 30-35 years was not a sufficient reason to justify a new contract as a sole source procurement. The reasons why is because the owner of IP may have the power to extract higher royalties or other licensing terms that reflect the absence of competitive alternatives. But that does not mean that that IP is not for sale at any price (however exorbitant)—a “supra competitive price”, to use the term coined by the COFC—for additional quantities of the weapon system because of the TDP.

In other words, unless the program office seeks a license to IP so unique as to be the equivalent of the trade secret formula for Coca-Cola® invented by John M. Pemberton in 1886, all IP licensed by the Department of Defense is available for a price. The only question that therefore remains is whether the price the Government would have to pay to acquire a Government Purpose Rights license to that IP sufficient to compete a follow-on acquisition would result in a substantial duplication of cost that could not be recovered through competition. In short, the program office must obtain a price from the contractor so it can include that information into its J&A as support for going sole-source.

In any event, if the program office intends to base its J&A in whole or in part upon the lack of rights in technical data and computer software sufficient to compete the acquisition of supplies and services needed by the program office, the J&A should include the following information consistent with the J&A Documentation Template referenced in the AFFARS:

a. Section V of the J&A Documentation Template. J&As that are based upon a determination that the program office would incur a substantial duplication of cost were the supplies and services to be competed must include the rationale for the amount of cost that would be duplicated. Accordingly, explain how the value of the technical data and computer software—and the associated rights—identified in Section IX of this template is subsumed within the amount of duplicated cost identified in this section.

b. Section IX of the J&A Documentation Template. Based upon the analysis performed consistent with Section III of this Handbook, identify what specific items of technical data and computer software—and the associated rights—the program office would need to compete the acquisition of supplies and services sought to be procured. Describe the approaches the program office used to calculate the value of those rights associated with those items of technical data or computer software (see Section V.G.4, below). Identify what rights the program office procured under existing contracts (see Section V.B.5, above).

c. Section XI of the J&A Documentation Template. Explain how the program office will attempt to acquire, as a priced option in the contract action that is the subject of the J&A, rights in technical data and computer software sufficient to compete follow-on
acquisitions for all or a portion of the supplies and services sought to be procured. Describe the actions the program office will take during the period of performance of the contract to identify, reverse engineer, or acquire technical data or computer software that not identified as a priced option in the contract action that is the subject of the J&A. State how the program office intends to challenge nonconforming or unjustified markings on technical data and computer software the contractor delivered to the Government under previous contracts so those markings can be removed so that that technical data and computer software may be used in support of a follow-on competitive acquisition. As required by Implementation Directive for Better Buying Power 2.0, discuss how the program office will take advantage of Open Business Model (i.e., MOSA) practices to break vendor-lock to minimize future sole source requests. Finally, the program office should keep in mind that, in accordance with DFARS PGI 206.304(a)(S-70), if the planned actions described in this section are not completed, a subsequent J&A for the same supplies or services must be approved at one level above the approval authority for the previous J&A unless the previous justification was approved by the Senior Procurement Executive (SPE)(in which case the approval remains at the SPE level).

4. Negotiate A Fair And Reasonable Price For The Rights To Data

The program office should not commence negotiations over, or request pricing for, data rights until the parties have arrived at a common understanding as to (1) the content of each CDRL the contractor will deliver, (2) the scope of the licenses that will apply to each CDRL, and (3) where each major system component to be delivered as part of the major system platform resides in the Offeror's proposed design of the major system platform. Once the parties have arrived at that common understanding, unless an exception applies to that acquisition, the offeror must provide certified cost or pricing data so that the Contracting Officer can determine the fairness and reasonableness of the proposed prices for the rights in technical data and computer software sought to be acquired.

The FAR defines “cost or pricing data” as all facts that, as of the date of price agreement, or an earlier date agreed upon by the parties as close as practicable to the date of price agreement, prudent buyers and sellers would reasonably expect to affect price negotiations significantly. The FAR also states that that data are factual (not judgmental, although they include the data forming the basis for that judgment) and encompass all facts that can be reasonably expected to contribute to the soundness of estimates of future costs and to the validity of costs already incurred. The FAR provides various examples of cost or pricing data, e.g., vendor quotations, nonrecurring costs, data supporting projections of business prospects and objectives and related operations costs, estimated resources to attain business goals, and information on management decisions that could have a significant bearing on costs.

So what does this mean in the context of rights in technical data and computer software? It means that, unless an exception applies to that acquisition, the contractor must provide certified cost or pricing data supporting its determination as to the value of the rights to a specific item of technical data or computer software.
Valuation of IP is a very complex subject—and it becomes even more complicated when one attempts to calculate the value of noncommercial technical data and computer software developed for military applications for which the marketplace is at best limited. There is no statute, regulation, or policy applicable to DoD contracts mandating that the parties utilize a specific approach for calculating a fair and reasonable price for the rights in technical data and computer software delivered under DoD contracts. (In fact, no resource issued by any DoD activity or the private sector other than this Handbook provides an extended treatment of this subject.) Put another way, the program office has the discretion to determine what methodology—and what cost or pricing data it should request consistent with that methodology—it should use to negotiate a fair and reasonable price for that IP.

