Intellectual Property Guidebook for DoD Acquisition

30 April 2025

Office of the Under Secretary of Defense
for Acquisition and Sustainment

Washington, D.C.

Distribution Statement A. Approved for public release: distribution is unlimited.

Approved by

TENAGLIA.JOHN.M.[redacted] Digitally signed by TENAGLIA.JOHN.M.[redacted]

30 April 2025

John M. Tenaglia

Date

Principal Director,
Defense Pricing, Contracting, and Acquisition Policy
OUSD A&S/DPCAP

Intellectual Property Guidebook Change Record

Date	Change	Rationale

This page is intentionally blank.

CONTENTS

SECTION 1: BACKGROUND 7

1.1. INTRODUCTION 7

1.2. INTELLECTUAL PROPERTY (IP) POLICY IN THE DEPARTMENT OF DEFENSE 8

1.3. FEDERATED IP CADRE 9

SECTION 2: FUNDAMENTAL CONCEPTS OF IP 10

2.1. BUILDING BLOCKS OF IP ACQUISITION 10

2.2. IP AND RETURN ON INVESTMENT (ROI) 11

2.3. IP AND COMPETITION 12

2.4. IP AND MODULAR OPEN SYSTEM APPROACHES (MOSA) 13

2.5. STANDARD DEFENSE FEDERAL ACQUISITON REGULATIONS SUPPLEMENT (DFARS) DATA RIGHTS 14

2.6. SPECIAL CATEGORIES OF DATA 16

2.7. FUNDING TEST AND DETERMINING STANDARD RIGHTS 21

2.8. THE DOCTRINES OF SEGREGABILITY AND MODULAR LICENSING 23

2.9. MISCONCEPTIONS ABOUT IP AND DATA RIGHTS 25

SECTION 3: THE 5W'S OF THE IP STRATEGY (IPS) 26

3.1. WHAT IS THE IPS? 26

3.2. WHY IP IS CRITICAL TO THE PROGRAM? 27

3.3. WHERE IS IPS DIRECTION? 29

3.4. WHEN IS THE IPS PREPARED? 29

3.5. WHO IS RESPONSIBLE FOR THE IPS? 30

3.6. IPS ATTRIBUTES 31

SECTION 4: DEVELOPING THE IPS 33

4.1. GATHER INFORMATION 33

4.1.3 IP REQUIREMENTS TO SUPPORT ENGINEERING AND TECHNICAL OBJECTIVES AND ACTIVITIES. 34

4.1.4 IP REQUIREMENTS TO SUPPORT ACQUISITION/BUSINESS OBJECTIVES AND STRATEGIES 36

4.1.5 IP REQUIREMENTS TO SUPPORT LIFE CYCLE PRODUCT SUPPORT (PS) 37

4.1.6 CONNECT DATA REQUIREMENTS TO DELIVERY REQUIREMENTS BY DETERMINING USE CASES: 38

4.1.7 BENEFITS OF USE CASES 40

4.1.8 CONDUCT MARKET INTELLIGENCE 41

SECTION 5: IMPLEMENT THE IPS 49

5.1. FIVE MAJOR STEPS TO CONTRACTING FOR IP 49

5.2. DETERMINE CONTRACT STRATEGY 49

5.3. DRAFT AND ISSUE THE SOLICITIATION 56

5.4. IMPORTANCE OF IP DELIVERABLES 60

5.5. EVALUATE IP AND DATA RIGHTS IN PROPOSALS (SOURCE SELECTION) 62

SECTION 6: MANAGING/ MAINTAINING THE IPS 67

6.1. INSPECTING AND ACCEPTING DATA DELIVERABLES 67
6.2. MAINTAINING DATA RIGHTS 69
6.3. VALIDATING RESTRICTIONS AND DATA RIGHTS CHALLENGES 71
SECTION 7: CONCLUSION 74
SECTION 8: GLOSSARY 75
APPENDIX A: REFERENCES 78
STATUTES 78
POLICY AND REGULATIONS 78
REGULATORY REFORM 79
KEY REFERENCES 79
APPENDIX B: TOOLS AND RESOURCES 81

TABLES

TABLE 1. STANDARD DFARS LICENSE RIGHTS (E.G., "DATA RIGHTS") 15
TABLE 2. SPECIAL CATEGORIES OF DATA 20
TABLE 3. ATTRIBUTES TO INTEGRATE IN AN IPS 31
TABLE 4. ATTRIBUTES TO AVOID IN AN IPS 32
TABLE 7. POTENTIAL SOURCES OR TACTICS FOR OBTAINING IP 46
TABLE 8. DFARS IP REQUIREMENTS RULES OF ENGAGEMENT 51
TABLE 9. OTHER TRANSACTIONS ISSUE TOPICS AND CONSIDERATIONS FOR IP 54
TABLE 10. DATA ORDERING TOOLS 59
TABLE 11. CHARACTERISTICS OF IMPROPER MARKINGS 68

FIGURES

FIGURE 1. SIGNIFICANT IP POLICY EVENTS 8
FIGURE 2. SIX CORE IP PRINCIPLES 9
FIGURE 3. BUILDING BLOCKS OF IP ACQUISITION 10
FIGURE 4. POTENTIAL NEGATIVE EFFECTS OF VENDOR LOCK 13
FIGURE 5. OMIT DATA VS. DMPD DATA 19
FIGURE 6. MAPPING NONCOMMERCIAL DATA RIGHTS AND DEVELOPMENT FUNDING 23
FIGURE 7. SWISS CHEESE DATA RIGHTS 24
FIGURE 8. THREE PHASES OF AN IPS 26
FIGURE 9. EXAMPLES OF PROGRAM UNCERTAINTY AND IP MITIGATION STRATEGIES 29
FIGURE 10. THREE STEPS TO DEVELOP AN IPS 33
FIGURE 11. OBJECTIVES OF THE DATA MANAGEMENT IPT 33
FIGURE 12. EXAMPLES OF ENGINEERING/TECHNICAL DATA REQUIREMENTS 34
FIGURE 13. EXAMPLES OF ACQUISITION/BUSINESS DATA REQUIREMENTS 36
FIGURE 14. EXAMPLES OF PS DATA REQUIREMENTS 37
FIGURE 15. IP USE CASE DEVELOPMENT: FILL-IN-THE-BLANK 39
FIGURE 16. IP USE CASE DEVELOPMENT: 5 W'S 39
FIGURE 17. FIVE MAJOR STEPS TO CONTRACTING FOR IP 49

FIGURE 18. CONTRACTING CONE 50
FIGURE 20. IMPORTANT INFORMATION FOR NEGOTIATIONS 64
FIGURE 21. IMPLEMENTING THE IPS THROUGH CONTRACTS 73

SECTION 1: BACKGROUND

1.1. INTRODUCTION.

Purpose:

"A strong IP system benefits every innovative community across America, from rural towns to bustling cities."[1] Department of Defense (DoD) needs a thriving, innovative, and healthy Defense Industrial Base to develop advanced technology to achieve and maintain technological strength and achieve National Security objectives. IP protects industry innovation and generates revenue while also serving as a linchpin for national security.

DoD IP Acquisition has the challenge of meeting the DoD's mission for national security while incentivizing innovation in industry and protecting the nation's resources. This task places a monumental responsibility on DoD acquirers to balance the inherent need to justly pay industry for their development and encourage continued innovative work, while also being good stewards of taxpayer dollars by acquiring what is necessary to sustain defense capabilities and protecting the Government's ROI.

The primary purpose of this guidebook is to aid acquisition professionals in the development, execution, and management of effective IP Strategies that support all functional areas' requirements and objectives across program life cycle. It provides guidance on the implementation of IP laws and regulations, explains legal and operational challenges in acquiring IP and associated IP rights, and promotes partnerships with industry. This guidebook will also assist other Department organizations and requiring activities as they consider IP requirements and protections outside of programs of record.

This guidebook complements the most recent version of DoD Manual (DoDM) 5010.12 which is the authoritative source of guidance for properly requiring data in contracts.

Scope and Structure of the IP Guidebook.

- **Section 1** provides an **overview** of policies and statutes that direct IP practices in the DoD while considering the evolution of IP that led to the current priorities.
- **Section 2** offers a strategic overview of **fundamental IP concepts** which must be understood prior to undertaking any efforts to develop an IPS for a program.
- **Section 3** describes the **core principles of an IPS** and its vital role in a program.
- **Section 4** discusses essential elements and considerations in **developing an IPS** including identifying IP needs for a program, integrating IP into other acquisition plans, and preparing for successful execution in contracts.

[1] United States Patent and Trademark Office, Latest USPTO report finds industries that intensively use intellectual property protection account for over 41% of U.S. gross domestic product, employ one-third of total workforce (Mar. 17, 2022), https://www.uspto.gov/about-us/news-updates/latest-uspto-report-finds-industries-intensively-use-intellectual-property-0#:~:text=A%20strong%20IP%20system%20benefits,by%20workers%20in%20other%20industries.

- **Section 5** explains **how to effectively execute the IPS** through crafting solicitations, evaluating IP, and negotiating for IP.
- **Section 6** outlines the importance of **managing IP** during the performance of the program, including delivery of data, managing data rights, and continuous updates to the IPS.
- **Appendices A and B** provide source references, resources, tools and resources.

1.2. IP POLICY IN THE DOD.

Figure 1. Significant IP Policy Events

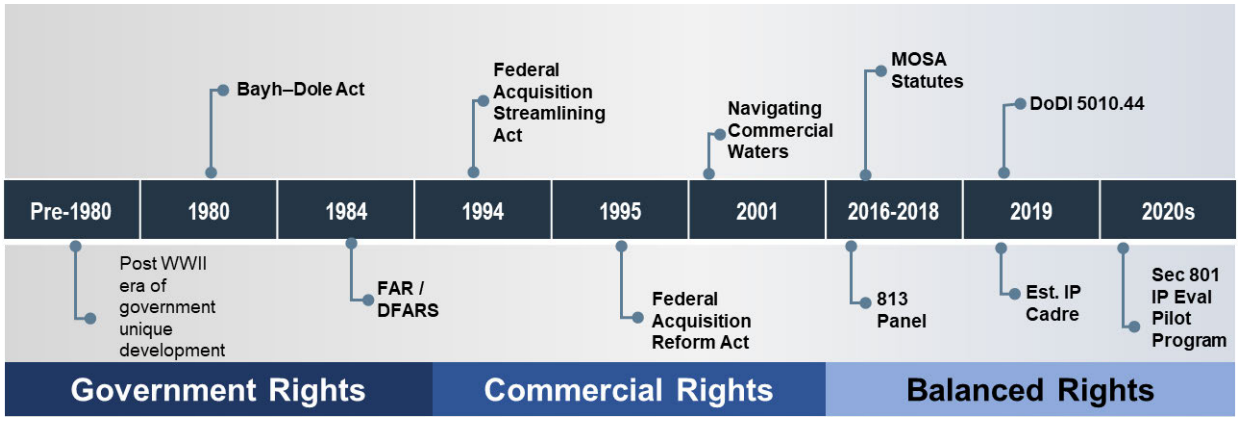


Figure 1 shows the evolution of IP policies and practices in the DoD which can be broken down into three general approaches to safeguarding the Government's rights and interests: a focus on the need to always acquire rights to all technical data (TD); a shift to the assumption that the Government needed little to no TD rights due to the focus on commercial; and currently an approach focused on tailored IP rights and a balancing of industry and DoD interests via Specially Negotiated License Rights (SNLRs), Other Transaction Agreements (OTAs), and MOSA.

In 2019, DoD issued the first consolidated IP acquisition policy for DoD: DoD Instruction (DoDI) 5010.44, IP Acquisition and Licensing, which provided six core principles regarding the acquisition, management, and licensing of IP (Figure 2).[2] These principles emphasize early life cycle planning, competitive acquisition of TD, interest-based negotiations, collaboration with industry, and tailored IP agreements.

[2] U.S. DEP'T OF DEF. INSTR. 5010.44, INTELLECTUAL PROPERTY (IP) ACQUISITION AND LICENSING 4 (16 Oct. 2019) [hereinafter DoDI 5010.44].

Figure 2. Six Core IP Principles

1) Integrate IP planning fully into the acquisition strategy (AS) and Product Support Strategy (PSS) to protect core DoD interests over the entire life cycle. Seek to acquire IP deliverables and license rights necessary to accomplish these strategies, bearing in mind the long-term effect on cost, competition, and affordability.
2) Ensure acquisition professionals have relevant knowledge of how IP matters relate to their official duties. Cross-functional input and coordination is critical to planning and life cycle objectives.
3) Negotiate specialized provisions for IP deliverables and associated license rights whenever doing so will more effectively balance DoD and industry interests than the standard or customary license rights. This is most effective early in the life cycle when competition is more likely.
4) Communicate clearly and effectively with industry regarding planning, expectations and objectives for system upgrade and sustainment. Avoid requirements and strategies that limit the DoD's options in accessing vital technology and commercial solutions available from industry [throughout the life cycle].
5) Respect and protect IP resulting from technology development investments by both the private sector and the U.S. Government (USG).
6) Clearly identify and match data deliverables with the license rights in those deliverables. Data or software deliverables are of no value unless and until the license rights to use it are attached, and the USG obtains and accepts those deliverables.

1.3. FEDERATED IP CADRE.

Under Section 838 of the NDAA for FY2020, Congress directed the establishment of the IP Cadre to ensure a consistent, strategic, and highly knowledgeable approach to acquiring or licensing IP by providing expert advice, assistance, and resources to the acquisition workforce on IP matters, including acquiring or licensing IP.[3] Recognizing the limited reach of a small OSD office and the criticality of robust accessible resources to the workforce, the functions of the IP Cadre extend to each Military Department (MILDEP) and to the Defense Acquisition University (DAU) with their own IP experts dedicated to assisting programs in the implementation of IP policy and best practices.

[3] *See* 10 U.S.C. § 1701 (2025).

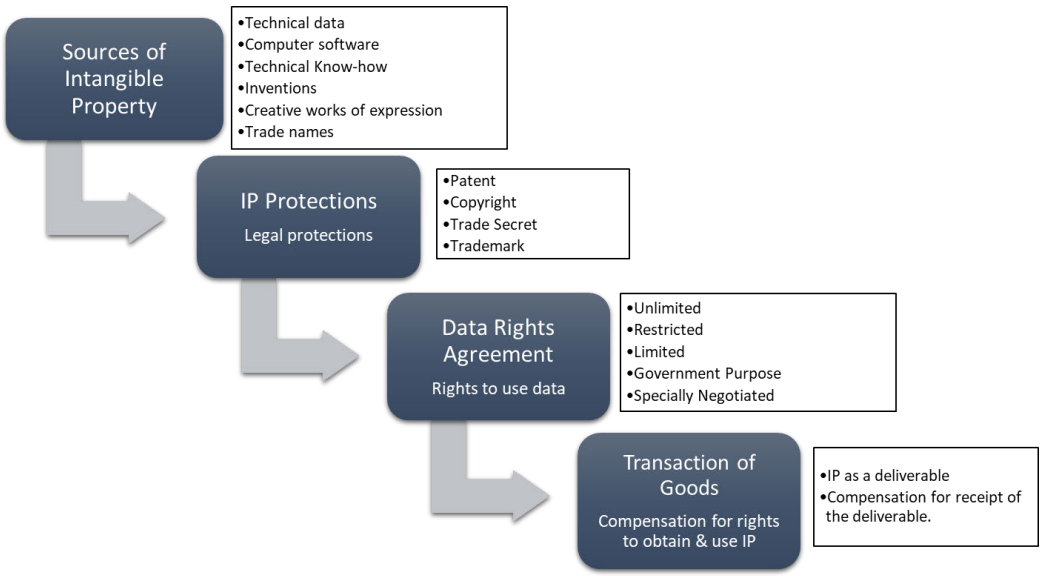
SECTION 2: FUNDAMENTAL CONCEPTS OF IP

2.1. BUILDING BLOCKS OF IP ACQUISITION.

IP is information, products, or services that are protected by law as a type of intangible property, including certain data (e.g., TD and computer software (CS)), technical know-how, inventions, creative works of expression, or trade names. Common types of IP include patents, trademarks, copyrights, and trade secrets.

In its simplest terms, IP acquisition is a transaction of goods: the deliverables and rights to use someone's IP in exchange for compensation. There are four key building blocks of this transaction: 1) types of intangible property sources; 2) the IP protection of that property; 3) the license agreement with the Government; and 4) the transaction of goods (deliverables) with the Government.

Figure 3. Building Blocks of IP Acquisition



1) The first building block to understand is that the creator of the IP is generally the sole "owner" of the IP. It is the sole property of the creator and remains the property of the creator throughout the transaction with the Government. The sources in this block are not necessarily IP unless they are protected by the legal protections in block 2. The Government does not "own" IP via a data rights agreement, even if the agreement is for Unlimited Rights. (There is a rare exception if the creator formally transfers ownership of the IP.)

2) The next building block includes the legal ways that creators are protected from others using their IP without permission and compensation. Patents, copyrights, trade secrets, and trademarks are the legal methods to protect the creator's rights and are foundational to many creators' business and licensing models. These protections allow the creator to justly receive

compensation for use of their IP. This is one mechanism to secure their return on their investment.

3) The third building block is where we start to frame the transaction through data rights agreements for specified IP. Data rights agreements are the mechanism by which the IP owner grants the license rights to use their IP with specified conditions or restrictions. The term "data rights" has historically been a short-hand way to refer to license rights acquired in copyrights and trade secrets relating to data deliverables — usually in the form of TD and CS. This approach to use the phrase "data rights agreements", allows DoD to use a single set of license rights to address what would otherwise be separate forms of IP protection for trade secrets and copyrights. "Data rights" do not cover patent or trademark rights.