Accordingly, a program office should consider using the methodology described below to negotiate the value of a specific level of rights to a specific item of technical data or computer software (e.g., CDRL) within the context of the statutory requirement to base the fairness and reasonableness of the negotiated price upon certified cost or pricing data. In this regard, program managers may want to retain a third-party valuation analyst to verify the offeror’s valuation of that technical data or computer software. For further details, contact the National Association of Certified Valuators and Analysts (NACVA) (http://www.nacva.com/) or the Licensing Executives Society (U.S.A. and Canada), Inc. (http://www.lesusacanada.org/).

a. The program office should require the offeror (or, if the owner of the IP in question is a subcontractor, its subcontractor) provide a copy of its written corporate policy for calculating the value of all IP in its corporate portfolio (e.g., patents, copyrights, trade secrets). The program office should also require the offeror to explain how it used that policy to calculate the value of the rights it proposes to deliver with the specific item of technical data or computer software at issue. If that policy exists but the offeror did not use that policy to calculate the proposed value, the program office should require the offeror explain why it did not use that policy in this case. If no such policy exists, the program office should require that the offeror affirmatively state that is the case.

b. The program office should require the offeror (or, if the owner of the IP in question is a subcontractor, its subcontractor) provide a copy of all financial statements (consolidated balance sheets) that summarize the value of all IP in its portfolio irrespective of whether the offeror included those financial statements in any of its U.S. Securities and Exchange Commission (SEC) filings. If the offeror is not a publicly traded company, the program office should require the offeror to provide equivalent information.

In either case, the program office should require that the offeror identify where the value of all IP in its portfolio is contained in those financial statements or equivalent information (e.g., as intangible assets). The program office should also require that the offeror explain how it subsumed the proposed price for the value of the rights it proposes to deliver with that specific item of technical data or computer software at issue within the total value of all IP within that portfolio reflected in the offeror’s financial statements.
(consolidated balance sheets) or equivalent information. If the former is not subsumed within the latter, the program office should require the offeror explain why that is the case. If the offeror does not summarize the value of all IP in its portfolio on its financial statements (consolidated balance sheets), the program office should require that the offeror affirmatively state that is the case.

c. Over the years, the accounting profession has settled on three general methods of calculating the value of IP: The cost approach, the market approach, and the income approach.\(^{22}\) The following discussion of these three approaches is intended only to provide the reader with a very basic understanding and should not be considered a comprehensive treatment of this very complicated subject.

(1). The *cost approach* calculates the cost to create an exact duplicate or replica of the technical data or computer software at current prices (“reproduction cost new”) less depreciation, the cost to create the functional equivalent at current prices (“replacement cost new”) less depreciation, or the cost the contractor incurred when creating the technical data or computer software (“actual costs”) less depreciation. This approach is particularly applicable for an intangible asset that does not normally exchange in a secondary market.

Irrespective of what type of cost method is used, the calculation should account for the following cost elements: direct costs (material, labor, overhead), indirect costs (material, labor, overhead), developer’s profit, and entrepreneurial incentive (opportunity cost). The cost approach provides a reasonable value indication for a tangible asset when it includes all of these cost elements and when the analysis has been adjusted for all applicable forms of obsolescence (physical deterioration, functional obsolescence, and economic obsolescence). In the case of computer software, when using the “reproduction cost new” or “replacement cost new” method the program office may choose to use various software development effort estimating models (*e.g.*, COCOMO® II, KPLAN, SEER-SEM).

In the context of defense contracting, the “actual cost” approach can be particularly useful for two reasons. First, the DFARS requires that contractors and subcontractors at all tiers maintain records sufficient to justify the validity of markings that impose restrictions on the Government’s ability to use, release or disclose technical data or computer software delivered or required to be delivered under the contract or subcontract. Those records include:

- The signed memorandum from the contractor’s management that established the IR&D project’s purpose, established its budget, and identified the specific internal project charge code to which employees’ time should be charged when

---

developing that particular item of technical data or computer software. As stated above, to be properly classified as IR&D, both the cost principles (FAR § 31.205-18(a)) and the Cost Accounting Standards (CAS § 9904.420-30(a)(6)) state that purpose cannot relate to performing any express requirement of a government contract.

- Accounting records contained in the contractor’s timekeeping systems demonstrating employees actually charging their time to that IR&D project along with those employees’ labor rates.
- An identification of where the item or component described by that technical data (or, for software-intensive systems, the software item/software subroutine) is identified in the offeror's proposed WBS and (for software-intensive systems) in its proposed SAD.
- Engineering notebooks.
- Drawing archives.
- IR&D reports.
- Technical papers and reports.

Second, the offeror has the burden of proving that a particular item of technical data associated with a major weapon system (i.e., ACAT I), subsystem or component was developed exclusively at private expense unless the major weapon system or a component of a subsystem was acquired as a commercial item. As described in Section V.B.2.g.(3) of this Handbook, this burden means the program office should require that the offeror demonstrate that it tracked the allocation of private and government funds to the development of the noncommercial item, component or process it accomplished with those funds and broke or separated the accounting trail for development of those technologies to indirect cost pools (e.g., IR&D), costs not allocated to a government contract, or any combination thereof. If it can do so, the offeror will have proved that it developed a particular noncommercial item, component or process (or all items, components or processes) described in a particular CDRL exclusively at private expense. The offeror must also demonstrate that its assertion that it developed the data exclusively at private expense is consistent with any CPRs submitted to the Government under any Government contract.