4) Finally, the transaction can take place for data, CS, and rights in exchange for just compensation. This step includes the identification of what IP is being requested, in what form the data will be delivered, paired with what rights will govern its use, and finally an exchange of just compensation, all of which are documented through a contract or other agreement.

2.2. IP AND ROI.

IP Protections are a primary mechanism to secure ROI.

To secure the Government's ROI – Ensure the program obtains deliverables and rights to the Government's investment.

ROI is an important topic to understand in approaching interest-based negotiations and tailored IP agreements because IP is a form of business capital that provides competitive advantage. IP holds immense value for businesses, and they should have the ability to monetize that IP as revenue so that they can re-invest in new development, distribute to investors, or increase corporate capital and ultimately continue the business cycle. To enable that, the Federal Government promises exclusive legal control of qualifying IP.

It is important to remember that not all companies calculate ROI in the same way because companies have different values, strategies, goals, objectives, funding, etc. Additionally, understanding that ROI is both short-term and long-term is critical to identifying the IP value.

Alternatively, the ROI for the Government and DoD is inherently different from industry because the Government is not working for profit to re-invest and continue the business cycle. In the most general sense, the DoD's ROI is an enhanced, sustainable, and affordable capability for warfighters. As such, ROI is measured in ways such as cost avoidance savings that can allow for other investments, agility to rapidly meet new capability requirements, or the ability to sustain and repair critical aging equipment. Additionally, Congress has highlighted that a critical measure of ROI is making sure that DoD "does not pay more than once for the same work."[4]

Due to the shared investments in most DoD acquisitions, acquisition professionals must understand the competing interests of the DoD and private business throughout the acquisition process. The outcomes of IP agreements are a fundamental means to demonstrate the ROI for

[4] National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 813(b)(3)(A), (2015).

each party; on the one hand the Government receives data, CS, and rights to accomplish its mission, and industry receives initial monetary compensation and potentially long-term advantage.

Leveraging competition while encouraging industry innovation is the core of IP strategic analysis and planning.

2.3. IP AND COMPETITION.

In today's global military competition, DoD needs to encourage continuous technological innovation and question the notion that a single solution from a single vendor will necessarily meet the warfighter's needs for the life of a capability requirement. IP plays a critical role in fostering and enabling competition throughout the life cycle of a capability and was a cornerstone of the President's statement on competition in the defense sector evaluation of the state of competition in the country.

> *"IP, as a return-on-investment model, both encourages and restricts competition. From a technology standpoint, the IP statutory and regulatory framework should drive competition to create innovative technology as a prerequisite to qualify for IP protection. From a business standpoint, the resulting IP protection itself establishes a form of limited monopoly to commercialize that new technology, creating tension with competition. IP, as a form of legal protection, grants exclusive or limiting rights to individuals (e.g., inventors or authors) for their intellectual creations, such as inventions, works of art or music, or technical know-how. The exclusive rights and legal remedies granted to IP owners are not undesirable or problematic merely because they may restrict full and open competition for technologies protected by those exclusive IP rights*."[5]

The question then becomes — how can the DoD use IP to directly enable competition? In simple terms, having a competitive environment in the future requires taking advantage of a competitive environment in the present by including IP rights as part of competitive source selection evaluation to acquire the data, CS, and associated rights needed for future competition.

When the Government does not have the data, CS, and rights to enable continued competition, the program becomes forced into a sole-source situation, also known as vendor-lock. This is different from a deliberate sole source acquisition which may be desired based on market intelligence and a business case analysis of alternative acquisition strategies. In a vendor-lock situation, the program did not intentionally transition to a sole source but later realized the Government didn't acquire the necessary data, CS, and rights often because of poor IP strategic planning from the beginning of the program. The negative effect of a vendor-locked situation may include higher prices, inability for future technology insertion, stagnating the incentive for innovation, and potentially not receiving the best value to the Government.

[5] U.S. Dep't of Def., Rep., State of Competition within the Defense Industrial Base 7 (Feb. 2022).

Figure 4. Potential Negative Effects of Vendor Lock

- Encourages higher (non-competitive) prices
- Reduces incentive for innovation
- Limits technology insertion from other sources
- Weakens assurance of best value

The reason that absence of competition may stagnate innovation is because the original equipment manufacturer (OEM) has locked in long term ROI on the current IP/capability and therefore does not need to continue innovative development into solutions that may better meet the mission. Additionally, the lack of competition may limit the ability to compete for technology insertions unless the sole source provider delivers a MOSA solution with modular system interfaces (MSIs) that could mitigate the impacts of a single vendor.

To avoid vendor-lock, the DoD must appropriately recognize and plan for the impact of restrictive IP rights, and judiciously use competitive pressure, its market power, and all the other tools available to mitigate against undesirable restrictions on competition. With effective advance strategic planning the DoD can obtain sufficient IP rights to enable sustainment while incentivizing innovation and cost effectiveness in the defense industrial base.

2.4. IP AND MOSA.

MOSA is both an engineering (design) and business/acquisition (IP, contracting, competitive environment) approach to design, develop, and acquire systems in a modular, segregable, and standardized manner. MOSA consists of a technical and business architecture that supports using system interfaces compliant with widely supported and consensus-based standards, to the extent that standards are available and suitable to facilitate increased competition and innovation while yielding significant cost savings or avoidance, schedule reduction, opportunities for technical upgrades, increased interoperability, and other benefits during the sustainment phase. Using MOSA to the maximum extent practicable is a statutory requirement for all Defense acquisition programs[6].

IP rights and MOSA support each other. Modular systems are only effective with clear and robust understanding of each vendor's IP, the interfaces between them, and with the appropriate delivery of data to facilitate use of the interfaces. Without necessary IP, the Government may not reap the business benefits of a modular system, which is counter to the intent of MOSA. MOSA also enables and motivates better recognition of contractor and Government investments in development of a system. MOSA strives to keep the fruits of those investments separated to avoid inequities that can result when a minimal investment by one party can effectively capture the fruits of substantial investment by the other party. Without using MOSA, the Government may require delivery of much more contractor IP to meet its needs, raising costs and creating negotiation challenges.

[6] *See* 10 U.S.C. § 4401 (2025) [hereinafter § 4401].

NOTE: This is discussed at greater length in the "Implementing a MOSA for Department of Defense Programs", or addressed in short form as the MOSA Guidebook which is linked in Appendix A.

2.5. STANDARD DFARS DATA RIGHTS.

Table 1 below provides high-level definitions of standard data rights applicable to Federal Acquisition Regulation (FAR)-based contracts. Note that different clauses apply to commercial[7] and noncommercial[8] products and services for TD. Noncommercial software and documentation have their own clause[9] while commercial software has policy[10] but no standard clause. All contracts or solicitations for which any portion of contract performance is governed by Small Business Innovation Research Program (SBIR), or Small Business Technology Transfer Program (STTR) policies have a special clause for SBIR/STTR data.[11] See the actual DFARS clauses for complete definitions. These terms are **NOT** applicable in non-FAR based agreements such as OTAs. (See Section 5 for more information on OTAs.)

While the data rights categories include common terms, the categories are often used incorrectly or without the proper context. Remember these words have very specific regulatory meanings. Note that the term "noncommercial" is interchangeable with "other than commercial," since DFARS 252.227-7013 and 7014 utilize the term "Other Than Commercial Products and Commercial Services" and "Other Than Commercial CS and Other Than Commercial CSD."

For purposes of this guidebook, the term "noncommercial item" generally refers to "any product or service other than a commercial product or a commercial service.

[7] *See* DFARS 252.227-7015 (2025) [hereinafter 7015].
[8] *See* DFARS 252.227-7013 (2025) [hereinafter 7013].
[9] *See* DFARS 252.227-7014 (2025) [hereinafter 7014].
[10] *See* DFARS 227.7202-1 (2025).
[11] *See* DFARS 227.7104-4(a)(1) (2025).

Table 1. Standard DFARS License Rights (e.g., "Data Rights")

Standard Rights	Description
Unlimited Rights (*for noncommercial TD or CS*)[12]	▪ Unlimited Rights give the Government the ability to use, modify, reproduce, perform, display, release, or disclose the data i n any manner, and for any purpose whatsoever, and to have or authorize others to do so (absent any separate security classification or export control restriction).
Unrestricted Rights (for *commercial TD*)	▪ The Government shall have the unrestricted right to use, modify, reproduce, release, perform, display, or disclose commercial TD, and to permit others to do so for specific types of data. Of note, unlike the term "Unlimited Rights," the DFARS does define Unrestricted Rights themselves.
Government Purpose Rights *(for noncommercial TD or CS)*	▪ Government Purpose Rights give the Government the ability to reproduce, modify, perform, display, use, disclose, or release the data for Government purposes without restriction.[13] However, the Government cannot release the data for any commercial purpose. Government Purpose Rights expire after a time limit (the standard is five years after contract execution unless another time is negotiated in the contract) at which point the Government Purpose Rights become Unlimited Rights.
Limited Rights *(for noncommercial TD)*	▪ Limited rights apply to TD associated with noncommercial products only. The Government may use the TD within the Government but not release the TD outside of the Government except in limited circumstances. The Government may not use the data for manufacturing additional quantities of the item. However, the Government may share this data with a Covered Government Support Contractor (CGSC).
Restricted Rights *(for noncommercial CS)*	▪ Restricted Rights apply to noncommercial CS only. The Government may only run the software on one computer at a time and may make only the minimum copies needed for backup. The software may not be released outside of the Government except in limited circumstances and only after notice is provided to the owner. However, the Government may share this data with a CGSC.
Specifically Negotiated License Rights	▪ Specifically (or "Specially," as commonly referenced) negotiated license rights (SNLRs) agreements are statutorily preferred when the standard data rights arrangements defined in the DFARS do not meet the Government's needs; or when the Government is willing to accept lesser rights in exchange for other considerations. The SNLRs negotiation allows for a mutual agreement between an IP owner and the Government to find a better balance of interests for both parties. The new terms are spelled out in a unique SNLR agreement. A SNLR agreement pertaining to TD associated with noncommercial products or software is usually a compromise between Limited or Restricted, SBIR/STTR, Government Purpose, and Unlimited Rights. A SNLR agreement for this type of data must not result in the Government having lesser rights than Limited or Restricted Rights as defined in the DFARS.
SBIR /STTR Data Rights *(for noncommercial TD or CS)*	▪ SBIR/ STTR data rights apply to both TD associated with noncommercial products and noncommercial CS. These rights apply when the Government enters a research and development effort awarded as a SBIR contract. If a product was developed as part of an SBIR/STTR effort, the Government is entitled to SBIR/STTR Data Rights, which are generally equivalent to Limited or Restricted Rights, but for a period known as the SBIR/STTR protection period. After the SBIR/STTR protection period, the Government is granted Government Purpose Rights perpetually.
Commercial Data Rights *(for commercial TD)*[14]	▪ Similar to "Unrestricted Rights," the DFARS does not define the term "Commercial Data Rights." The Government may use, modify, reproduce, release, perform, display, or disclose TD within the Government only. The Government shall not—(i) use the TD to manufacture additional quantities of the commercial products; or (ii) release, perform, display, disclose, or authorize use of the TD outside the Government without the contractor's written permission unless a release, disclosure, or permitted use is necessary for emergency repair or overhaul of the commercial products furnished under this contract, or for performance of work by CGSC.

[12] As explained in Section 2.5, the term "noncommercial item" generally refers to "any product or service other than a commercia l product or a commercial service.

[13] A "Government purpose" means any activity in which the United States Government is a party, including cooperative agreements with international or multi-national defense organizations, or sales or transfers by the United States Government to foreign governments or international organizations. Government purposes include competitive procurement, but do not include the rights to use , modify, reproduce, release, perform, display, or disclose technical data for commercial purposes or authorize others to do so.

[14] For Commercial CS, there is no standard set of "data rights"; however, it is advisable to note the default policy for standard rights in commercial CS under the DFARS. It states that the DoD shall acquire commercial CS under the licenses customarily provided to the ***public*** unless such licenses are inconsistent with Federal procurement law or do not otherwise satisfy user needs. (Emphasis added).

2.6. SPECIAL CATEGORIES OF DATA

Confusion on the unique rights and limitations of these categories creates challenges for meeting DoD needs for data, CS, and rights. There are five main categories of data[15]:

- Operations, Maintenance, Installation, and Training (OMIT)
- Form, Fit, Function (FFF)
- Modular System Interfaces (MSI)
- CS Documentation (CSD)
- Detailed Manufacturing or Process Data (DMPD)

2.6.1 OMIT

OMIT is data necessary for operation, maintenance, installation, or training purposes (other than detailed manufacturing or process data). OMIT data will be required regardless of development funding when the Core Logistics Analysis determines there is a requirement for a core capability.[16]

As part of the "standard rights" for noncommercial items, DoD may require contractors to grant the Government Unlimited Rights in TD necessary for OMIT purposes, regardless of the source of development funding.[17]

2.6.2 FFF

Another special type of data is FFF data. FFF is defined in the commercial[18] and noncommercial[19] TD rights clauses and the SBIR/STTR data rights clause[20] as "TD that describes the required overall physical, functional, and performance characteristics (along with the qualification requirements, if applicable) of an item, component, or process to the extent necessary to permit identification of physically and functionally interchangeable items."

FFF is another type of data for which the Government may require Unlimited Rights (noncommercial) or an unrestricted right to use (commercial) regardless of development funding. It is not subject to a DMPD exclusion like OMIT data. However, like OMIT and DMPD, there is also possibility of FFF overlapping with DMPD. In this case, the data is treated as FFF for the purposes of determining rights regardless of the overlap. For example, DMPD for some physical part should have dimension and tolerance information and that same dimension and tolerance information would also be necessary in FFF data and therefore receives Unlimited Rights.[21] Traditionally, FFF data was used for what may now be viewed as an earlier incarnation of MSIs to enable MOSA. Until the MSI-related statutory requirements in 10 U.S.C. § 3771(b)(7) are

[15] There are other special categories such as test data, analyses, and studies that are not covered in this guidebook, but detailed information can be found in the DFARS. *See e.g.*, DFARS 227.71 (2025); *see also* DFARS 227.72 (2025).
[16] 10 U.S.C. § 2464 (2025), (hereinafter 2464).
[17] *See id.; see also* DFARS 252.227-7018(c)(1)(ii) (2025) [hereinafter 7018].
[18] *Id.* at (a).
[19] 7013, *supra* note 8, at (a).
[20] 7018, *supra* note 17, at (a); *see also* Class Deviation 2020-O0007, Protection of Technical Data and Computer Software Under Small Business Innovation Research Program Contracts (2020) [hereinafter Deviation 2020 -O0007].
[21] *See* Sec. 2.8.2 for a detailed discussion of how FFF data can be used to implement MOSA objectives.

implemented in the DFARS data rights clauses, FFF data will play a major role in meeting program MOSA requirements

2.6.3 MSI

To implement MOSA, the Government will have to identify MSIs. MSIs are defined in 10 U.S.C. § 4401(c)(4) as "a shared boundary between major systems, major system components, or modular systems, defined by various physical, logical, and functional characteristics, such as electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software elements."[22]

MSI TD rights are defined in 10 U.S.C. § 3771(b)(7) for both mixed funding and exclusively private expense funding scenarios. When the DFARS is updated to reflect that definition, MSI TD will become a special type of data, and the Government will be able to require Government Purpose Rights in certain TD pertaining to MSIs. The data rights rules are expected to go into effect in the future; check with the legal office to verify they have been implemented.

2.6.4 CSD.

CSD is the software equivalent of what is traditionally considered OMIT. The DFARS defines it as "owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the CS or provide instructions for using the software."[23] As such, the Government is granted Unlimited Rights in CSD.

2.6.5 DMPD

DMPD is the TD that describe the steps, sequences, and conditions of manufacturing, processing or assembly used by the manufacturer to produce an item or component or to perform a process.[24] The license rights for DMPD depend on development funding or negotiation rather than automatically qualifying for Unlimited Rights like other forms of OMIT data.

The Government **can** order DMPD, and the contractor **can** agree to deliver it. But the Government cannot require the contractor to grant Unlimited Rights to DMPD related to privately developed products or processes.

DoD activities should be judicious in requiring such data, especially when DMPD is a result of investment made at private expense. However, when data and associated rights are truly needed for mission objectives (e.g., for statutory depot requirements[25], advanced manufacturing in a contested logistics environment, to supplement the supply chain for a long lead item, or when IP owners cannot meet DoD's operational objectives), the Government should detail the specific use case for the DMPD, then negotiate just compensation for the delivery and use of the DMPD for the particular component and uses. This is a guiding principle for tailoring license rights. In contrast, when DMPD is developed using Government funding, DoD activities should

[22] § 4401, *supra* note 6, at (c)(4).
[23] 7014, *supra* note 9.
[24] 7013, *supra* note 8.
[25] *See e.g.*, § 2464, *supra* note 16; 10 U.S.C. § 2466 (2025); 10 U.S.C. § 2469 (2025).

proactively plan to order necessary data and associated license rights in the contract and ensure delivery requirements are met to realize the Government's ROI.