If the contractor cannot sustain its burden of proof in this regard by means of the types of records described above, the Government may presume that the Government has already paid those costs. Under those circumstances, the offeror should be willing to sell Unlimited Rights associated with that technical data to the Government at zero cost. In contrast, if the item, component or process to which that technical data pertains is a commercial item or COTS, the Government must presume that the offeror developed that item of technical data or computer software exclusively at private expense unless the Government can demonstrate that it contributed to the development of the item, component or process in question.

(2). The market approach estimates a value based upon an analysis of the sales and prices of guideline technical data or computer software. To implement this approach, the program office would (a) determine the criteria for selecting comparable
uncontrolled (arms'-length) transactions (CUT), (b) convert CUT prices to pricing metrics (e.g., price per drawing, price per line of code) that could be applied to the technical data or computer software at issue, (c) compare the CUT intangible assets to the technical data or computer software at issue, (d) select subject-specific pricing metrics derived from the CUT intangible assets, and finally (e) apply the selected pricing metric to the subject intangible asset to estimate a value.

This approach is particularly applicable where relevant CUT data exists. That data may be in the offeror’s possession or in government or commercial databases (e.g., SEC filings, GSA Federal Supply Schedules, company press releases, analyst reports, news articles, trade or industry journals, scholarly or academic publications, court decisions, KtMINE®, Royalty Connection™, RoyaltySource®, RoyaltyStat® LLC, Licensing Economics Review, IPRA, Inc.). When establishing and applying pricing metrics, the program office should consider various elements of comparison like the scope of license rights granted (e.g., geographic or territorial restrictions, duration, purpose restrictions), special financing terms or arrangements, the existence or absence of arms'-length conditions, economic conditions existing in the secondary market at the time the comparable transactions occurred, the industry within which the guideline intangible asset was used, who is responsible for continued development/commercialization/protection, and the inclusion of other assets in the sale or license of a portfolio of assets.

(3). The income approach analyzes the value today of future estimated net income the technical data or computer software may generate for whatever remaining expected useful life that technical data or computer software may have. When using this approach, the program office should (a) determine from whose perspective should it value the projected future net income to be generated by the technical data or computer software, (b) identify the length of time during which the net income is measured and the frequency of the income measurement, and finally (c) select the appropriate yield capitalization rate (present value discount rate) or direct capitalization rate (conversion of a perpetual income flow to present value). In doing so, the program office should use the following factors: market evidence, the risk associated with the offeror achieving the income projection, consistency with the income measured projected in the analysis, forward-looking, and consistency with the expected term of the income projection.

The accounting profession recommends use of the following factors when selecting which of the three approaches discussed above would be the most appropriate to use when calculating the value of a specific item of IP:

- Quantity/quality of available data.
- Access to available data.
- Supply of relevant transactional data.
- Type/nature of the intangible asset.
- Industry conditions in which the intangible asset operates.
- The bundle of rights included in the analysis.
- Statutory/judicial/contractual/administrative requirements and considerations.
- Informational needs of the customer.
• Purpose/objective of the analysis.
• Compliance with any relevant professional standards.
• Professional judgment and experience of the analyst.
• Instructions from legal counsel.

That profession also recommends using multiple approaches and determining the appropriate weighting to be assigned to each valuation approach.

For the reasons stated above, in the DoD environment, the actual cost method is particularly useful because the actual cost method is based upon documentation created at the time the contractor developed the technical data or computer software at issue. In contrast, the market method requires the existence of comparable CUT—and the income method requires that the parties foretell the future.

It may be difficult for a program office to conceive how it could use any of the three methods described above to estimate the value of rights to a specific item of technical data acquired under a DoD contract. Accordingly, we provide the following not-too-hypothetical scenario for the reader’s consideration: A program office wants to award a sole-source follow-on contract to the incumbent to acquire additional receivers, some of which will be of the identical configuration as the program office procured under the existing contract and some of which will be of a configuration that features improved capabilities. Although receivers procured under the existing contract came with a warranty, the contract also contained provisions permitting the program office to direct the contractor to perform out-of-warranty repairs based upon a price-per-repair rate included in the contract. The incumbent performed out-of-warranty repairs during the performance of the contract. As a result, both parties know precisely how many repairs occurred each year of contract performance and precisely how much each repair cost the program office.

Under the follow-on contract, the program office wants to acquire Government Purpose Rights to a TDP that would constitute a full design disclosure. As a result, the program office will be able to provide that TDP to offerors as government-furnished-information in order to compete depot-level maintenance of those receivers. If the program office acquires that level of rights to that technical data, however, the remaining value to the owner of that IP may be negligible. The reason why that is the case is because the contractor will no longer be in a sole-source position to gain the profit it would have otherwise received had the program office continued to have it perform those out-of-warranty repairs under the follow-on contract.

As a starting point, therefore, the parties could use the income approach to calculate the remaining expected useful life of that technical data. First, the parties would extrapolate data supporting projections of business prospects cost or pricing data (i.e., the historical repair incidence rate) to calculate the total quantity of future out-of-warranty repairs the incumbent would have otherwise performed under the follow-on contract on identical-configuration receivers each year after the warranty for those receivers had expired. Second, since no historical data exists for the repair-incidence-rate for improved-
capability receivers, the parties would perform a regression analysis to determine the probable repair-incidence-rate for out-of-warranty repairs the incumbent would have otherwise performed under the follow-on contract for those receivers each year after the warranty for those receivers had expired. Third, the parties would agree as to the profit percentage applicable to those out-of-warranty repairs the contractor would have otherwise performed each year. Fourth, the parties would multiply that percentage by the total number of out-of-warranty repairs the incumbent would have otherwise performed under the contract each year for both types of receivers. Fifth, the parties would discount that sum to present value for each year. The result will be a quantification of the profit (net income) it is likely the incumbent would have otherwise received were it to have performed all out-of-warranty repairs under the follow-on contract as it did under the existing contract.

H. Post-Award.

1. CDRL Review Upon Delivery

“Examples like the Challenger explosion . . . demonstrate the states of complacency and familiarity we can fall into when it comes to dealing with large technological decisions. This is not to say that we should become paranoid about technology, but there is much to be said for a healthy skepticism among engineers and nonengineers alike. The most dramatic failures have occurred in a climate of overconfidence and carelessness, and the least we can learn from those incidents is to be more vigilant. Accidents and near accidents remain our surest reminders that engineering is a human endeavor that takes place in the context of other human endeavors, including calculated risk and celebration. None of the sane among us willfully wishes to place fellow human beings in imminent danger, but we sometimes minimize or forget what dangers lurk among our technological creations. The surest way for us to be vigilant is to be aware of past mistakes and thereby to be armed with the evidence of case studies to bolster, when need be, our arguments against the launching of a space shuttle on a cold winter morning. . . .”

What is true in war and in systems engineering is true after award in the context of technical data and computer software rights: complacency kills. Moreover, like in war and in systems engineering, the root cause of such complacency in this context after award is usually attributable to a breakdown in discipline. Specifically, all of the program office’s hard work in negotiating rights in technical data and computer software prior to award will be for naught if it fails to ensure after award that the contractor is complying with the requirements of its contract relative to the rights in technical data and computer software.

the contractor ultimately delivers to the program office. By that time, the contractor may be experiencing “seller’s remorse” with respect to the rights in technical data and computer software it agreed prior to award to deliver to the program office after award.

The results of that breakdown in discipline in the program office usually manifest themselves in three ways. The first way is that program office negotiates away for a pittance after award via bilateral contract modifications to the rights it negotiated prior to award. Years later, the program office may regret acceding to the contractor’s demands. By that time, however, the program office will just have to live with those constraints on its ability to execute successfully the program. Of course, if the program office can no longer successfully execute the program due to that breakdown in discipline, the program manager and the Program Executive Officer may have to explain to their MDA why they ever permitted that situation to occur.

The second way for discipline to break down is for program office personnel to begin empathizing with the contractor’s complaints about the “proprietary” rights it freely agreed to relinquish prior to award associated with a specific item of technical data or computer software. Those personnel may then decide that this problem is so inconsequential that it must not get in the way of the parties achieving some allegedly critical milestone. In the alternative, those personnel conclude that the parties can sweep that problem under the proverbial rug or conclude that the parties can defer resolution of that problem to a more convenient time—which, of course, never occurs because those personnel then focus on meeting the next schedule-driven milestone.

Next, program office personnel enter into a verbal side agreement with the contractor relative to the level of rights associated with that item of technical data or computer software that is inconsistent with the express terms and conditions of the contract. Inevitably, those side agreements possess one or more of the following distinguishing features. First, those agreements may violate the U.S. Constitution because the program office will have never received consideration for relinquishing its IP rights without obtaining authority from Congress to do so. Second, those agreements may violate the CICA because the agreement may have surrendered Unlimited Rights in the types of technical data described in Section V.C.1.b of this Handbook to which the Government was otherwise entitled to receive pursuant to 10 U.S.C. § 2320 that are not in dispute. Third, the competition under which the program office ran the source selection may have been compromised because, had the contractor proposed the level of rights prior to award that it will now proposes to deliver after award, as discussed above, that fact “would have materially affected the source selection decision.” By this time, the contractor, having exploited the program office’s lack of discipline once, will seek to exploit it ad nauseam—so that reality will soon bear no relationship to the express terms and conditions of the contract.

This undisciplined approach to program management and proper contract administration is unwise at best, as it increases the probability that months or years hence, the program office will have to untie the Gordian Knot caused by mismarked CDRL deliverables or missing content in the CDRLs that it now desperately needs in order to
successfully execute the program. (Of course, by that time the program office personnel who created this situation will have received more prestigious assignments, promotions, and cash awards and military decorations based in part upon false pretenses, i.e., the “success” they achieved in meeting that allegedly critical milestone.) Only those who have spent years of their professional career handling such issues can truly understand the time and effort the program office will need to expend to bring successfully reality back into alignment with the terms and conditions of the contract.