There are some important considerations for acquiring DMPD:

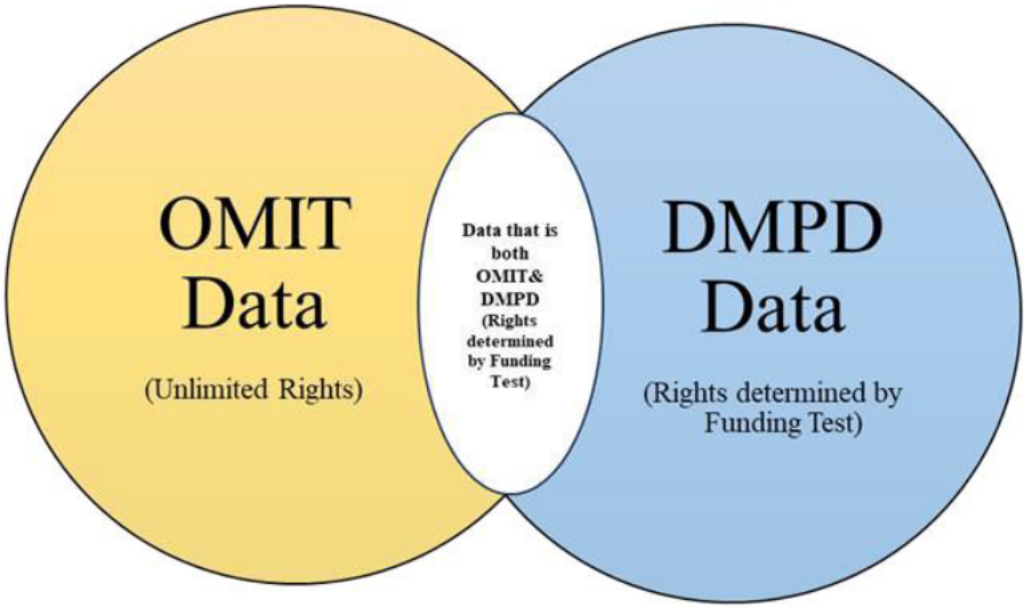
- DoD may acquire DMPD associated with commercial items **if** there is an applicable exception to the general policy which is to acquire only the TD customarily provided to the public with a commercial product, commercial service, or commercial process. [26]
- DMPD appears as a limitation in the data rights rules for TD. DoD may not normally share TD in which it has Limited Rights or SBIR/STTR Data Rights with third parties. However, in certain circumstances the Government may share DMPD data with third parties (e.g., for emergency repair and overhaul or for certain disclosures to a CGSC[27]).
- Reprocurement needs **may not** be a sufficient reason to acquire DMPD under two circumstances: 1) when items or components can be acquired using performance specifications, FFF data; **or** 2) when there are a sufficient number of alternate sources, which can reasonably be expected to provide such items on a performance specification or FFF basis.[28] While this is a true statement of a factual possibility, it is not a prohibition on requiring DMPD.

2.6.6 OMIT and DMPD Overlap.

What about data that is both OMIT and DMPD? For any portion of OMIT data that also qualifies as DMPD, Government rights in that DMPD will be determined by the usual application of the development funding test (rather than the standard grant of Unlimited Rights for OMIT data regardless of development funding). The OMIT rule excludes DMPD from both noncommercial[29] and commercial[30] TD that contractors may be required to grant Unlimited/Unrestricted Rights regardless of development funding. The DoD can require Unlimited Rights in OMIT data but not in DMPD data related to privately developed technology.

[26] *See* DFARS 227.7102-1(a) (2025).
[27] 7013, *supra* note 8, at (a); 7018, *supra* note 17, at (a); Deviation 2020-O0007, *supra* note 20.
[28] DFARS 227.7103-2(b)(1) (2025).
[29] 7013, *supra* note 8, at (c)(1)(v).
[30] 7015, *supra* note 7.

Figure 5. OMIT Data vs. DMPD Data



This DMPD exclusion mentioned above does not prohibit sale or delivery of that DMPD by the contractor. If specific data is necessary for OMIT purposes but is also DMPD used for detailed manufacturing or process, it can be requested by the Government in the requests for proposal (RFP). The contractor may agree to deliver or furnish this data, but the Government cannot compel the contractor to provide it. This exclusion is often a point of confusion and misused as a justification to avoid providing any DMPD or OMIT data.

Plain English: If technical data is considered both necessary for OMIT purposes and DMPD, the rules for DMPD apply regarding standard rights. This does not relieve the contractor of providing the data necessary for OMIT, but the data may not be required to have Unlimited/Unrestricted Rights.

Table 2. Special Categories of Data

Categories	Definition/Description	Example Uses	Example Data Products
Detailed Manufacturing or Process Data (DMPD)	▪ TD that describes the steps sequences and conditions of manufacturing, processing or assembly used by the manufacturer to produce an item or component or to perform a process.[31]	▪ Depot level repairs (when a repair requires DMPD that the SAE GEIA-STD-0007 standard cannot address, use MIL-STD-31000)	▪ Additive Manufacturing requires DMPD data to 3D print or manufacture spare parts and components and SNLRs when development was funded at private expense
Form, Fit, & Function (FFF)	▪ TD that describes the required overall physical, functional, and performance characteristics (along with the qualification requirements, if applicable) of an item, component, or process to the extent necessary to permit identification of physically and functionally interchangeable items.[32]	▪ Design interface ▪ Sustaining engineering ▪ Support equipment ▪ Facilities and infrastructure ▪ Maintenance planning and management ▪ Performance & Impact analysis, ▪ Design conformance	▪ Engineering drawings (e.g., Design/ Interface control-type drawings, performance specifications), configuration management, SysML/UML models, interface control documents, wiring diagrams, some provisioning data. ▪ Depot maintenance work requirements technical bulletin (dis-assembly and reassembly) repair and overhaul procedures. Engineering data for provisioning
TD necessary for Operation, Maintenance, Installation, or Training (OMIT)	▪ TD necessary for operation, maintenance, installation, or training purposes (other than detailed manufacturing or process data)[33]	▪ Maintenance planning and management ▪ Training and training support ▪ Supply support ▪ Packaging, handling, storage, & transportation ▪ Manpower and personnel ▪ Support equipment ▪ Design interface ▪ Performance of depot maintenance activities	▪ Level of Repair Analysis (LORA), Failure Mode, Effects, and Criticality Analysis (FMECA), Middle-Tier Acquisition, Reliability-Centered Maintenance, FTA, bill of materiel, Logistics Product Data, Engineering data for provisioning, screening data, preliminary provisioning parts list, provisioning parts list, test incident reports, diagrams, XML, schematics, quality reports, quality deficiency reports, provisioning conference, physical configuration audit ▪ Modeling & Simulation referent data
CSD	▪ TD that describes owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium that explain the capabilities of the CS or provide instructions for using the software."	▪ IT Systems Continuous Systems Report ▪ Performance of depot maintenance activities	▪ Software user manual

[31] 7013, *supra* note 8, at (a).
[32] *Id.*
[33] *Id.* at (c)(1)(v), note there is not a formal definition of OMIT in the DFARS or statute.

2.7. FUNDING TEST AND DETERMINING STANDARD RIGHTS

2.7.1 Three funding sources: There are three basic funding scenarios in DoD acquisition that drive standard/default rights and create a consistent framework of ROI. The three scenarios are:

1. Industry as the sole developer/investor of IP
2. DoD as the sole developer/investor of IP
3. A joint development/investment arrangement

1. Industry as Sole Developer/Investor: In this scenario, the development of a capability is entirely funded by industry and DoD is a pure "consumer." In this role, industry has borne all the development risk and as the exclusive IP creator/owner, the contractor controls the IP and can impose limitations on who may have rights to it and required compensation. This is typically the situation for commercial items. A typical commercial consumer requires little IP to satisfy life cycle use and care of the product (e.g., a user manual and minimal care and maintenance instructions). Detailed design specifications, manufacturing information, and other TD or CS are not typically provided to commercial users.

Also, industry naturally seeks greater market power and ROI considering its private investments. DoD needs to be mindful of potential disincentivizing effects of constraining private ROI in its attempts to meet the mission and get a good deal. Constraining industry's IP ROI may discourage future investment or participation in the DoD market. Accordingly, the DoD should balance industry ROI concerns with DoD mission goals when tailoring and negotiating delivery requirements and associated data rights during the acquisition process to foster an ongoing relationship with industry.

Due to DoD's unique mission and regulations, the Government is likely to need additional data rights necessary for OMIT purposes, DMPD, and FFF data to conduct repairs and do more extensive maintenance organically down range or as needed for core logistics capability required by statute.[34] DoD may also require broader rights to software source code to address cyber vulnerabilities, mission assurance, or supply chain risk considerations. DFARS data rights allow for the acquisition of data for these purposes even though DoD did not invest in the development of the IP.

2. DoD as Sole Developer/Investor: In this scenario, the Government has either fully funded the industry's IP development, or the IP development was done organically by a Government organization (lab, engineering center, etc.) or individual Government employee[35] and subsequently transferred to industry through either a formal technology transfer (T2) program or as Government Furnished Information (GFI) on a program, the Government has unlimited rights to the IP.

Because the DoD has fully funded the initial risk-capital, it therefore should have Unlimited Rights to the IP. The Government should always make it a priority to secure those rights and

[34] *See e.g.*, § 2464, *supra* note 16.
[35] Government employee inventions made in the scope of their employment are subject to a determination of rights under Executive Order 10096 as to whether the invention should belong to the government or the inventor or the government should have license rights. In addition,

associated ROI through appropriate documentation, contracting language, and receipt of deliverables. The Government must order and receive the required deliverables to exercise its rights in that data.

NOTE: Even as sole investor, the Government must request delivery of its IP. The Government's rights due to its investment (the funding rule) are useless without delivery. Additionally, there will be costs associated with packaging deliverables (e.g., compiling software code or formatting and marking technical data for delivery, converting from contractor format to Government format), even if the Government invested in the IP's development.

3. DoD and Industry as Co-Developers/Investors: Most commonly, DoD capabilities are developed as a partnership between industry and Government. DoD and its industry partners are often co-investors and sometimes co-developers of military technology and systems. These situations rely on thorough IP strategies and agreements to assure both parties interests are achieved, and each receives the just value for their investment. This will likely include a combination of the standard rights and specially negotiated licenses (SNLs). To facilitate an equitable share of IP rights in this collaborative environment, it is critical that all parties have a good understanding of acquisition laws and policies as well as fundamental implications of IP rights and protections.

Government funding of non-FAR development is not recognized as Government funding for purposes of the funding test in the DFARS. Only direct charges for efforts under FAR contracts are necessarily treated as Government funding for the data rights funding test. It is possible that non-FAR grants, agreements, or other vehicles with Government funding may lead to subsequent FAR contract acquisition of that technology making it critically important that IP agreements in OTAs and other non-FAR vehicles cover Government data rights.

Separately, in FAR contracts, indirectly reimbursed costs, such as Independent Research & Development (IR&D) costs, do not count as Government funding under the funding test.[36] Legal counsel should be consulted about non-FAR-to-FAR transitions and the handling and ramifications of indirect costs and IR&D for data rights purposes.

Non-FAR agreements do not automatically grant data rights under the funding rule. Rights need to be specifically stated in the agreement.

government employee-inventors, whether civilian or military may be entitled to a cash award or even a share of any royalties from licensing. *See* DEPT. OF DEF. INSTR.5535.08, DOD DOMESTIC TECHNOLOGY TRANSFER PROGRAM, para. 3.3.d [hereinafter DoDI 5535.08] for additional information.

[36] *See e.g.*, ATK Thiokol, Inc. v. U.S., 598 F.3d 1329 (Fed. Cir. 2010), https://casetext.com/case/atk-thiokol-v-us.

2.7.2 Pairing standard rights and funding source for noncommercial.

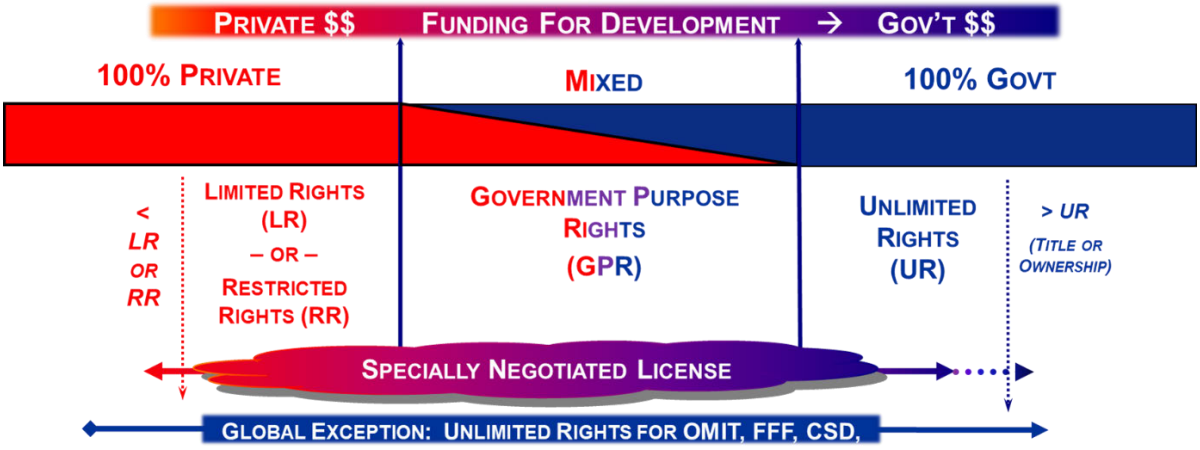
Figure 6 below depicts Government license rights under the DFARS for noncommercial TD and CS as a spectrum from fully private funding on the left to fully Government funding on the right. Note: The funding test does not apply to commercial items.)

The graphic illustrates the three funding scenarios just covered paired with the associated standard data rights: Limited/Restricted Rights with private funding; Government Purpose Rights with mixed funding; and Unlimited Rights with Government funding.

The SNL "cloud" in Figure 6 indicates that, regardless of funding, a unique license agreement can be entered between the two parties and can provide a range of rights based on tailored requirements.

Below that, the blue "Exception" box spanning from left to right indicates that, regardless of funding, the Government's has standard unlimited license rights in TD necessary for OMIT (other than DMPD) and FFF TD.

Figure 6. Mapping Noncommercial Data Rights and Development Funding



2.8. THE DOCTRINES OF SEGREGABILITY AND MODULAR LICENSING

2.8.1 Doctrines of Segregability: As discussed in the mixed funding scenario of joint development (subsection 2.7.1, paragraph 3), there is likely to be a combination of rights across a system to account for the co-development of a system by Government and industry. The funding test doctrine of segregability for rights refers to the situation in which different physical parts of a system or sections of software have different data rights based on the noncommercial funding test. Generally, the assessment of the funding source should be at the lowest practicable segregable level of the system architecture.[37] This feature has been coined "the doctrine of segregability," and more recently and informally as the "doctrine of modularity," or "modular licensing."

[37] *See e.g.*, DFARS 227.7103-4(b) (2025); DFARS 227.7203-4(b) (2025).

In practice, this may result in discrete subsystems or components of a larger system being categorized as developed exclusively at private expense and therefore subject to the most significant license restrictions from the Government's perspective (e. g., Limited Rights in noncommercial TD, or Restricted Rights in noncommercial CS[38]). Since these narrower or restrictive categories of license rights generally do not allow release of the data or software for competition, this practice can result in the Government having incomplete data, CS, and rights for a system or subsystem — sometimes referred to as "Swiss cheese" data rights.

Figure 7. Swiss Cheese Data Rights

In such a case, DoD would be unable to release the complete, detailed TD package with data rights covering the entire system for a competitive solicitation due to the restrictions on the data covering the proprietary subsystems or components. This circumstance can limit competition on large systems funded substantially by the Government. Often, this license schema compels the Government to rely on the discrete subsystem OEM for parts, new units, or maintenance or repair on the entire system.

A related type of DFARS segregability is known as clause segregability and applies only to TD. Per DFARS 227.7103-6(a), for commercial items (other than software), if the Government paid for any portion of the development of a commercial item, the clause at DFARS 252.227-7013 will govern the TD pertaining to any portion of the commercial item that was developed in any part at Government expense. DFARS 252.227-7015 will govern the TD pertaining to any portion of a commercial item that was developed exclusively at private expense. This means that the funding-based rights can sometimes apply to portions of a commercial item (other than software).

2.8.2 Mitigation - Modular Licensing: To mitigate IP-based restrictions on competition in these scenarios, DoD can utilize MOSA and SNLs. MOSA combines system engineering open architecture techniques with open licensing and related legal and business considerations to isolate proprietary technology and prevent overleveraging of limited private investments and undermining of return on Government investment. By mitigating the impact of these "Swiss cheese" holes, the Government can effectively manage the whole "cheese".

MOSA enables the Government to limit the impact of restrictions on privately developed components by treating those components and technology as proprietary "black boxes" that are described with releasable FFF data and well-defined and described functionalities, interfaces, and MSIs to the remainder of the system components. This allows other vendors to identify suitable alternatives for the proprietary black boxes, or, if necessary, to contract with the OEM

[38] *See e.g.,* 7013, *supra* note 8, at (a); 7014, *supra* note 9, at (a).

for support for those black boxes, but to limit such sole-source efforts to the black box itself. If the Government needs to ensure capability to repair or replace components in such a black box, MOSA does not necessarily solve that problem, but it offers a useful tool in addressing IP licensing challenges.

2.9. MISCONCEPTIONS ABOUT IP AND DATA RIGHTS

1) It's too early in the program life cycle, so the program can't plan for IP now: FALSE!

- EARLY and continuous analysis using historical data from similar systems identifies logistic, maintenance, and operational concepts; the need for enabling organic/in-house (Gov't personnel/facilities) sustainment (depot) capability, and training which informs EARLY data needs required to develop PS input to the IPS, prior to RFP, re-procurement, or similar activity. There are various risk mitigation strategies that may be incorporated into a program's IPS (see Figure 9 Examples of Program Uncertainty and IP Mitigation Strategies).

2) The program can't get delivery of DMPD data: FALSE!

- There is no preclusion or restriction on Government requiring delivery of DMPD data.
- The Government may receive DMPD data with lesser rights than Unlimited Rights. When ordering DMPD data, request delivery in a contract data requirements list (CDRL) and consider developing a SNL tailored to the specific use case.

3) If the program paid for the development of the item, then it can automatically get the data later, when it needs it, and it will have all the rights to use the data: FALSE!

- There is no relationship between source of funding and ability to require delivery after contract award. Having rights to data, but not asking for delivery of the data does not meet the need. Both are required and they are separate contractual agreements.
- The Government must secure rights in data, during solicitation and ideally during competition, by requiring delivery of data by including terms in the contract, documented in a CDRL and appropriate data item description (DID) that require the contractor to provide specific TD and software items that satisfy the Government's needs.
- Unless the program required delivery of the data in a CDRL, the Government may not be able to use the data when they need it even if the Government is entitled certain rights.

SECTION 3: THE 5W'S OF THE IPS

This section will cover the foundations of the IPS: what it is, why it's critical, where to find direction for the IPS, when to consider it, who writes it, and key attributes.

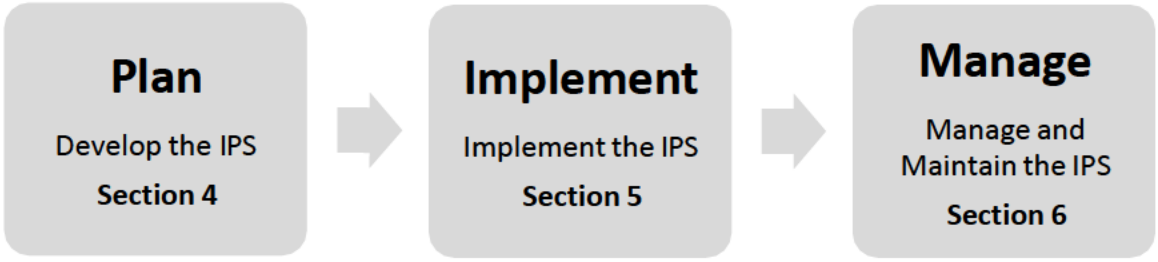
3.1. WHAT IS THE IPS?

DoDI 5010.44 states "each DoD program will have a robust IPS" and provides IP implementation guidance for "the full spectrum of IP and related matters (e.g., TD and CS deliverables, patented technologies, and license rights)."[39] DFARS 207.106 discusses assessing IP needs of the system and establishing an AS that provides for the TD and CS deliverables with associated license rights needed to sustain the systems over their life cycle.[40] Importantly, among other requirements, both the assessment and IPS must be developed "before issuance of a solicitation for the weapon system or subsystem."[41]

The (IPS, which is embedded in the AS and reflected in the IP Management Plan for PS in the life cycle sustainment plan (LCSP), is the strategic plan to meet data requirements for the whole program and for the life of the program. The IPS is the result of strategic planning and critical analyses of data requirements derived from sources like the capability development document (CDD), AS, systems engineering plan (SEP), PSS, program protection plan (PPP), test evaluation management plan (TEMP), and business financial plan. It provides a strategic framework or architecture that maps use cases for data to execute plans and deliverables that address risks, issues, and opportunities for how to satisfy those requirements.

3.1.1 Three Phases of the IPS.

Figure 8. Three Phases of an IPS



The IPS is a living document and follows the basic phases of any strategy:

1) Plan and formulate the strategy: The first phase is the formulation or development of the IPS itself.
2) Implement the strategy: Contracts or other formal agreements are the mechanism in which the Government implements strategies so, this phase is focused on the contracting process from pre-solicitation to RFP and CDRL planning to negotiations.

[39] DoDI 5010.44, *supra* note 2, at sec. 4.1.
[40] DFARS 207.106 Paragraph (S70)(1)(i)-(ii) (2025).
[41] *Id.* at (S-70)(2)(i).

3) Control, evaluate, and manage the strategy: This phase includes critical activities like deliverable reviews for markings and managing data rights. Additionally, managing the IPS includes updating it as assumptions and risks are realized, the program objectives change, or other major decisions are made.

The IPS should not be viewed as a one-time compliance check.

3.2. WHY IP IS CRITICAL TO THE PROGRAM?

"I have always found that plans are useless, but planning is indispensable."

- Dwight D. Eisenhower

3.2.1 Critical to Program Execution: IP is of critical importance for national security, national prosperity, competition, and innovation at the strategic level. But IP is most critical for successfully executing the program with effective, affordable, and agile solutions for the warfighter's required capability. The analysis and critical thinking that drives the IPS is a mechanism to break down the complex derived requirements that the program depends on. The IPS documents these findings so that the program can have a consistent understanding of the requirements and approach throughout the life cycle.

A few examples of data, CS, and rights necessary to execute program requirements are:

- TD to support maintenance and repairs by deployed warfighters, or activities at DoD depots, sustainment centers, and shipyards in accordance with 10 U.S.C. § 2464[42].
- TD for airworthiness certification of repaired equipment.
- Software source code and other software components required for operability may be necessary to ensure cybersecurity depending on the method of vulnerability testing.
- Test results or performance envelope data may be needed for aircraft accident investigations.
- Other types of data may be necessary for Government contract management activities (e.g., Earned Value Management needed to report to various Government offices beyond the original program.)

Failure to plan for and secure necessary data and IP rights can hinder DoD's ability to execute its critical missions and increase operating costs in the near and long-term.

3.2.2 The IPS is Risk Mitigation for Program Uncertainty: One of the most important reasons to think through a robust IPS early is that it reduces risk to the program. Acquisition of

[42] § 2464, *supra* note 16.

warfighter capabilities and planning for weapon systems with potential life cycles exceeding 30 years inherently carries uncertainty and risk. Many programs highlight the uncertainty of data requirements (final technical design, sustainment strategy, etc.) as a reason NOT to consider IP acquisition early in the program during competition.

This uncertainty has led programs down two common but opposite approaches: **buy everything or buy nothing**. Both paths have pitfalls that can limit flexibility and options for agile decision making throughout the life of the program. However, the uncertainty is the reason why it is so important to do detailed analysis, tailor the strategy, and buy the right data early.

Much uncertainty in data requirements can be reduced through detailed independent PS Analyses (e.g., level of repair analyses, PS business case analyses using historical analogous system data, data from market research and intelligence, and data from industry days). These types of analyses help identify critical components and modules that will be candidates for sustainment activities like depot level repair, additive manufacturing, re-procurement, MOSA and then to plan for data deliverables and license rights that provide flexibility to implement future updates or changes to program strategies and plans throughout the life cycle.

The objective of developing a complete and executable IP Strategy is to achieve a balanced approach, ensuring the acquired IP is neither excessive nor insufficient.

Figure 9 below highlights some examples of uncertainty programs may face, how they drive uncertainty in IPS development, the resulting IP implementation, and ways to mitigate those outcomes regarding data, CS, and rights. For example, program uncertainty in future operational requirements will create uncertainty in what specific data requirements to plan for. The IPS then may be built to either overreach and as for "everything" driving challenges with industry or may underestimate the need and create long-term vendor lock as well as mission impacts. To mitigate this scenario, a combination of tactics may be employed such as deferred ordering, priced options, and use of historical data for similar systems.

All these mitigation tactics are enabled by a robust IPS that considers and acknowledges uncertainty upfront and builds flexibility into the framework.

Figure 9. Examples of Program Uncertainty and IP Mitigation Strategies

3.3. WHERE IS IPS DIRECTION?

The requirement to prepare an IPS is codified in several statutes and regulations: namely, 10 U.S.C. §§ 4211[43] and 3774[44] as well as DoDI 5010.44[45] and accompanying Adaptive Acquisition Framework (AAF) Pathway policies. All programs should develop and prepare an IPS; this is especially true for any acquisition that will involve technology development, organic sustainment, planned competitive evolutionary or incremental upgrades, interoperability, or integration with other systems, or that will otherwise call for acquisition of IP or IP rights.

3.4. WHEN IS THE IPS PREPARED?

Developing an IPS is most impactful early and should be initiated as early as practicable and updated at appropriate milestones or whenever events or circumstances materially affect the associated assumptions, conditions, risks, issues, or opportunities.

As with all planning, the greatest freedom of maneuver or trade space exists at the beginning of the planning process. This is especially true in acquisition when opportunities for competition are at their peak. Additionally, the nature of contractual agreements understandably makes it harder to change once an agreement is signed; so, it is best to be clear about requirements, value, and expectations for future needs as early as possible to build in flexibility.

Two common factors have encouraged the delay of meaningful discussion of data rights issues until after contract award:

1) The first is the reality of program acquisition priorities focused on short term cost, performance and, most critically, schedule rather than long-term impacts. However, this short-term or near-sighted approach often leads to higher costs, inferior performance, and

[43] 10 U.S.C. § 4211 (2025).
[44] 10 U.S.C. § 3774 (2025) [hereinafter § 3774].
[45] DoDI 5010.44, *supra* note 2.

significant schedule delays down the line when alternative solutions become necessary. Planning early should enable the program to build in cost into the initial budget estimates and ensure the data necessary for performance is negotiated prior to contract award.

2) The second is that DFARS data rights procedures[46] allow merely documenting IP owner assertions of restrictions on use of data in the contract at award and postponing Government scrutiny of asserted restrictions until after contract award. However, postponing decisions on IP often does not have favorable outcomes for the Government due to reduced trade-space and negotiating power post-award. Addressing IP concerns and assertions of data restrictions post-award often takes an extended period to resolve. Unfortunately, during the period for dispute resolution, the Government must abide by the asserted restrictions even if the restrictions are ultimately determined to be unjustified.

The IPS is required for all major program decision points in accordance with the specific AAF Pathway guidance and should be updated throughout the program life cycle anytime a major change (like a solicitation or engineering change proposals) occurs. Additionally, similarly to other program strategies, there may be an accompanying plan that implements the strategy. For example, while the formal AS signed by the Milestone Decision Authority (MDA) may not be updated often, the program management plan, risk management plan, contract plan etc. are often revisited and updated to reflect status of the program and important changes like budget. IP should be viewed in a similar way because the specific implementation of the high-level strategy will require more granular detail, and new information may cause a change to the data rights framework.

3.5. WHO IS RESPONSIBLE FOR THE IPS?

The program manager (PM) is ultimately responsible for the AS and developing a plan to meet the program requirements, but IP must be a team effort. The development and continuous updating of an effective and robust IPS will require active participation of subject matter experts from a wide variety of disciplines, including engineering, logistics, contracting, cost, accounting, and legal.

To strategically plan for all data needed on the program, the support of a robust and knowledgeable cross-functional Integrated Product Team (IPT) is necessary. In support of writing the AS, the PM should establish a cross-functional IPT under the leadership of a data manager, or personnel serving in that role. The IPT should identify and evaluate data requirements and a framework of rights that will meet program life cycle objectives and draft the IPS. The IPT includes the PM, engineers, test managers, PS Managers (PSMs) and logisticians, contracting officers, data managers, IP subject matter experts (SMEs) or specialists, and acquisition and IP lawyers to fully cover the analysis necessary to determine the IP requirements. Each functional expert will contribute essential information to understand the data requirements, contracting tools, and legal limitations or opportunities available to collectively craft a plan that meets the program objectives and mitigates risk.

[46] *See e.g.*, DFARS 252.227.7017 (2025).

3.6. IPS ATTRIBUTES

A good IP Strategy reflects critical analysis that shows that the supporting set of planned tactics to achieve IP strategic goals are realistically achievable within budget and time constraints.

DoDI 5010.44 outlines what the IPS should minimally contain as part of the AS and LCSP.[47] The strategy should contain sufficient details to allow senior leadership and the MDA to assess whether the strategy makes good technical, business, financial, and legal sense, effectively implements laws and policies, and reflects the Department's acquisition, sustainment, and modernization priorities. It should describe the PM's plans for the acquisition, use, and protection of IP (e.g., TD and CS deliverables, patented technologies, and license rights), and identify and manage the full spectrum of IP and related matters (e.g., TD and CS deliverables, patented technologies, and license rights). Further guidance for what "sufficient detail" may look like is below.

Table 3. Attributes to Integrate in an IPS

Examples of Attributes/Measures to Integrate in an IPS	
⊕ Maps IP requirements to program objectives	⊕ Supported by IP market intelligence
⊕ Describes use cases for data requirements (5Ws): (the right data, with the right rights, at the right time)	⊕ Recognizes that IP owners can decline to sell data and data rights and contains strategies to encourage IP owners to meet war fighter needs
⊕ Tailors TD and software deliverables, and associated license rights necessary to equitably meet mission and program objectives (e.g., MOSA, reprocurement manufacturing, detailed depot repair.) and industry interests	⊕ Updated as necessary and appropriate as new material information emerges, such as IP owner data rights assertions or refusals to sell data
⊕ Describes how the strategy aligns with the applicable rules of the chosen contracting strategy (full and open competition, OTA, sole source, etc.)	⊕ Considers needs for all types of data including TD, CS, financial and administrative data
⊕ Estimates life cycle costs related to TD and license rights.	⊕ Addresses both short-term needs (such as for developmental or operational testing, airworthiness, or source qualification) and long-term needs (such as for maintenance, repair, and reprocurement)
⊕ Incorporates analysis of data, CS, and rights already possessed to determine gaps	⊕ Leverages source selection evaluation
⊕ Identifies risk mitigation strategies and flexible options. (e.g., priced options, deferred ordering, deferred delivery, data escrow agreements, access agreements, and SNL agreements)	⊕ Identifies risks related to data deliverables and rights

[47] An LCSP is required for all covered systems and is the principal document establishing the system's PS planning and sustainment, pursuant to 10 U.S.C. §4324, for "covered systems" defined in that statute. For covered systems, the LCSP must contain a comprehensive PSS; *see also* DoDI 5010.44, *supra* note 2.

Table 4. Attributes to Avoid in an IPS

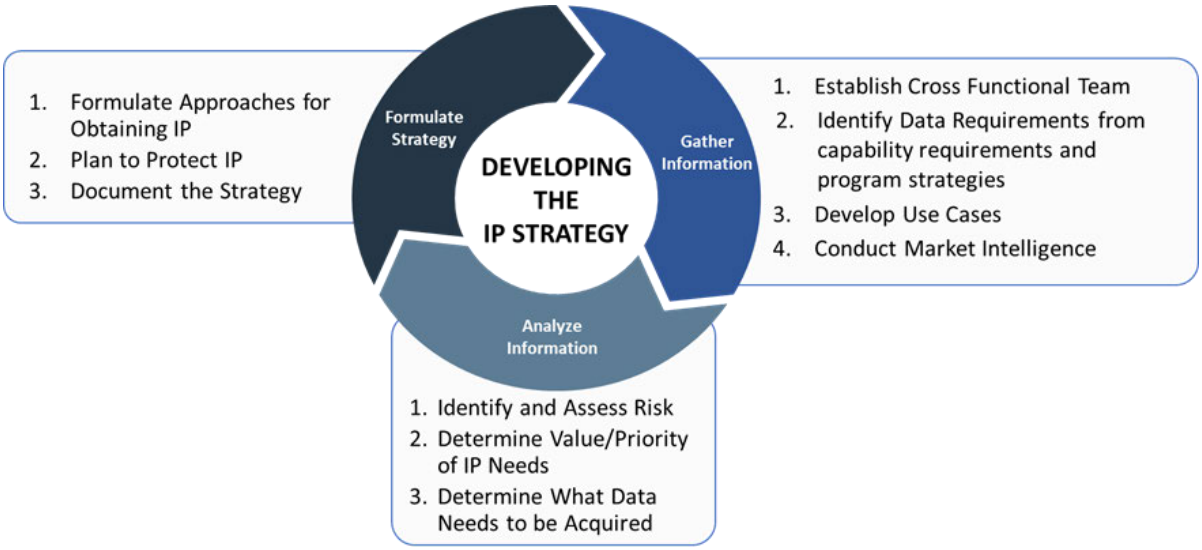
Examples of Attributes/Measures to Avoid in an IPS	
Ø States a requirement for unlimited or Government purpose rights "in everything"	Ø Assumes the IP owners will agree to sell all data, CS, and rights requested at an affordable price
Ø Copies from another program without tailoring to specific needs and circumstances; considering updated policy and guidance	Ø Assumes reverse engineering can be done using Limited Rights, manufacturing data, or other proprietary data
Ø Fails to assess and mitigate effects of "doctrine of segregability" as necessary	Ø Fails to plan for fulfillment of all data, CS, and rights needs for all types of data for the full program life cycle
Ø Does not identify use cases for non-standard data rights requested	Ø Does not map rights to deliverables
Ø **Simply stated, "the Program shall acquire all TD and software, and rights needed for the Program" without any further detail on implementation**	

WARNING: Referencing old IP strategies that pre-date DoDI 5010.44 and other current statutes and policies may not provide good examples of a tailored, balanced, and robust IP strategy.

SECTION 4: DEVELOPING THE IPS

As discussed in Section 3, the first phase of the IPS is to formulate the strategy itself. There are three major steps in formulating the IPS: gather information, analyze information, and formulate the strategy. There are many components to each of these steps that will be covered in this section.

Figure 10. Three Steps to Develop an IPS



4.1. GATHER INFORMATION.

4.1.1 Establish Cross-Functional IPT: To effectively acquire necessary IP and associated rights, the cross-functional IPT must consider all aspects of the program that require IP to be successful. This team includes the PM, engineers, test managers, PSMs and logisticians, contracting officers, data managers, and acquisition and IP lawyers to fully cover the analysis necessary to determine the IP requirements. The right team is essential to understanding the tools available and the constraints on the Government's ability to require what it desires in the way of IP rights. Identifying the right team is a deliberate step and should not be overlooked.