The third way for discipline to break down is for the program office to be so mesmerized by the content of a contractor’s CDRL deliverable that it forgets to check whether the contractor has properly marked its deliverable with the proper restrictive markings (assuming the contractor should have affixed any markings to that deliverable). There is only one way to solve this problem: The program manager, the product support manager, and the Contracting Officer must implement procedures that ensure that the first thing the program office’s initial recipient of a CDRL delivered by the contractor will not do is start reviewing the content of the CDRL for accuracy and completeness or (worse yet) immediately distribute those trade secrets to any non-Government employee in a manner that may not be authorized by the contract.

Instead, with respect to technical data the recipient should verify that the cover page of the CDRL contains technical data rights restrictive legends identical to the restrictive markings required by the Data Rights Attachment described above for that CDRL. The recipient should then verify that no restrictive markings are included on any page of that CDRL that are inconsistent with the restrictive legends on that cover page. In a similar fashion, the recipient should ensure that, if the CDRL requires the delivery of computer software, all restrictive markings contained within that deliverable are identical to the restrictive legends required by the Data Rights Attachment described above for that CDRL. In this regard, the program office may want to use a computer software program to scan the CDRL for any “nonconforming” or “unjustified” markings using a commercial software program (e.g., IpScan). If it does not, the types of technical data or computer software restrictive markings the contractor may have affixed to that CDRL will be a “nonconforming” or an “unjustified” marking. For details regarding what are “nonconforming” and “unjustified” markings and how to handle those markings, see Section V.H.3 below.

Next, the recipient should read the licenses to understand precisely to whom they may furnish copies of that technical data and computer software for what purposes for what specified period. Then—and only then—should the recipient review the content of the CDRL for accuracy and completeness. Assuming the program office structured its Data Rights Attachment in a manner similar to that described above and trained its personnel to use the following decision tree, it should take the recipient of a CDRL less than 30 seconds to determine to whom that recipient can disclose that CDRL for what purpose(s) for what period:

a. Is the data contained in a CDRL? If the answer is no, read the license contained in subsection c.(5) of the Data Rights Attachment (see Appendix 1 (“Excerpts
from SE&I Follow-On RFP” Attachment 10)) and carefully read to whom that data may be used, released, or disclosed and for what purposes. If the answer is yes, go to the next question.

b. Is that CDRL listed in Table 3 of the Data Rights Attachment? If the answer is yes, the recipient should carefully read the license contained in subsection c.(3) to learn the conditions under which he/she may use, release, or disclose that technical data or computer software outside the Government. If the answer is no, go to the next question.

c. Is that CDRL listed in Table 2 of the Data Rights Attachment? If the answer is no, then that CDRL contains no commercial item technical data or computer software in which case the recipient should skip to question (4). If the answer is yes, does the license contained in Appendix A listed in Column 3 of that table associated with that CDRL encompass the technical data or computer software contained in that CDRL? If the answer is no, the CDRL must contain only noncommercial technical data or computer software, and the recipient should skip to question (4). If the answer is yes, the recipient should carefully read that license (or those licenses) and subsection c.(2) to determine to whom, for what purposes, for what duration of time, that commercial item technical data or software may be used, disclosed or released outside the Government. If (i) any technical data contained in that CDRL is marked in red as required by the Data Rights Attachment but Table 2 did not list that CDRL, or (ii) the license listed in Column 3 of that Table for that CDRL does not encompass the technical data contained in that CDRL, the recipient should notify the PCO immediately.

d. Since the CDRL contains only noncommercial technical data or computer software, the recipient should skim down Column 1 of Table 1 of the Data Rights Attachment until he/she locates the CDRL number. Go across that corresponding row and read the cell in Column 3 associated with that CDRL. If that cell contains the word “Unlimited”, there should be no restrictive marking on the CDRL and the recipient may use, release or disclose that technical data or computer software to anyone for any purpose. If, however, any restrictive markings are contained on that CDRL, the recipient should notify the PCO immediately. If that cell contains the word “Government Purpose”, that term should be in the restrictive marking on the CDRL and the recipient may use, release or disclose that technical data or computer software to authorized persons for government purposes. If, however, those words are not in the restrictive marking on the CDRL, the recipient should notify the PCO immediately.

2. Use, Release, And Disclosure Of Technical Data And Computer Software

The program office should use the following guidelines to determine whether it may release the technical data and computer software delivered under the awarded contract outside the Government.

Assuming that the technical data or computer software delivered to the program office is not subject to the Arms Export Control Act (e.g., a Distribution Statement “D” is not affixed to the cover page), if that noncommercial technical data or software contains
no restrictive markings it is presumed to have been delivered with Unlimited Rights. The program office may therefore release that item outside the Government without restrictions.

Section II.C of this *Handbook* describes to whom, for what purposes, and for what period of time noncommercial technical data or computer software the Government may use, release or disclose that item marked with Government Purpose Rights, Limited Rights, Restricted Rights, Specifically Negotiated Rights, or SBIR Rights restrictive markings outside the Government. The program office may only use, release and disclose commercial technical data and computer software in accordance with the terms and conditions of the license associated with those items. That is why the recipient of any CDRL should read the commercial licenses before reviewing the content of that CDRL for accuracy and completeness.

Finally, the program office should ensure that all conditions described in the NDA between its “covered Government support contractor” and the contractor who created that CDRL are satisfied prior to releasing or disclosing any CDRL to that “covered Government support contractor” to which is affixed “Limited Rights” or “Restricted Rights” restrictive markings or commercial technical data the content of which the Government did not acquire “Unrestricted Rights”. Of course, this condition only applies if the Government did not obtain a waiver of that requirement prior to award from the contractor who created that CDRL.

3. Identifying And Correcting Improperly Marked CDRLs

For the reasons described above, it is imperative that the program office ensure that proper markings are affixed to CDRLs delivered to it by the contractor. In this regard, a “nonconforming” marking is one that does not contain the following terms: “Unlimited Rights”, “Government Purpose Rights”, “Limited Rights”, “Restricted Rights”, or “Special License Rights”. (Examples of nonconforming markings include the terms “proprietary” and “competition sensitive.”) In contrast, an “unjustified” marking is one that is one that is described above (e.g., “Restricted”) but is not the level of rights to that CDRL the Data Rights Attachment described above required the contractor to deliver to the program office (e.g., “Unlimited”). In either case, the program office should immediately notify the Contracting Officer so the Contracting Officer may take appropriate action.

Specifically, the Contracting Officer should notify the contractor and request it remove that nonconforming marking and redeliver that deliverable with conforming markings at its own expense. If the contractor fails to do so, within 60 days, the Government may ignore or, at the contractor’s expense, remove or correct that nonconforming marking. If the contract includes DFARS § 252.227-7030 (“Technical Data—Withholding of Payment”), the Contracting Officer should also consider withholding payment of ten percent of the total contract price until such time as the contractor removes that nonconforming marking.
In contrast, if the contractor affixed an unjustified marking to the CDRL, the Contracting Officer must invoke the validation procedures described in the DFARS. Specifically, the Contracting Officer may first submit a prechallenge request for information to the contractor or subcontractor requesting that it provide a written explanation for any restrictions on the Government’s ability to use technical data or computer software. The request may include a statement of facts accompanied by supporting documentation. The contractor and subcontractor are required to have, maintain, and follow written procedures sufficient to assure that restrictive markings are used only when authorized by the terms of the contract, and maintain records sufficient to justify the validity of any restrictive markings on technical data or computer software. Accordingly, the type of records the Contracting Officer should request the contractor provide would include, but not necessarily be limited to, those records described in Section V.G.4 above.

Consistent with the funding rules described in Section V.B.2.g.(3) above, the Contracting Officer should request that the contractor or subcontractor submit those records in a manner that facilitates analysis. For example, if computer software residing within a subsystem consists of 115 different software items/software subroutines, the Contracting Officer should request the contractor or subcontractor provide the supporting documentation described above in a 3-ring binder as follows: Tab 1 should identify the first software item/software residing within that subsystem and provide a detailed written explanation of the facts upon which the asserted restriction is based. Immediately following that explanation should be the supporting documentation. The contractor or subcontractor would then use that format to populate Tabs 2 through 115 in that 3-ring binder. The written explanation should cross-reference specific pages in the memorandum and accounting records so that anyone reviewing the contents of any Tab could read the written explanation and quickly validate the basis of the contractor’s or subcontractor’s assertion that every single software item/software subroutine currently residing within that subsystem was developed exclusively at private expense. If the name of a project changed over time, the written explanation should so state. If any of those 115 different software items/software subroutines were not developed exclusively at private expense, the contractor or subcontractor would identify those items/subroutines and then identify which of those items were developed with mixed funding or exclusively with government funds.

If the prechallenge request is associated with asserted restrictions affixed to technical data associated with a major weapon system (i.e., ACAT I), subsystem, or component, the request should also note that the contractor or subcontractor has the burden of proving the validity of its assertion that any item of technical data or computer software to which the asserted restriction applies were developed exclusively at private expense unless the major weapon system or a component of a subsystem was acquired as a commercial item. In contrast, if the technical data pertains to a commercial item or the computer software is a commercial item, then the Contracting Officer must presume that the contractor’s or subcontractor’s asserted restrictions are justified on the basis that
the item, component, or process was developed exclusively at private expense unless the Contracting Officer has information to the contrary.

In any case, the Contracting Officer may make a formal challenge to the “unjustified” restrictive marking. The program office has three years from the date the contractor delivers the technical data or computer software to the program office, or three years following final payment under the contract, whichever is later, to challenge the validity of a restrictive marking affixed to that data or software. The written challenge must state the basis for the challenge, require the contractor to respond with 60 days and provide justification for the assertion based upon records kept that are reasonably available to the contractor in sufficient detail to enable the Contracting Officer to determine the validity of the asserted restrictions, and state that a Contracting Officer’s final decision or decision by a court or the Armed Services Board of Contract Appeals (ASBCA) shall serve as justification for the asserted restriction. If the contractor fails to respond to the challenge, or the Contracting Officer determines that the contractor’s written explanation for the asserted restriction is unjustified, the Contracting Officer shall issue a final decision pertaining to the validity of the asserted restriction.