Figure 11. Objectives of the Data Management IPT

Objectives of the IPT	
1. What data and associated rights do we need to support development (when relevant), fielding, short- and long-term production, and operations and sustainment?	5. What risks, issues, and opportunities result from lack of or availability of data and associated rights?
2. What data and associated rights do we already have and what are the Government's rights/licenses for that data?	6. What is the best approach or combination of approaches for meeting the identified needs considering the associated risks, issues, and opportunities?
3. When do we need the data and associated rights to use it?	7. What will it cost over the life of the system, program, project, mission, or K?
4. Is the data best sourced from the public domain, a private party, or internally from the Government?	8. What measures. metrics, or other results will be integrated to guide implementation?

4.1.2 Identify Data Requirements: The objective of this step is to identify specific data, CS, and rights needed (e.g., TD, CS, contract administration data) to execute DoD capability requirements during all phases of a program: development, manufacturing, sustainment, demilitarization, and disposal. While some of this information may not be known with certainty, there are several methods to plan for and mitigate that uncertainty, especially independent PS analysis.

IP requirements are derived from the program's primary capability requirements documents (e.g., Initial Capabilities Document, CDD) and subsequent functional strategies (e.g., Single Acquisition Management Plan, SEP, TEMP, PSS, LCSP, PPP, etc.) to meet technical, functional, and operational requirements. These program strategies are enabled by and dependent on IP data in several ways. As such, the IPS should directly inform, support, enable, and implement these plans through robust and collaborative critical thinking as an IPT.

One way to break down the program's unique requirements for hardware and software as they support the various functional areas is to conduct a requirements analyses guided by the work breakdown structure (WBS) and subsequently conduct a LORA. These cross-cutting analyses help all functional areas understand cost, schedule, and performance risks, as well as potential issues and opportunities associated with the data needed to implement program plans. These analyses also inform the data needs mapped to use cases: the who, what, where, when, why, and how the data is needed.

Identifying requirements by subject matter helps determine where the IPT can find the derived IP requirements and what they might be.

4.1.3 IP Requirements to Support Engineering and Technical Objectives and Activities.

Figure 12. Examples of Engineering/TD Requirements

- Hardware and software design data
- Developmental or operational test data
- Qualification or certification data
- Software defect reports and various technical progress reports
- Briefings

Engineering tasks inherently require data: test data, finite element analysis results, drawings, performance measurements, etc. As such, it is important to ensure that this data is captured in the data requirements. These requirements can then be integrated into a robust IPS to acquire and maintain engineering data throughout the program. The key documents that guide the identification of engineering and TD requirements are the CDD, SEP, TEMP, PPP, and WBS. Examples of considerations for engineering data include:

- Development data, including any data about a proprietary system used to develop the system, that could be used over program life cycle for sustainment and procurement.

- Data required to obtain and maintain airworthiness certification is critical to qualifying aircraft to be flown and to ensure the safety of aircrews and noncombatants.
- Data to support nuclear surety is critical to ensuring the safety of warfighters and noncombatants.
- Unique uses for test data to support other program activities, future competitive upgrades or improvements, sustainment assessments, interoperability with other systems, and sharing engineering data between programs.

IP planning should be part of initial system engineering design considerations because the ability (or probability) of getting the necessary IP and associated rights may drive specific engineering solutions like commercial versus non-commercial solutions or MOSA. The IPS should be customized based on the common, shared, and unique characteristics of the system to include architecture and interfaces, PSS, core logistics analyses, depot source of repair determination, and commercial availability of the item.

Implementing MOSA requires a thorough IPS that ensures MSIs are identified and what rights are needed to create an open architecture and black boxes. In turn, anticipated IP challenges to be mitigated help to inform where modularity and black boxes are desirable. The program's plan for MOSA should be documented in both the AS (including the embedded IPS) and in more detail in the SEP. Identifying MSIs and the appropriate data, CS, and rights to enable that strategy throughout the program is an example of how closely functional plans and strategies are tied to the program IPS implementation. (See Appendix A References for a link to the MOSA Guidebook)

If a program is implementing digital engineering as part of its systems engineering approach, careful consideration needs to be given to acquiring the necessary technical baseline documentation accompanied by the appropriate IP rights. Otherwise, the program will fail to reap all the benefits of digital engineering. Additional guidance and a comprehensive list of digital engineering data considerations can be found in the Digital Engineering policy DoDI 5000.97. Examples of considerations for digital engineering data include:

- Digital models, simulations, threads, artifacts, and all associated data to support model-based systems engineering.
- Digital models, simulations, threads, artifacts, and all associated data to support mission engineering analysis.
- Digital models, simulations, threads, artifacts, and all associated data to support certifications, other program activities, future competitive upgrades or improvements, sustainment assessments, interoperability with other systems, and sharing all engineering data between programs.

4.1.4 IP Requirements to Support Acquisition/Business Objectives and Strategies.

Figure 13. Examples of Acquisition/Business Data Requirements

- Integrated Master Schedule
- Earned Value Management Data
- Vendor Risk and Mitigation Data
- Data Enabling Competition Objectives
- IP Valuation Data
- Market Factors
- Contract Administration Data

The acquisition and business requirements for IP may be less obvious than the engineering/technical ones. A good place to start is the draft AS that identifies key plans, activities, and objectives that rely on data. The contract strategy is also a significant consideration for the IPS because a certain contract strategy may implicate which IP regulations, if any, are applicable (i.e., FAR vs non-FAR). Some data required to support acquisitions may not be TD or CS so, even if using a FAR contract, may not be covered by the DFARS clauses for rights in TD and CS. Some considerations include:

- Competition objectives.
- Small business partners plans and strategies.
- Information sharing requirements (like financial reporting and analysis).
- Long term contract strategy.
- Industry's business objectives.
- The market economy for the program's tech space.
- Commercial best practices.

Some of these considerations drive IP requirements and, conversely, others may be decisions driven by IP requirements from other functional areas. This is why it is so critical to conduct this cross-functional analysis of requirements early in the program before major decisions are made. For example, if the AS is to have periodic competition for planned upgrades throughout the life cycle, the Government needs to ensure the IP requirements contain IP data, CS, and rights to support that acquisition objective. On the other hand, if the IP requirements highlight a need for other than standard rights, the acquisition and contracting approach needs to plan for that.

As always, cost and budget are critical factors to planning that may influence or be influenced by IP requirements. If there is not sufficient budget at the current phase to order all necessary data required, mechanisms such as deferred delivery and priced options (see Section 5.3) can be utilized to ensure that the Government negotiates and plans for the right IP even if it cannot be acquired in the initial contract award. IP requirements that are identified early in the program,

should be included in the Life Cycle Cost Estimate and subsequently in the Program Objective Memorandum (POM)/Budget.

Additionally, as mentioned in the ROI discussion in Section 2, it is very important to consider who the potential contracting partner is and how their business model and objectives impact their position on IP for the program, as this could greatly influence the acquisition and PSS.

Finally, another aspect of the acquisition that will greatly affect the IPS is if the program is joint, multi-national, or part of the Foreign Military Sales or Excess Defense Articles programs. IP rights that only directly cover Government needs may not be sufficient to address the needs of security cooperation partners such as desire for their own organic sustainment capability or joint military operations. If there is any contemplation of international security cooperation in connection with a weapon system, it is a best practice to consult with and include representatives of those interests in the cross-functional IPT for IP planning.

4.1.5 IP Requirements to Support Life cycle PS.

Figure 14. Examples of PS Data Requirements

- **Technical Manuals**
- **Provisioning**
- **Depot Maintenance**
- **Software User Manuals**
- **Training Manuals**
- **PS Analysis (PSA)**

The PSS is the strategy to deliver affordable and effective PS across the life cycle. Decisions made early in the life cycle have significant impact on life cycle costs and help formulate initial system cost positions. PS Managers (PSMs) and Logisticians must complete a detailed analysis of the sustainment Key Performance Parameters and Key System Attribute in the CDD (availability, maintainability, etc.) and account for the overarching AS and PSS.

These analyses will include PSA, such as FMECA, LORA, and Business Case Analysis (BCA). The results of the initial LORA and PS BCA determine tailored data needs and necessary rights to begin to incrementally develop the PS package over the design, development, test, production, and fielding phases to meet user demonstration and test events required to deliver a validated and verified PS package. The PSM is crucial in the development and delivery process, as the PM's advocate to the Integrated PS Element for cost input into the planning, programming, budgeting, execution, and POM process to ensure funds are available to execute future PS activities.

Delivery of depot repair package data (e.g., depot repair manuals, support equipment and tools) can be delayed for a reasonable period until those data deliverables are required (mid-way into initial operational capability plus four years). The data rights must be established at contract inception, but those deliverables may not be required until sometime later to establish initial depot capability and capacity. This combination of information will frame the holistic approach to IP needs for life cycle PS planning by identifying required TD and levels of rights and tailoring PS inputs for the IPS.

The PSM should coordinate with the cross functional IPT early on any needs they might have in sustainment that haven't been considered and/or verify that their needs are captured in the IPS

(e.g., TD package and CS deliverables, method of delivery, and associated license rights, etc.). **For detailed guidance on IP Planning for PS see Appendix B for access to the IP for PS Toolkit.**

4.1.6 Connect Data Requirements to Delivery Requirements by Determining Use Cases:

Once the IPT has developed data requirements based on the core functional considerations, and pursuant to 10 U.S.C. § 4324, the PS BCA, the functional Subject Matter Experts (SMEs) on the IPT need to validate and verify data needs are tailored using Figure 2-2 of the LCSP Outline, Version 3.0, hosted on DAU.[48] This table is a best practice tool to assist the PSM IPT in tailoring data needs to uses at the WBS level, based on data analysis and stakeholder guided critical thinking. This process is not limited to the PSM IPT and can be used by other functional IPTs for documents such as the SEP, TEMP, and PPP, to guide the team in understanding "how to" articulate data needs and licenses necessary to implement program plans.

Use case pairs connect program data needs with one or more use cases, or how the data will be used at that time, to determine when the data is needed and what rights the Government needs. The connection of data with uses provides the IPT a guide for when to ask for data, what type of data to ask for, and how to structure the contract specifically for the types of license arrangements and other arrangements that will satisfy the use cases, prior to developing an RFP. For example, original equipment manufacturer (OEM) design data and SNLs may be necessary for qualification of additive manufacturing parts and to implement maintenance in contested environments. The data and licenses need to be tailored to where, who, and how the data will be used. This structure should also clearly define the content and formatting requirements for each corresponding deliverable via CDRLs and DIDs.

Use case analysis ensures the PM and all stakeholder equities (e.g., data needs, uses, risks, opportunities, delivery timing aligned with program test and developmental or operational demonstration events) have been considered and incorporated into actionable deliverables through contracting methodologies and CDRLs, source selection and evaluation factors and criteria, that incentivize desired outcomes.

A use case tailored to IP requirements provides a practical description of all needs for data and IP rights by identifying particular TD, software, or other data along with the intended purpose, effect, and condition of use.

[48] U.S. DEP'T OF DEF., LIFE CYCLE SUSTAINMENT PLAN VERSION 3.0, FIG. 2-2 at 17 (13 Oct. 2022).

Figure 15. IP Use Case Development: FILL-IN-THE-BLANK

IP FILL-IN-THE-BLANK
Mapping IP To Use Case

To map IP to use case(s) an IP requirement should take a form substantially like:

"**Data**_____[*e.g., TD, software, or other*] **necessary for** _____ [task] (*or other data description*) **and rights for** _____[who] (*e.g., Government employees, IP owners, contractors, consultants, foreign allies, the general public, etc.*) [location] (*e.g., a particular deport, in theater, the IP owner or contractor's facility, anywhere, etc.*) **to perform**_____[a task] (*e.g., maintain an engine, repair fuselage damage, diagnose a system failure, train warfighters to operate a rangefinder, identify a sonar target, etc.*) **on/under** _____**[condition]** (*e.g., obsolescence, supply shortage, exercise of an option, expiration of a more restrictive license, etc.*) **in the** _____[timeframe] (*e.g., immediately upon delivery and perpetually, ten years after contract award and thereafter*)."

Another simple way to frame use cases is to answer the 5W's plus how for each data requirement (Fig. 21). The answers to these questions create a problem statement clearly defining the task deliverable and informing the necessary rights. These statements can be used in the RFP to clearly communicate to industry what the tailored requirement is. An example is: Engine TD is needed to conduct scheduled maintenance by active-duty maintainers in CONUS and OCONUS locations every 250 flight hours for the life of the system. Additional examples of IP use cases will be published as a job aid.

Figure 16. IP Use Case Development: 5 W's

What data is needed? (technical data, computer software, etc.)

Why is the data needed? (what task relies on the data (repair engine, replace a circuit card, perform maintenance on a motor)

Who needs to use the data? (the entire government, the government depot, third party integrator, support contractors, etc.)

Where will the data reside and be used (physical location, vendor IDE, etc.)

When will the data be used? (contingency, daily, 20 years in the future, etc.)

How will the data be used? (Are there other intended uses beyond the core task? additive manufacturing, competition, reprocurement, etc.)

The Work Breakdown Structure may also provide a useful framework for identifying potential use cases and data but may not lead to inclusion of all IP needs for the life cycle of a system including, for example, operational and contract administrative purposes, upgrades or technology refreshes, environmental disposal, and demilitarization.

While several approaches for identifying use cases have been presented, no single approach directly addresses all IP needs or circumstances. So, care and attention should be paid to determining the best approach for a given system and acquisition effort. In many instances, multiple approaches can and should be used in the same system and acquisition effort to generate use cases and corresponding data requirements.

4.1.7 Benefits Of Use Cases:

Use case pair analysis enables precise characterization of the Government's IP needs by stating the needs as use-based performance objectives from which Government rights to the data may be negotiated.

Use case pairs provide a useful method of drafting SNLs, which are statutorily preferred[49] and should be negotiated whenever doing so will more effectively balance DoD and industry interests than the standard or customary license rights.[50] Identifying use cases promotes tailored IP requirements which naturally should correct the common approach of making broad requests for Unlimited Rights or Government Purpose Rights in all data, which are more likely to meet industry resistance.

Use case pairs may inform the development of IP-related evaluation factors. For example, use case pairs may be used in a Value Adjusted Total Evaluated Price (VATEP) source selection evaluation methodology, which is described (along with other IP-related evaluation methodologies) in Section V. Thus, the use case pair approach helps source selection and special license negotiations to complement each other. Use case pairs allow for better prioritization and understanding of the timing of when IP is needed, resulting in a more effective and executable IPS.

Understanding schedule requirements associated with data requirements help to establish delivery requirements, inform negotiation parameters, and prioritize data requirements and negotiation objectives. IPTs can analyze the data, CS, and rights appropriate for use of deferred delivery and/or priced options at the initial contract when competition is in play. Programs should consider not requiring early delivery of data with broader license rights when data may be delivered later (and broader license rights may "spring" or be conditioned upon a particular date or the occurrence of an event). An important example of timing in use cases is software because it is in a continual cycle of development, testing, and continuous operation through disposal. In this case, programs should document in their IPS the 5W's plus how the Government needs to use TD and software in such continuous efforts and consider that timing rhythm in determining data, CS, and rights use case pairs.

Use case pairs are a very effective approach to interest-based negotiations that maximizes value to both parties. For example, data, CS, and rights necessary for organic maintenance and repair of certain portions of a system may not be required until a later point in the life cycle (e.g., when a system goes into sustainment and transitions from contractor logistics support (CLS) to organic support) allowing the IPS to consider different options to achieve delivery, like priced options,

[49] *See* § 3774, *supra* note 44, at (c).
[50] DoDI 5010.44, *supra* note 2, at Sec. 1.2(b)(3).

rather than delaying delivery because the data isn't needed now. (See subsection 4.3.1 on Select methods for obtaining IP and data).

4.1.8 Conduct Market Intelligence.

The last step in Gathering Information for the IPS is to conduct market intelligence specific to the relevant market. With the knowledge of the program's technology or information needs, the IPT should gather additional supporting information about the market's offerings and investment related to these needs. In this context, the marketplace includes private industry, intra-department acquisition efforts, and inter-Government acquisition efforts. This market intelligence will inform risk assessments, assumptions, and cost estimates that will be critical in the next steps to analyze the information and formulate the strategy. A primary objective is to determine whether there will be any obstacles to securing the required TD, CS, or associated license rights based on prior private investments in the marketplace. Market information will help the program understand potential budget constraints and anticipate industry IP positions in proposals.

This information can be gathered through activities such as open-source market research, industry days, science and technology (S&T) assessments, and competitive prototype developments. Even if the procurement is known to be a sole source acquisition, there is still value in conducting broad market research regarding the IP requirements for comparable IP data to help inform the strategy and subsequent negotiations. The IPS should summarize how the Program Management Office communicated with industry regarding Program Strategies related to data and data rights.

At the early stages of a program, the market intelligence will look generally at the economic market and approach to IP in the targeted technology space. Some critical sources of information include how many potential vendors there are, how competitive the marketplace is, common industry practices regarding certain types of data, historical agreements, past performance of potential vendors regarding IP approaches, business strategies of potential vendors, the value of IP to the potential vendors (early tech development, commercial revenue, estimated cost for various data and license rights which may vary by vendor, etc. With this information the IPT can inform the IPS based on anticipated vendor's approaches to data and license rights. Additionally, the market intelligence should evaluate the scope of privately developed technology (including development performed using Independent Research and Development funding) to better understand the Government's anticipated license rights.

Understanding industry's perspective on their own IP's value should be considered as part of the market intelligence effort. IP valuation plays a major role in the mergers and acquisitions of businesses, in IP litigation, in commercial IP licensing transactions, and, often behind the scenes, in defense acquisitions. Industry values IP using three primary methods:

- Cost – the cost of developing or building the IP asset, which could also be viewed as the cost of replacing the asset.
- Market Value – the market value of comparable assets.
- Income – the discounted present value of the expected income stream from the asset.