If, however, the Contracting Officer determines the contractor’s written explanation validates the claimed asserted restriction, the Contracting Officer shall issue a final decision validating the asserted restriction. If the Contracting Officer’s final decision denies the validity of the asserted restriction, the Government must still honor that restriction for 90 days or one year from the date of that decision to allow the contractor to appeal to the ASBCA or the COFC, respectively. (Between the date that final decision is issued, and the periods specified above, only the Secretary of the Air Force is authorized to determine that urgent or compelling circumstances do not permit awaiting the filing of suit—and if the Secretary determines those circumstances exist, they must notify the contractor accordingly.) After that period, the Government may strike, correct, or ignore the restrictive marking. If upon final disposition of that litigation the Contracting Officer’s decision is sustained, the restrictive marking shall be cancelled, corrected or ignored, and if that restriction was not substantially justified, the contractor shall be liable to pay the Government its costs of reviewing the asserted restriction and the fees and other expenses incurred by the Government in challenging the restriction unless special circumstances would make such a payment unjust. Conversely, if the Contracting Officer’s decision is not sustained, the Government shall be bound by the asserted restriction and if the Government’s challenge was not made in good faith, the Government shall be liable to pay the contractor fees and other expenses incurred by the contractor in defending the restriction.

When reviewing the contractor’s response to either the Contracting Officer’s prechallenge request for information or to a formal challenge that provided the information described in Section V.G.4 above, the Contracting Officer should compare that information with information in the program office’s possession listed in Section V.B.5 above. The following hypothetical examples are provided for the reader’s consideration:
The noncommercial technical data in question—a full design disclosure TDP containing detailed manufacturing process data for a component—is affixed with a Limited Rights restrictive marking. The SOW and a CDRL in the contract required the contractor to develop and deliver that TDP to the Government. The contract incorporated by reference DFARS § 252.227-7013, and included a WBS written to the level of that component consistent with Section 2.1 of the program's SEP. The contractor's substantiating records indicate that it allocated all costs of the development of the component's TDP to an IR&D project, contrary to FAR § 31.205-18. However, the contractor's CPR CDRL submitted during contract performance indicate the costs to develop that component—and thus the costs the contractor incurred to develop that TDP—were funded with both contractor funds and Government funds. Unless the parties otherwise agreed in the contract prior to award, the Government acquired Government Purpose Rights to that TDP.

The commercial technical data in question—an ICD—is affixed with a restrictive marking. In other words, that commercial technical data contains form, fit, and function data (e.g., data that describes the physical characteristics of a 120V AC electrical plug including the dimensions of each prong and their spatial relationship to each other). The contract under which the contractor delivered that technical data incorporated by reference DFARS § 252.227-7015. Unless the parties otherwise agreed in the contract prior to award, the Government is entitled to Unrestricted Rights in that technical data.

A contract required the contractor to develop a noncommercial software-intensive system in accordance with MOSA principles. That major system platform is comprised of 328 noncommercial major system components (in this case, software items/software subroutines), 200 COTS major system components, and 75 OSS major system components. The SOW and CDRL in the contract required the contractor to develop and deliver this software-intensive system, including major system ICDs and a SAD that described the relationship between all noncommercial, COTS, and OSS major system components residing within the system. The WBS appended to the contract identified all such components at the appropriate level of indenture. The contractor's substantiating records demonstrate it created 28 of those noncommercial major system components prior to award, the development of those components was not specifically required in the performance of any government contract ever awarded to it by any Federal agency since the contractor or any of its predecessors in interest came into existence, and that it properly allocated the costs to develop those components to an IR&D project—including the costs to develop the major system interface control documents between some of those 28 noncommercial components. The contractor's CPR CDRL submitted during contract performance indicate the costs to develop the remaining 300 noncommercial major system components were developed exclusively with Government funds. Unless the parties otherwise agreed in the contract prior to award, the Government acquired Government Purpose Rights to all major system ICDs between all noncommercial, COTS, and OSS major system components in the systems'
software architecture, Unlimited Rights to 300 noncommercial major system components, Restricted Rights to the remaining 28 noncommercial major system components, and commercial licenses to the remaining 200 COTS and 75 OSS major system components residing within the system.

4. Delivery Of Technical Data/Software Created During Contract Performance That Was Not Expressly Identified In The Contract

If the Deferred Ordering clause (DFARS § 252.227-7027) is contained in the contract, the program office may require the contractor to deliver any data or software to the program office, not expressly identified in the contract but generated in the performance of the contract or any subcontract, anytime during performance of the contract or within three years after acceptance of all items (other than technical data or computer software). If that clause is not included in the contract and the data or software is not the subject of a CDRL, the program office will not be able to require the delivery of that data or software under the Changes Clause.

5. Correction Of Defective Technical Data Or Computer Software

With respect to technical data, if the program office discovers that the technical data delivered by the contractor is defective, the program office has three years to obtain the remedies described in DFARS § 252.246-7001 (“Warranty of Data”) from the date of delivery if that clause was included in the contract. Those remedies include requiring the contractor to correct or replace at the contractor’s expense the nonconforming technical data, a downward adjustment of the price of that technical data, or correcting or replacing the nonconforming technical data and charging the cost to the contractor. With respect to computer software delivered under a fixed-price contract, the program office receives only that warranty for which it bargained under the contract; if it did not purchase an express warranty, its remedies are limited to those described in FAR § 52.246-2 (“Inspection of Supplies – Fixed Price”): latent defects, gross mistakes amounting to fraud, or fraud. With respect to computer software delivered under a cost-reimbursable or time-and-materials/labor-hour contract, FAR § 52.246-3 (“Inspection of Supplies—Cost-Reimbursement”), FAR § 52.246-6 (“Inspection—Time-and-Material and Labor-Hour”), and FAR § 52.246-8 (“Inspection of Research and Development—Cost-Reimbursement”), states that if the program office discovers within six months of delivery (or other period specified by the contract) that the computer software delivered is defective, it may require the contractor to replace or correct nonconforming computer software at no increase in fee (although in most cases it will have to pay the contractor the costs it incurred to correct those defects).

6. Changes In Requirements

If requirements change after award so that the program office must modify the contract to require the contractor to deliver additional CDRL items (i.e., additional items of technical data or computer software) or additional CDRL content in pre-existing CDRLs, the program office should revise its Data Rights Attachment to add those items. The program office should then obtain certified cost and pricing data for the rights in
technical data and computer software for those items, require the contractor to revise their DFARS § 252.227-7017 certification/representation and provide copies of any applicable commercial licenses, review those licenses for consistency with the Government’s minimum needs, and bilaterally modify the contract accordingly. For details, see Section V.G of this Handbook.

7. Post-Award Analysis Of Rights In Technical Data And Computer Software

Occasionally, the program office may need to analyze the rights in technical data and computer software it purchased under one or a myriad of contracts over the past decade (or more) because it failed to use an approach similar to that recommended above to expressly identify its technical data and computer software rights requirements under those contracts prior to award. Instead, the program office merely incorporated by reference standard FAR or DFARS clauses—or even worse, failed to include the DFARS § 252.227-7017 certification/representation into Section K of the RFP.

The circumstances under which the program office may need to perform that analysis include: (1) determining whether the program office acquired sufficient rights in technical data or computer software to compete follow-on acquisitions or, conversely, (2) whether the program office may be forced to acquire supplies/services sole-source because it did not acquire sufficient rights in technical data or computer software to compete that acquisition. Those circumstances may also include determining whether the program office may release technical data or computer software to covered government support contractors so those contractors can advise the Government regarding the accuracy and completeness of that technical data or computer software. The types of documents the program office will need to perform that analysis include, but are not limited to, the sources of information listed in Sections V.B.5 and V.G.4.c.(1) of this Handbook.

If the Government did not use the disciplined approach described in Section V above to acquire various rights under multiple contracts over the past decade (or more), the analysis described above can literally take months to complete. Similarly, if the program office must use litigation to get the contractor to remove an “unjustified” marking after implementing the formal challenge procedures, that litigation could take as long as 9.5 years to resolve. (Of course, after the litigation has run its course, the value of that technical data or computer software to all parties may be negligible.) Thus, the benefits of structuring the RFP using the approach recommended above are three-fold. First, that approach will facilitate proper acquisition planning. Second, it will reduce the probability that the program office must perform a complicated technical data/computer software rights analysis years after contract award. Third, it will reduce the probability that litigation may be necessary to resolve a dispute between the contractor and the Government regarding what rights the Government actually purchased under those multiple contracts.

VI. Epilogue
Although complicated statutes and regulations govern the proper acquisition and enforcement of rights in technical data and computer software, anyone can master those resources by taking the time to understand “why” rights must be acquired, “what” rights must be acquired, when” rights may be acquired, and “how” rights may be acquired. Moreover, this topic becomes relatively easy to understand when one keeps in mind the following principles discussed above. First, a program office acquires only a license—not ownership—to use, release and disclose technical data or computer software outside the Government. Second, a program office needs to carefully determine during formulation of an acquisition strategy who will need to use technical data and computer software delivered after award for what specific purpose it intends to use, release or disclose that technical data or computer software for what specified period. Third, if a program office carefully structures licensing provisions in its RFP it can more effectively evaluate offerors’ proposals prior to award and ensure delivery of the appropriate licenses after award. If you keep these principles in mind, you will enhance competition and increase SMC’s ability to develop, produce and sustain the space system and its subsystems over their life cycle thereby helping to achieve SMC’s mission: To deliver resilient and affordable space capabilities for the nation.
Appendix 1

Relevant Excerpts from GPS SE&I Follow-On RFP
Appendix 2

Relevant Excerpts from GPS OCX Phase B RFP
Appendix 3

Relevant Excerpts from GPS III RFP