It is not clear that direct application of industry IP Valuation methods (cost, market, and income) will necessarily assist the Government team in determining the value of IP, but variations or hybrids of the above may be useful. These are not unique to IP, and can be applied to houses, cars, and other assets that are bought and sold. Each of these methods has strengths and weaknesses, and prerequisites for use.

4.2. ANALYZE INFORMATION

4.2.1 Identify and assess Risk, Issues, Opportunities.

Risk and Issues: Once the IPT has gathered the necessary information, the first step in analyzing it is to review it for risks and issues. The objective is to use the risk analysis to tailor the IPS to acquire only the data needed while protecting the Government's investment. There are two perspectives of risk to consider with IP:

- The probability or likelihood of needing a specific piece of data and the consequence of not having it. Put another way, how likely is the program to need the data?
- The probability of not receiving the requested data, CS, and rights (i.e., known needed data) and the consequence of not having that data.

Another way to look at risk in the context of IP is that IP can both be the risk **and** be a mitigation for other program risks:

- IP as the risk itself: for example, a program may need a particular type of maintenance data or it cannot maintain an associated component.
- IP as a risk mitigation strategy: a component has a high likelihood of failure, and the consequence of failure is inability to meet operational availability requirements. So, the risk mitigation strategy is to ensure the program has the data necessary to have multiple tiers of sustainment solutions.

Use cases provide a foundation for discussing probability and consequence in operational contexts. Subsequently, risk mitigation strategies can be put in place. If the use case indicates that there is a low probability of needing a specific piece of data for contingencies, but should that situation arise and there is a catastrophic result because the Government doesn't have the data, then the IPT should consider a strategy like a priced option or data escrow account (see Section 5.4.1) to ensure the program can get the data if needed, without requiring payment and delivery of up front.

Additionally, if the risk analysis determines there is a high likelihood industry may not provide the necessary rights to a critical piece of data, the IPT can plan for that early. In some instances, the IPT may adjust their IPS to re-evaluate the need, find another way to obtain the data, or use a back-up plan to meet the operational requirement. Conducting this risk analysis will help the IPT clearly and objectively understand where to focus specific tactics and techniques in the IPS as well as begin to prioritize requirements for investment.

Opportunities: An often-overlooked aspect of risk management is opportunity management. A question for the IPT is how the IPS can create or realize opportunities in the program. For

example, if the program has identified a future opportunity to potentially team with another service or integrate technology from another program, the IPT should evaluate how the right data strategy could help realize those opportunities. IP opportunities are not hard requirements for the system but rather potential positive paths for the program to utilize that are only enabled with the proper data rights. If the program does not consider those data rights and acquire them, the opportunity becomes an impossibility.

4.2.2 Determine value and evaluate priority of IP needs.

Value is not primarily about cost; it is about what an entity is willing to pay for something based on its priority/value to program objectives. For industry, their objective may be long-term revenue, so the value is based on how much income they can bring in by retaining data rights. For the Government, the program may have a cost objective for sustainment that is dependent on competing sustainment solutions, so the value of the IP should reflect sustainment cost avoidance. IP Valuation is an essential part of the program office's strategy because it helps shape the future negotiating position by clearly understanding tradeoffs/mitigations/plan which directly drives the best alternative to a negotiated agreement and what the program is willing to negotiate on.

As discussed in the Market Intelligence section, industry conducts detailed IP valuation that ultimately determines the price of their IP—or what they are willing to accept in exchange for their IP rights (recall Section 2 that describes IP acquisition as a basic transaction of goods). For the Government, IP Valuation is the reverse—it is what the Government is willing to pay for the IP in exchange for meeting mission requirements. To determine this valuation, there is an analysis of priority and affordability.

The value of IP to the Government may be measured in attributes such as sustainment cost avoidance, warfighter capability, agility, speed, flexibility, national security, and how the Government can approach risk/opportunity tradeoffs. Some of these attributes are not readily reducible to dollars and cents. These inherent differences in approach to the value of IP between Government and industry lead to several challenges when discussing, evaluating, and negotiating IP rights.

Fortunately, at this point in the IPS development, the IPT has a robust set of use cases that create a framework for IP Valuation. As one example of their benefit, by having the "when" clearly identified, rights available immediately versus rights exercisable can be analyzed as more or less valuable to the Government and the IP owner. At times, such valuations may be complementary and lend themselves to "win-win" scenarios. Early life cycle data rights for certain use case pairs may be of little value to the Government, but of great value to the IP owner.

To be smarter and more strategic, DoD officials must become more knowledgeable of how industry values IP so that they can come to the negotiating table with a respectful understanding of what IP means to their industry partner. Similarly, it is important to communicate to industry the importance (value) of IP data, CS, and rights to the success of the program strategy and for capabilities for the warfighter. There is no simple calculation to equate or compare these two sets of values, but one cannot ignore the other and still expect a balanced and fair agreement.

One way to encourage and enable mutually beneficial outcomes is to negotiate specialized provisions for IP deliverables and associated license rights whenever doing so will better address the parties' interests than the standard or customary license rights. To do this, officials must understand where the value exists in IP and its amount. A potential approach to merging IP valuation and evaluation in source selection is the VATEP method, described in Section 5.5.

4.2.3 Establish data to be acquired.

The final step in analyzing the information is to fuse the analysis and determine what the program needs to acquire. With the information of use cases, risks, and value, the IPT should be able to prioritize the data and data rights needed to execute the program successfully.

An essential part of this process is taking that prioritized list and determining where the data needs to come from: IP owner/vendor, other Government programs, previously acquired in the program, etc. Do not assume that all the data must be acquired from the vendor because the Government may already have data available. Should it be determined that the Government has already acquired data to support a system, the IPT needs to determine if the rights previously obtained are sufficient to meet the current and future needs of the program. This information can be found in the data assertions tables from previous contracts.

The IPT should research prior program contracts to determine if the DFARS Deferred Ordering Clause 252.227-7027 ordering period is still open to acquire required data and associated rights to determine whether this may be a preferable way to meet IP requirements in lieu of acquiring in a new contract. The IPT should also investigate whether the Government has any priced options for data or rights in data that could be legitimately and economically exercised to meet the contemplated requirements. In assessing these two alternatives—deferred ordering and exercise of options—the IPT should recall the adage "a bird in hand is worth two in the bush."

Whatever the investigation and assessment determine, the IPS should document the difference between the needed data, CS, and rights and existing data, CS, and rights already available to a program. If the assessment recommends actions to obtain needed data, CS, and rights under already existing contracts, the assessment should include realistic assessments of the likelihood of successfully securing the needed data, CS, and rights.

4.3. FORMULATE THE IPS

4.3.1 Select methods for obtaining IP and data.

With the robust analysis of IP requirements discussed above, the IPT is ready to select the methods for obtaining the right data, with the right rights, at the right time. There are many sources of IP to consider at the early stages of a program that include a range from organic development in a Government lab to reverse engineering to contracting with a commercial vendor.

The IPT should carefully consider mix of the possible sources (also assisted through earlier market intelligence) and consult with appropriate SMEs about how to leverage the range of sources to meet program needs. It is important to work with contracting and agreements officers

and IP counsel on how to build in flexibility so the program can adapt overtime and possibly introduce other tactics for certain IP requirements as supplementary. For example:

- teaming with a government lab for that technology will inherently give the program greater data rights than if they use a FAR contract to have an industry partner do the work.
- circumstances might suggest an opportunity to supplement a multi-phase FAR/DFARS effort with T2 or reverse engineering to satisfy certain IP requirements or to address emerging or urgent requirements.[51]

Not all acquisition efforts are established programs of record and are looking at broader technology capabilities. Or perhaps through the IPT's analysis, they may determine that a certain needed technology is not available through industry currently. In those case, IP can play a major role in determining how to pursue that technology. Table 7 explores these options, recognizing that effective solutions may leverage agreements beyond the FAR and encompass sources beyond traditional private-sector partnerships.

[51] *See e.g.*, DoDI 5535.08, *supra* note 35, at para. 3.3.d.

Table 7. Potential Sources or Tactics for Obtaining IP

Approaches	Advantages	Disadvantages
Completely organic development	▪ DoD has maximum IP rights ▪ May cost less	▪ Potential lack of expertise and capability ▪ May cost more
Repurpose of legacy technology	▪ May have shorter development time ▪ May cost less	▪ May not meet needs ▪ May cost more
Use of Reverse Engineering	▪ May cost less ▪ Avoids development time and effort ▪ May be combined with re-engineering for technology enhancement	▪ May cost more ▪ May require new certification and testing ▪ Alone, only replicates existing capability ▪ May require higher level approvals[52]
T2 Partnerships (e.g., Cooperative Research and Development Agreements[53])	▪ Allows tapping into Government and industry expertise ▪ More flexible IP rights allocations possible	▪ Activity scope may be constrained by rules (e.g., CRADAs require program to partner with a Federal Labs) ▪ Direct Govt funding may not be allowed ▪ Requires smart negotiation of IP rights because there are no standard or required clauses
Non-FAR vehicles (e.g., Public Private Partnerships. Cooperative Agreements, Other Transactions)	▪ May provide more flexibility for the allocation of IP rights ▪ May attract nontraditional industry participants	▪ Does not provide IP tools and framework of the FAR and DFARS ▪ May require familiarity with other rules such as the DODGARs or consortia OTAs
FAR/DFARS contracting without IP -related Evaluation Factors in Source Selection Evaluation Plan	▪ Most traditional and familiar approach ▪ Extensive framework and rules for adjudication of IP disputes ▪ Allows timely award of contracts without delay for IP dispute resolution	▪ Complex rules not thoroughly understood in DoD ▪ Usually has the effect of postponing resolution of IP disputes to when there is no competition. ▪ Prevents use of disputed data rights until final IP dispute resolution
FAR/DFARS contracting with IP-related Evaluation Factors in Source Selection Evaluation Plan	▪ May traverse some limitations of traditional IP contracting. ▪ May avoid IP dispute delays by awarding to "most advantageous"[54] bids and proposals. ▪ May avoid lengthy post-award delays in use of needed data for IP dispute resolution. ▪ Potentially recognizes pros and cons of all offers more fully and equitably by looking at IP and life cycle costs more holistically	▪ Requires understanding of complex rules as well as well as unfamiliar IP evaluation and valuation techniques and DFARS Source Selection Procedures ▪ Presently, for full compliance with all rules, may require a lot of data and analysis to implement rigorously and defensibly against protest. ▪ May dissuade industry participation or offers of best technology due to perception of lack of due advantage from purported private innovation and investment

[52] *See* DFARS PGI 217.7504(4) (2025).
[53] *See e.g.*, 15 U.S.C. §3710(a) (2025); DoDI 5535.08, *supra* note 35.
[54] *See e.g.*, 10 U.S.C. § 3302(b) (2025); 10 U.S.C. §3303(c) (2025).

4.3.2 Plan to protect IP.

One vital aspect of IP that must be planned for is how to protect the IP received throughout the program, as documented in the PPP. There are at least two negative outcomes to failing to properly plan.

- Failure to properly protect IP may negatively impact national security by disclosing technological secrets providing battlefield advantage for the United States. Such disclosures may share that advantage with adversaries or reveal vulnerabilities or countermeasures.
- Industry concerns that their IP might be handled incorrectly leading to a spill that could be detrimental to their business. The Government should always endeavor to meet its contractual obligations, and unnecessary legal liability is a financial drain on the Government and taxpayer and may divert funding from important national security priorities.

IP planning must include consideration of the level of sensitivity of Controlled Unclassified Information and the classification of any classified information and ensure that the systems and procedures contemplated for handling and processing IP and other sensitive information is appropriate for the information. One challenge in the protection of IP is special license terms. License terms should be drafted with the practicalities and logistics of Government compliance in mind.

Licenses can be overly complex with contradictory terms that similarly can lead to disputes and noncompliance. In advanced IP planning, especially when contemplating specially negotiated terms, attention should be paid to the impacts on intended users and IT systems of any contemplated special license terms. Conversely, the impact and limitations of human compliance and the operating logic and capabilities of existing or contemplated IT systems and the willingness of prospective offerors to trust those capabilities should be considered before building reliance on specific bespoke license terms into an IPS.

Sometimes these spills are not the result of poor license drafting, basic neglect, or even intent on the part of the Government. Government systems are frequent targets of adversarial attacks trying to steal our data. IP is often the target of cyber threats either for theft or for potential covert corruption.

- This could be the theft of proprietary design and testing data such as for stealth aircraft. Malicious activity to gain access to IP, designs, or technical information to weaken U.S. technological and military advantage.[55]
- Accordingly, all appropriate measures for protection of proprietary or sensitive critical TD and software including nondisclosure agreements (NDA) and procedures for handling of classified technical information should be strictly followed. This is also an aspect of supply chain risk management.

[55] U.S. DEP'T OF DEF., INSTR. 5000.83, TECHNOLOGY AND PROGRAM PROTECTION TO MAINTAIN TECHNOLOGICAL ADVANTAGE Sec. 3.2 (21 May 2021).

Programs should pay particular attention to identification and protection of technical information, the majority of which resides on unclassified systems. If stolen, this information provides adversaries with insight into U.S. defense and industrial capabilities and allow them to save time and expense in developing similar capabilities or countermeasures.

Therefore, protecting this information is critical to preserving the IP and competitive capabilities of the defense industrial base and the technological superiority of our fielded military systems.[56]

4.3.3 Document the IPS.

The information gathering, analyzing, and strategizing phases are complete. The next step is to capture everything in writing. Depending on the phase of the program, the IPS will either be included in the AS or reflected in the IP Management Plan for PS in the LCSP; it may also be a stand-alone document that is summarized in either the AS or PSS. This step is crucial, as the members of the IPT may not be on this program indefinitely, and it is important to memorialize all the work for future use on the program. A unique reference architecture for data, CS, and rights may be created for this program, serving as a map to meet the requirements. While the requirements may change, this research and analysis provide a solid foundation for future decisions.

Remember: an IPS is not a blanket statement stating that the program will acquire the data necessary. Rather the IPS describes what data is needed, why it's needed, who and how it will be used, when it's needed, and how to get it. Do not confuse the IPS with the contracting strategy that is the detailed implementation of the IPS. The contracting strategy (covered in Section 5) includes detailed CDRL identification, source selection evaluation approaches, drafting special license agreements, and more.

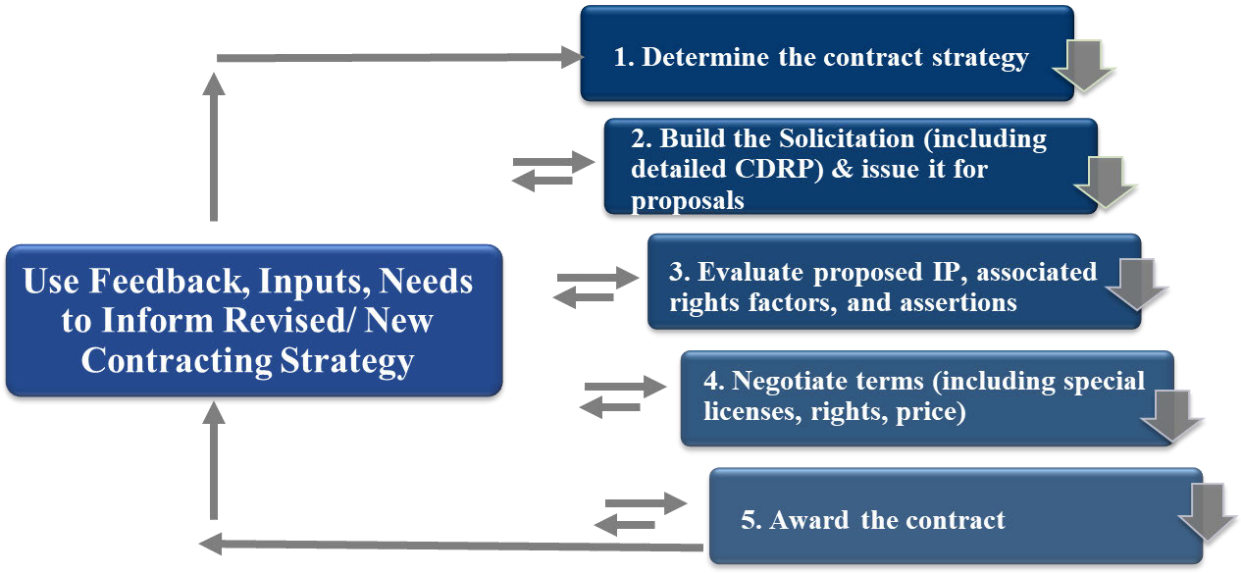
[56] *See* Off. of the Under Sec'y of Def for Res. and Eng'g., Dep't of Def. Technology and Program Protection Guidebook (July 2022).

SECTION 5: IMPLEMENT THE IPS

Armed with an IPS that supports and aligns to the other program acquisition documentation, the program will be ready to implement those strategies. Assuming that to meet the program data needs some data requirements will need to be satisfied by a contractor, the mechanism in Government acquisition to execute any transaction is a contractual agreement of some kind. These agreements may be FAR-based contracts or other non-FAR agreements, but in either scenario, they are the path to implement the program strategy. Contracting officers should work closely with data managers and program personnel to assure that data requirements are included in solicitations and consistent with the policy expressed in DFARS 227.7103-1 and 227.7203-1. Recalling the discussion of approaches for obtaining IP in Section 4.3, the guidance in this section goes more extensively into the approach of FAR contracting with use of IP as a source selection factor as it is a best practice when it is feasible; this becomes less feasible post milestone B in noncompetitive environments. The contracting process for acquiring IP in each contract generally involves five major steps:

5.1. Five Major Steps To Contracting For IP.

Figure 17. Five Major Steps to Contracting for IP



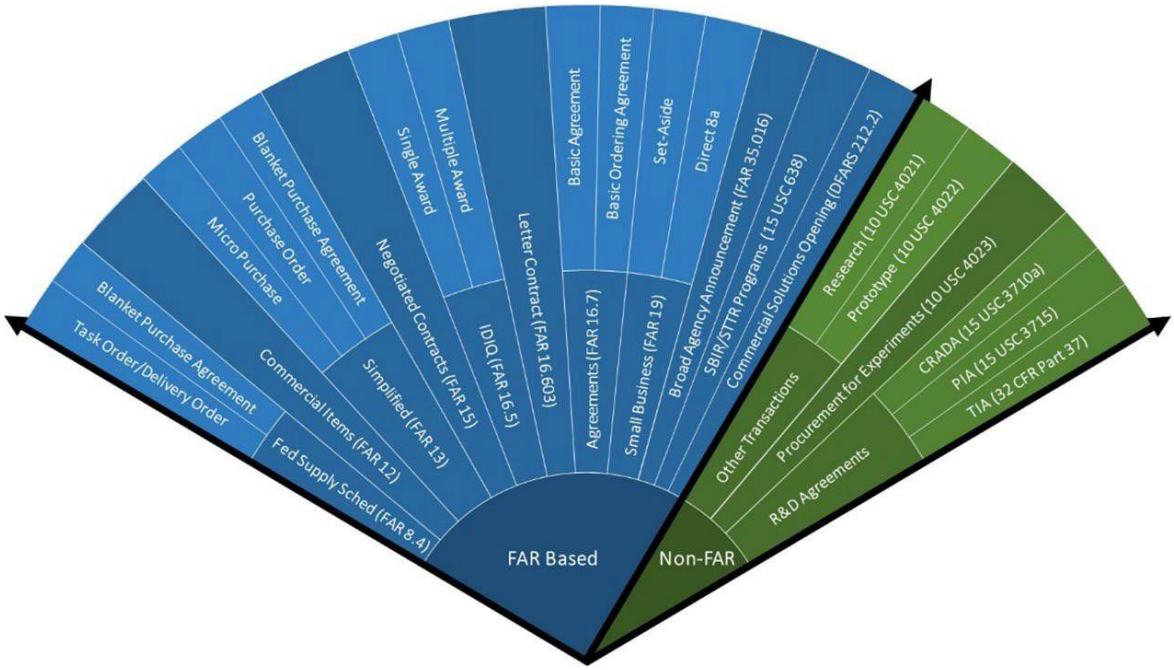
5.2. Determine Contract Strategy.

At a high level, there are two options for the contract strategy, FAR and non-FAR, which have significantly different approaches and regulations regarding IP. The familiar contracting cone, below in Figure 18, highlights that there are many options to consider within these two broad categories. It is critical that the team understands how to integrate IP considerations appropriately based on the chosen contracting strategy.

The DoD is accustomed to FAR contracts and the associated standard DFARS clauses used for them. As such, there is a strong temptation to apply those concepts to non-FAR

agreements which can create pitfalls and challenges. This section will briefly cover some of the important rules of engagement for each broad contract strategy.

Figure 18. Contracting Cone[57]



5.2.1 Federal Acquisition Regulation (FAR).

Recall that DoD cannot always effectively require an IP owner to sell the Government data or associated rights that it needs. There is a complex set of rules for the data rights the Government may or may not require. These act as rules of engagement for the conduct of IP acquisitions subject to the DFARS. The Government may state its negotiation objectives for data and data rights, but the rules of engagement constrain what may be treated as hard requirements, i.e., requirements for which a proposal could be deemed nonresponsive if not met.

These rules of engagement provide a framework for designing and executing both source selection evaluation of IP, and IP negotiations in sole-source awards. However, because of these rules of engagement, some DoD buyers and DoD contractors have mistakenly believed that evaluating IP in source selections was entirely prohibited. This is contrary to long-established policy within the DFARS as indicated in Table 8.

[57] DEF. ACQUISITION UNIV., CONTRACTING CONE (2025), https://aaf.dau.edu/aaf/contracting-cone/.

Table 8. DFARS IP Requirements Rules of Engagement

Type of Data	Prohibited Requirements	Expressly Permitted Evaluation	Source(s)
Noncommercial TD	▪ Requiring rights beyond standard rights as condition of award or responsiveness ▪ Prohibiting or discouraging items developed exclusively at private expense solely because of rights restrictions	▪ Evaluation factors that assess impact (including impacts on costs, short and long-term mission goals, and competition) created by restrictions on the USG's ability to use or disclose TD	▪ DFARS 227.7103-1 (c) and (d) ▪ DFARS 227.7103-10(a)(5)
Noncommercial CS	▪ Requiring rights beyond standard rights as condition of award or responsiveness ▪ Prohibiting or discouraging software developed exclusively at private expense solely because of rights restrictions	▪ Evaluation factors that assess impact (including impacts on costs, short and long-term mission goals, and competition) created by restrictions on the USG's ability to use or disclose CS	▪ DFARS 227.7203-1(c) and (d) ▪ DFARS 227.7203-10(a)(5)
Commercial TD	Requiring rights beyond standard rights and data beyond data customarily provided to the public, except as mutually agreed, except for: ▪ form, fit, function. ▪ data needed for repair, maintenance, installation, operating, or handling. ▪ data on USG funded modifications.		▪ DFARS 227.7102-1
Commercial CS and software documentation	▪ Requiring rights to software or related technical information, beyond customary commercial, except as mutually agreed, terms that conflict with federal law or except for agency needs	▪ When establishing contract requirements and negotiation objectives for commercial software and software documentation, consider technical and business factors identified in DFARS 227.7203-2(b) and (c)	▪ DFARS 227.7202-1(d)
Small Business Innovation Research/ Small Business Technology Transfer ***Data***	▪ Requiring more than SBIR/STTR data rights in SBIR/STTR data as condition of award or responsiveness	▪ Government may use information from offerors in response to SBIR/STTR solicitations to assess the impact of proposed restrictions on the use or disclosure of TD or CS in the source selection process, as per 227.7103-10(a)(5), 227.7203-10(a)(5), and other relevant acquisition guidance.	▪ DFARS 227.7104-1 ▪ SBIR/STTR Policy Directive 8. (b)(6)

5.2.2 "Requiring" Data, CS, and rights.

The FAR restrictions on "requiring" data, CS, and rights are commonly misunderstood within both industry and Government. Acquirers often talk about "requirements" in the sense of capability requirements and what is "needed." So, programs can indicate that certain data are "needed" for the program and include certain contractual data requirements and standard license rights in a solicitation. However, the Government cannot "compel" private entities to enter contracts with the Government. Confusion on this issue may lead to "no bids" on data requirements or requests by IP owners to omit certain data requirements and data rights clauses[58] from a contract.

The fundamental principle of freedom to contract[59] (or not to contract) effectively results in DoD being unable to *compel* any IP owner to agree to sell data or data rights, regardless of DoD's needs. Additionally, even if an IP owner agrees to sell certain data or data rights in the contract, DoD cannot force or compel an IP owner to perform its contractual obligations(e.g., if the IP owner elects to breach its contractual commitments).[60] Although the DoD may ask for greater than standard data rights, the IP owner can't be required to sell or relinquish greater than standard data rights as a condition of being responsive to a solicitation or as a condition for the award of a contract.[61]

A best practice to minimize confusion is to avoid using a form of "requires" or "requirements" when describing the data rights in a solicitation. Instead, programs should reference use cases for TD and CS and short and long-term mission goals or objectives, such as cost avoidance, sustainment, and competition. It is also recommended to clearly communicate with industry during opportunities like industry days and draft RFP periods to describe the use cases and needs.

5.2.3 Inapplicability and Consideration of DFARS Clauses in Non-FAR Agreements.

Non-FAR agreements include, but are not limited to, no-cost agreements, cooperative agreements, OTAs, CRADAs, and test service agreements. Users of non-FAR instruments should be familiar with any rules specific to those instruments.

There are some generally applicable considerations and terms, which may be helpful for both FAR and non-FAR agreements. However, specific DFARS rules are not mandatory for non-FAR agreements nor automatically included in their terms. If advantageous and not otherwise prohibited, the detailed guidance for TD and CS in FAR/DFARS contracts may be considered when developing terms for rights in TD and CS in non-FAR/DFARS contacts or agreements. In the absence of other applicable rules specifying default IP terms, the situation is analogous to special license negotiations with terms to be negotiated for the situation. While non-FAR

[58] Omitting required DFARS data rights clauses is a deviation that requires higher approval. *See* DFARS 201.402(1)(ii) (2025).
[59] Other than exercising authorities like eminent domain (under the Fifth Amendment to the Constitution) or the Defense Production Act (or other very specialized authorities).
[60] Although there is a well-established legal framework for challenging data rights assertions for TD and CS, there is no case precedent where the Court of Federal Claims issued an order compelling a contractor to deliver TD or CS under a DoD contract.
[61] *See* 10 U.S.C. § 3771(b)(8) (2025).

agreements may provide much greater IP flexibility, drafters should consider the downstream ramifications for use and handling data acquired with bespoke licensing terms.

While FAR and DFARS terminology and terms may be borrowed as appropriate or smart for use in non-FAR agreements when consistent with applicable rules, drafters and negotiators of agreement terms should utilize the generally greater flexibility offered by non-FAR agreements to make smart deals for DoD. In some cases, there may be consortium or other umbrella agreement that establishes reusable terms or framework for follow-on agreements.

Agency specific regulations and guidance for the specific non-FAR agreement type should be reviewed in drafting all IP agreement terms.

Modifying standard terms while keeping the standard labels for these modified terms can cause significant confusion, especially when managing data from such modified agreements alongside data from standard FAR/DFARS contracts or within common data management systems. Altering definitions of established terms can lead to inefficient data utilization or non-compliance with agreed upon license terms due to confusion over the meaning or scope of license requirements.

IMPORTANT CONSIDERATION

When drafting a non-FAR agreement, it is advisable to avoid using terms defined in the DFARS, such as Government Purpose Rights or Limited Rights, or copying a DFARS clause with its number (e.g., 252.227-7013) while modifying the words of the definition or clause.

5.2.4 Other Transactions, Agreements, and Authorities.

An OTA (e.g., commonly referred to as an "OT") refers to an agreement type under the 10 U.S.C. §§ 4021 and 4022 authorities that enable DoD to enter into transactions other than contracts, grants, or cooperative agreements for research projects, prototype projects, follow-on production OTAs and contracts. As such, the "A" in OTAs can mean "authorities" or "agreements;" this guidebook generally refers to the agreement (OTA) made under OT authorities. When leveraged appropriately, OTAs provide the Government with access to state-of-the-art technology solutions from traditional and non-traditional defense contractors (NDCs), through a multitude of potential teaming arrangements tailored to the project[62]

The most prominent feature of OTAs for the purposes of this Guidebook is that they are not subject to the contracting laws and regulations in the FAR and DFARS concerning data rights, rights in patents, and copyrights. However, they do not exist outside of the generally applicable laws regarding patents, copyrights, trade secrets and trademarks, or criminal law, such as regarding theft of trade secrets. For example, 28 U.S.C. § 1498, related to Government liability for patents and copyrights, applies to activities authorized under an OTA. Further, the fact that acquisition contract laws and regulations are not strictly applicable to OTAs does not make those rules entirely irrelevant.

[62] *See* Office of the Under Sec'y of Def for Acquisition and Sustainment, Other Transactions Guide (July 2023).

It may be useful for the Agreements Officer (AO) to be familiar with FAR-based IP rights as these laws and regulations are often used as models and starting points for drafting IP license terms. Personnel supporting existing OTAs may see terms copied from or similar to FAR contract and grant IP terms. Those laws and regulations may also serve to alert license drafters to points to consider.

Since these laws and regulations do not apply to OTAs, negotiation of rights that either mirror standard DFARS rights or are of different scope and operation is necessary. The AO should ensure consideration of the following when drafting IP terms for OTAs:

Table 9. Other Transactions Issue Topics and Considerations for IP

Issue Topic	Considerations
Disputes	Disputes clauses included in the agreement can accommodate specialized disputes arising under borrowed IP terms, such as the exercise of IP march-in rights or the validation of restrictions on TD/CS if such terms are borrowed.
Flow-down	Consider whether IP terms applicable to the awardee should flow down to sub awardees, including whether sub awardees should submit IP licenses or deliverables directly to the USG. In some cases, achieving flow down may involve multi-party negotiations (e.g., with Government, prime, and sub-contractors).
Licensing	Consider restricting awardees from licensing technology developed under the OTAs to domestic or foreign firms under certain circumstances that can hinder domestic manufacture or use of the technology.
Export	Be aware that export restrictions may prohibit awardees from disclosing or licensing certain technology to foreign firms.
Additional rights	Consider including in the IP terms any additional rights necessary for the USG in the case of inability or refusal of the private party or team to continue to perform.
Time based	It may also be appropriate to consider negotiating time periods after which the USG will automatically obtain greater rights.
Patents	Bayh-Dole Act (35 U.S.C. §§ 201-204) requirements on patent/invention rights do not apply to OTAs. Negotiate a patent/invention rights clause necessary to accomplish program objectives and foster the Government's interest while balancing the needs of the awardee. The AO should consider the USG's needs for patent rights to use the developed technology, or what other IP rights will be needed should the agreement provide for trade secret protection instead of patent protection. The AO should also consider clauses that require tracking and reporting of subject inventions made in the performance of OTAs. OTAs are not subject to the Bayh-Dole Act governing the Government's rights in inventions and patents.[63]
Trade Secret Protection	Consider allowing subject inventions to remain trade secrets as long as the USG's interest in the continued use of the technology is protected. In making this evaluation, the AO should consider whether allowing the technology to remain a trade secret creates an unacceptable risk of a third party patenting the same technology or otherwise jeopardizes the USG's right to utilize this technology with third parties, and whether there are available means to mitigate these risks outside of requiring patent protection.

[63] Bayh-Dole Act 35 U.S.C. §§ 201-204 (2025).

Issue Topic	Considerations
TD and Software Rights	These rights do not exist unless written into a non-FAR agreement. License negotiations often center on the USG's ability to release or disclose data or software outside the USG. The OTA should address license considerations as described for SNLs elsewhere in this guide but excluding concerns with rights minimums in the DFARS. OTA drafters should consider TD and software rights for Government requirements while balancing awardee interests. Section 4022(f) authorizes follow-on production OTAs and contracts when specified conditions are met. Recall the warning box in Section 2.7 that in later FAR contracts, for purposes of the data rights funding test, earlier Government OTA spending is not considered Government funding for funding-based data rights. So, especially in OTAs that may lead to later production of a prototyped system, OTA drafters should consider Government requirements throughout the life cycle of the project or system. Again, remember that DFARS type data rights or restrictions will not apply unless they are written into an OTA deliberately.
Data Rights Markings	In addition to those considerations, since there are no prescribed restrictive data rights markings for OTAs, consideration of restrictive markings should get special attention. There is ostensibly a lot of latitude on the part of the parties regarding markings indicating proprietary restrictions. However, USG drafters and negotiators should bear in mind the operational impacts of the markings and associated license rights, especially if data from an OTA is expected to be used and/or distributed extensively and for a long time, or to other agencies or third parties, such as contractors. Bespoke markings for a particular agreement may be very useful, but if data marked with unique markings needs to circulate in the larger DoD data ecosystem, such markings may impede efficient data utilization or risk compliance failures with agreed upon restrictions . Consultation with data managers and IP attorneys may be especially useful regarding marking issues.
Commercial Data	The AO should consider commercial TD and commercial CS. The USG typically does not need extensive rights in commercial TD and software. However, depending on the project scope and goals, the USG may need to negotiate for greater rights to utilize the developed technology. If the OTA incorporates terms and conditions from a commercial software license agreement, it would be prudent to negotiate with the IP owner regarding any terms that are inconsistent with Federal law or do not meet the Government's needs
Cyber Incident Reporting	Ensure the company is properly protecting data and compliant with any applicable specific USG reporting procedures in the event USG data is compromised.
Authorization and Consent	Authorization and consent policies provide that work by an awardee under an agreement may not be enjoined for patent or copyright infringement and shifts liability for such infringement to the USG.
Notice and Assistance	If included, notice policy requires the awardee to notify the AO of all claims of infringement that come to the awardee's attention in connection with performing the agreement. If included, assistance policy requires the Awardee, when requested, to assist the USG with any evidence and information in its possession in connection with any suit against the USG, or any claims against the USG made before suit has been instituted that alleges patent or copyright infringement arising out of performance under the agreement.
Indemnity	The USG's liability for damages in a suit for patent infringement may ultimately be borne by the awardee in accordance with the terms of a patent indemnity clause, if included. Indemnity clauses mitigate the USG's risk of extra costs caused by infringement of a third-party owned patent. Such a clause may be appropriate if the supplies or services used in a technology developed under the agreement normally are or have been sold or offered for sale to the public in the commercial open market. Since the operation of U.S, law is limited to the U.S., including an authorization and consent clause when both complete performance and delivery are outside the United States, its

Issue Topic	Considerations
	possessions, and Puerto Rico may not be necessary.[64] In addition, where trade secret protection is allowed in lieu of patent protection for patentable subject inventions, a perpetual patent indemnity clause might be considered as a mechanism for mitigating risks.[65] Conversely, the agreement should not include a clause whereby the USG expressly agrees to indemnify the awardee against liability for patent infringement. Absent specific statutory authorization, indemnifying an awardee risks an Anti-Deficiency Act[66] violation.

5.3. Draft and Issue the Solicitation.

Now with the contract type decided (FAR/non-FAR, competitive/non-competitive), the team is ready to build the RFP. The RFP should be aligned to the IPS and the chosen approaches for seeking data, CS, and rights to support the program objectives for the current phase as well as future phases. The critical steps in aligning the RFP to the IPS are to identify how the program will order deliverables, describe the specific business and technical needs, build the contract data requirements package, and finally plan the IP Evaluation Criteria.

Myths: There are a couple of common pitfalls that lead programs to delay or not procure the data they may need:

Incorrect Assumption: Data is too expensive and not in the budget.

Fact Check: Obtaining a copy of data generated by an IP owner should not be cost-prohibitive if priced while still in the competitive stages of acquisition. Obtaining data and securing rights will mitigate additional (premium) cost for the data, CS, and rights later after competition has concluded. Ultimately, ordering data earlier should be viewed as cost avoidance to help programs reach their planned cost objectives rather than an added cost. It IS true that buying the data, outside of competition and well into program execution, could be extremely expensive.

Incorrect Assumption: Because the Government paid for development and therefore has data rights under the funding rule, the Government has rights to the data any time needed.

Fact Check: For FAR/DFARS contracts, securing data rights requires delivery. The program might be entitled to rights to the data based on the funding rule (see Sections 2.7), but this does not equate to a requirement for an IP owner to deliver the TD or CS. If the Government needs the data, the Government needs to buy the deliverables.

These misconceptions and pitfalls leave programs with little effective recourse to obtain needed data, CS, and rights. In some cases, IP owners may state that the Government had time-limited opportunity to order data from funded development activity and failed to do so. Or IP owners assume the Government made a conscious decision in not ordering delivery of data and that was factored into the IP owner's business plans, and they assumed that it was factored into the Government's acquisition plans as well. Ideally, Government decisions to acquire (or not

[64] *Compare* FAR 52.227-1 (2025).
[65] *Compare* FAR 52.227-3 (2025).
[66] *See* 31 U.S.C. § 1341 (2025).

acquire) necessary data, CS, and rights are thoughtful and purposeful and are fully documented within the IPS.

5.3.1 Data ordering mechanisms.

In FAR contracts, there are tools that are used to acquire data, (e.g., regular ordering, deferred delivery, deferred ordering, priced options, and escrow accounts). It is important to understand what the tools enable and when they are appropriate for use. As covered in the use case discussion (see Section 4.1.6), timing of the data needs should be a critical factor in determining the most effective ordering mechanism. Table 10 describes the role, scope, and conditions on using each tool.

Definite data requirements with known dates of need should be addressed with regular ordering at contract award. Deferred delivery may be used to acquire definite TD and CS needs on a more flexible or longer schedule. Deferred ordering is best used as a backstop to regular ordering but should not be used as the primary means for acquiring data and data rights. The Deferred Ordering clause (DFARS 252.227-7027) may only be used to order data generated in performance of the contract where the clause was incorporated. The clause may not be used to order data generated under another Government contract where the clause was not included or outside any Government contract. It does NOT allow for ordering of data that was utilized in a contract but not generated in that contract.

Priced options can be advantageous for securing data, CS, and rights that are often not needed until a later time. However, in limited situations where data, CS, and rights acquired by option are obtained with the intent of enabling either organic or third-party competition with an IP owner, and the option is exercisable at award, there may be a lot of uncertainty to the IP owner in its projections of potential future revenues. So, any potential discount for options compared to regular ordering might be minimal or even negative due to the uncertainty for the prospective contractor when an option is exercisable immediately upon award. Therefore, it is important to evaluate the price of the option during competition to leverage competitive pressure on both the option holder and potential replacement contractors. In simpler terms, priced options may come with a higher price tag than using regular ordering.

Alternatively, if the Government is unlikely to want or be able to exercise the option for some period, declining to order data with competitive rights with regular ordering, but instead postponing competition capability with an option with a future exercise period may be mutually beneficial. Having an option exercise period some years in the future may give the IP owner greater certainty in calculating ROI and allow a longer period of ROI before facing renewed competition. It may also be preferable to order data by standard ordering and take delivery early in a contract to allow early technical validation of the data including its suitability for use by third parties, but with greater rights being granted with the later exercise of the option. If data validation is likely to require IP owner support, it may be beneficial to solicit a special license with the ability to use IP owners for early validation activities with an option exercisable later for additional rights to facilitate the full competitive use.

Data Escrow Accounts are agreements the Government makes with the IP owner to place the data with a third party (escrow agent) for safe keeping. The agreements stipulate under what

time or conditions (e.g., 10 years, when the company goes out of business, etc.) the data will be delivered to the Government. There will be a cost associated for the escrow services which will need to be paid. This might be an attractive tool to contractors for negotiation of data and data rights that may mitigate Government concerns regarding data necessary to address diminished manufacturing sources and material shortages (DMS/MS) or parts obsolescence.

Table 10. Data Ordering Tools

Tools	FAR/DFARS/PGI Section; & Purpose	Data Rights	Features & Functions	Pricing	Benefits
Regular Ordering	DFARS 215.470(b); To order data as required.	Rights specified by DFARS clauses, special licenses, or commercial licenses.	Delivery of data timing is specified in DD1423 Contract Data Requirements Lists and must be during the contract period of performance (POP).	Price for data, CS, and rights should be determined and evaluated at the time of award.	Allows definite data, CS, and rights requirements to be met on a defined schedule.
Deferred Delivery	DFARS 252.227-7026; To order delivery of TD and CS identified in contract as deferred delivery.	Rights specified by DFARS clauses, special licenses, or commercial licenses.	Executable during POP, within 2 years after later of: 1) acceptance of all items (other than data or CS); or 2) contract termination, for subcontractor TD, executable within 2 years after contractor accepts the last delivery for the contract of the item (to which the data pertains) from the subcontractor.	Price for data, CS, and rights should be determined and evaluated at the time of award.	Allows definite TD and CS and rights requirements to be met on a flexible schedule.
Deferred Ordering	DFARS 252.227-702; To order TD and CS generated in performance of the contract.	Rights specified by DFARS clauses or special licenses.	Executable during POP or within 3 years after: 1) acceptance of all items (other than TD or CS); or 2) the termination of the contract. For subcontractor TD, within 3 years after contractor accepts the last delivery for the contract of the item (to which the data pertains) from the subcontractor.	Contractor is only compensated for converting the data or CS into the prescribed form, for reproduction and delivery. The price of rights should be part of the initial contract price and evaluated then.	Allows initially unknown requirements for TD or CS generated in contract performance to be determined and added during a contract.
Priced Option	FAR 17.2; To obtain a firm price for data, CS, and rights that, except in limited circumstances, are not needed at the earliest possible date.	Rights specified by DFARS clauses, special licenses, or commercial licenses.	Options must be established at contract award. May be exercised during the contract at a time or period specified in the option. Depending on circumstances, option periods longer than 5 or 10 years may require higher level approvals. It especially important to consult counsel on option timing and related fiscal issues.	Price for data or data rights option should be determined and evaluated at the time of initial award.	Allows identifiable but optional requirements for data, CS, and rights to be priced at contract award, preferably competitively.
Escrow Account	DFARS .227.7203-2 and PGI 227.7203-2; To allow a third-party escrow agent to safekeep designated TD or CS until a specified condition occurs	Rights specified by DFARS clauses, special licenses, or commercial licenses.	If a contractually specified condition occurs, then the Government may obtain delivery of the escrowed TD or CS. Requires agreements with third parties for support.	Price for data, CS, and rights should be determined and priced at the time of award.	Not preferable, it may be useful when formal delivery or access is not feasible or cost-effective during the contract period of performance or delivery schedule

5.4. IMPORTANCE OF IP DELIVERABLES.

5.4.1 "Possession is nine-tenths of the law".

Most have heard the adage that "possession is nine-tenths of the law." While this is not literally true in many legal contexts, there is some wisdom in the concept. For a DoD program, it is important to have necessary data rights, but rights in data without possession of the data (called "inchoate rights") is of very little real value because they cannot be exercised. In plain terms, "the program can't use what it doesn't have."

Because IP is a type of intangible personal property interest, making it tangible with clearly defined deliverables is critical to exercising any kind of rights. The confusion between having "data rights" and having "data deliverables" has led many programs to not procure data deliverables early in a program.

Utilizing the needs assessment for IP in the IPS, a Contract Data Requirements Package (CDRP) is developed in accordance with DoDM 5010.12. A CDRP is comprised of CDRLs (DD Form 1423) and other data related instructions such as DID. CDRLs provide instructions to a contractor for data preparation and/or delivery that will meet specific approval and acceptance criteria.

It is a best practice to ensure CDRLs are mapped to Statement of Work or Performance Work Statement requirements to ensure contractors deliver required data, and to document a clear record of what was developed in performance of the contract and required to be delivered. This also helps the Government understand funding-based rights that it may be able to require in later contracts.

NOTE: DoDM 5010.12, *Acquisition and Management of Contractor-Prepared Data*, provides detailed guidance on the procedures for properly ordering data.

5.4.2 Planning for IP evaluation in proposals.

DoDI 5010.44 directs DoD Component Heads with contracting authority to "[i]ncorporate types of IP deliverables and level of associated license rights into source selection evaluation factors, and as negotiation objectives in sole-source awards, as appropriate."
This is appropriate in both FAR and non-FAR acquisitions, but applicable rules and policies differ.

Clearly articulating and communicating in an RFP the IP information desired by the Government and how it will be evaluated serves as a strong signaling function for communicating Government interests and priorities regarding IP in any source selection. The objective of Government-industry negotiations is a mutually beneficial outcome for both parties for which the solicitation sets the stage for more in-depth negotiations in most cases. Careful and thoughtful drafting of the solicitation, and description of desired IP and IP rights are excellent first steps to achieve successful negotiations.

Guidance about DFARS rules of engagement and evaluation of IP in DFARS source selection are not directly applicable to non-FAR agreements. So, while that guidance may be informative,

it should NOT simply be used verbatim in a non-FAR situation. Evaluation for non-FAR agreements can be approached as a determination of best value for the Government. Agency specific regulations and policies should also be consulted.

Competitive source selection evaluation of IP rights is often the best tool available to ensure that the Government can affordably obtain needed IP rights. However, "IP evaluation" can occur in many contexts, including non-competitive environment such as sole source negotiations, negotiations of special licenses, and even at an earlier stage in requirements development.

IP Evaluation was the primary subject and focus of the FY2020 NDAA Sec. 801 Pilot Program. The 801 Pilot Program explored novel, alternative, and commercial methodologies for IP valuation and evaluation. Based on the Pilot Program, one of the key takeaways was that the DoD can and should evaluate IP in its competitive source selections and include IP in its negotiation objectives in sole source awards.[67]

TD rights evaluation criteria can be crafted and used to support the source selection process. When using source selection to acquire IP, data and license rights, requirements should be directed at the data that supports short and long-term objectives of the program. Caution should be exercised to avoid asking for broad IP and associated rights at the system level as a source selection objective. For example, seeking Government Purpose Rights for entire systems as a source selection factor may be overreach, and in most cases is unwarranted. The VATEP approach based on IP and rights use cases evaluated in accordance with DFARS 227.7103-10(a)(5) and 227.7203-10(a)(5) is recommended when the size and importance of the acquisition warrants the time and effort necessary to execute such an approach.

Current DoD policy and regulations permit considering the effects of contractor IP rights restrictions on meeting the Government's objectives.[68] The ability to consider the effects of IP rights on meeting Government mission objectives in source selection can be a powerful signal and motivator to offerors as to what is most important for the Government and what the Government would like to see proposed for any given contract. Source selection criteria have long served this function generally but perfecting this tool with respect to IP is still a work in progress.

5.4.3 Request feedback from industry and issue final RFP.

A pre-solicitation best practice is to issue a draft RFP for feedback from industry. From an IP perspective, this feedback will help ascertain the likelihood of receiving what was requested and any potential risk areas.

This approach is particularly important to prepare for effective interest-based negotiations regarding IP issues. The feedback will provide insight into industry's interests and objectives and help the program understand primary opportunities for compromise. These communications may be viewed as the opening round of dialogue and engagement with industry on IP issues leading to negotiation of special license terms.

---

[67] *See* Appendix A – Key References (e.g., "Report to Congress on Pilot Program on IP Evaluation for Acquisition Programs for FY 2023, Pursuant to Sec. 801 of the NDAA for FY 2020 (P.L.116-92); Sec. 6. Enclosure 3) FY23 [Government Data Call] on IP Evaluation & Valuation – List of Figures and Tables; and Figure 2-5: TTPs Used by FY23 Respondents and Corresponding Impact on Mission Goals.)".

[68] *See e.g.*, DoDI 5010.44, *supra* note 2, at 6; *see also* DFARS 227.7103 (2025); DFARS 227.7203 (2025).

5.5. EVALUATE IP AND DATA RIGHTS IN PROPOSALS (SOURCE SELECTION).

As noted previously, the evaluation of IP is not only for competitive source selections, but due to their priority and complexity, this section will focus on IP Evaluation in a FAR Part 15 Source Selection. DFARS PGI 215.300 makes the DoD Source Selection Procedures (SSP) mandatory "when conducting negotiated, competitive acquisitions utilizing FAR part 15 procedures".

The SSPs set out detailed procedures for conducting competitive source selections using several evaluation factors in accordance with FAR 15.304. Factors to be evaluated must always include cost or price to the Government. Other factors include technical factors, past performance, and small business participation.

The SSPs do not mention IP or data rights as an independent factor so IP needs to be considered through use of other factors, such as technical factors or cost or price. The SSPs include an Appendix E[69] regarding evaluation of IP in source selection.

5.5.1 Methods for IP evaluation.

This guidebook will highlight two best practices for IP Evaluation Methods: use cases and VATEP.

1) **IP- Evaluation Factors based on Government Use Cases**:

IP-related technical evaluation factors may allow the Government to assess proposals (or approaches provided in proposals) based on impacts on use cases of mission readiness, competition, obsolescence risk, and long-term license fees. Such evaluations allow programs to have a comprehensive understanding of an offeror's proposal, including how the Department can execute its long-term sustainment goals, facilitate competition, and manage program risks.

Offerors may be given a strength or a weakness in an IP-related evaluation factor (or subfactor) based on whether the proposal of approach supports a particular goal, such as competitive procurement goals, MOSA implementation goals, or cost avoidance savings for commercial licenses. For example:

- The offeror's proposal may be given a strength for a proposed approach that permits the Government to competitively procure hardware from third parties using acquired IP and associated rights, and a strength for a proposed approach that permits the Government to competitively procure hardware maintenance and sustainment services from third parties.
- The offeror's proposal may be given a weakness for a proposed approach that does not permit the Government to competitively procure hardware from third parties, and a weakness for a proposed approach that does not permit the Government to competitively procure hardware maintenance and sustainment services from third parties.

In accordance with 10 U.S.C. § 3771 and DFARS 227.7103-1, offerors would not be required, either as a condition of being responsive to a solicitation or as a condition for award, to sell or otherwise relinquish to the Government rights in TD related to items, components or processes

[69] DFARS PGI 215.3 Source Selection Procedures, 2 (20 Aug. 2022) [hereinafter PGI 215.3].

developed exclusively at private expense except for the data, CS, and rights identified at DFARS 227.7103-5(a)(2) and (a)(4) through (9).

An offeror that does not propose to sell or otherwise relinquish any additional rights in TD related to items, components or process developed exclusively at private expense would still be considered responsive.

2) **IP Evaluation using VATEP**:

VATEP is a "tradeoff source selection process with adjustments to an offeror's evaluated price to reflect the value of certain enhanced performance characteristics."[70] The VATEP Technique "monetizes different levels of performance that may correspond to the traditional requirements process of defining both threshold (minimum) and objective (maximum) performance and capabilities."[71] The Government must then determine if a higher rated technical offer is "worth" the additional cost to the Government.

REMEMBER: During the IP Strategy development phase, the program should have determined the value of the IP requirements for the program based on a combination of use cases, priority, likelihood of need, consequence of not receiving the IP, etc. With a VATEP approach, value is understood as the intersection of capability acquired versus cost.

The description of VATEP in the SSPs is especially relevant: "Value and cost are separate concepts that VATEP links in the RFP to inform industry decisions on what to offer to gain a competitive advantage. As described herein, VATEP is merely a structured technique for objectivizing how some (or all) of the requirements would be treated in the tradeoff process and then communicating that to offerors via the RFP."[72]

There are four core building blocks for applying the VATEP approach to IP Evaluation:

- Use cases: Identify purposes or uses for all TD, CS, and other information needed to support all program needs in the near term and long term.
- What Price to Adjust: Identifying requirements which could incentivize an additional grant of rights from the IP owner for an adjustment in proposal price based on the "value" placed on better performance.
- Application: assess the extent to which the offered IP rights enable the various use cases with incremental VATEP credit per enabled use case to come up with an overall VATEP adjustment.
- Variations/Best Practices.

[70] *Id.*
[71] DEF. ACQUISITION UNIV., VALUE ADJUSTED TOTAL EVALUATED PRICE (VATEP) (2025), https://www.dau.edu/acquipedia -article/value-adjusted-total-evaluated-price-vatep.
[72] PGI 215.3, *supra* note 69, at App. B.2.

Additional resourcing on conducting VATEP can be found through the DAU website (see Appendix E for Resources and Tools).

5.5.2 Negotiating for IP.

IP acquisition can be as simple as identifying needed data, CS, and rights, following the procedures to implement these in a contract or agreement, getting a reasonable price and executing the contract. However, sometimes a contractor's business objectives may not readily align with that. Therefore, it is important for acquiring activities to understand other tools to incentivize proposals regarding data and IP rights that better align the mutual interests of DoD and industry. Other than simply cash, the primary tool available to acquiring activities is evaluation of IP rights in competitive source selection.

To effectively plan for IP negotiations, Government personnel need to identify and articulate IP needs, objectives, and interests and any desired IP rights to contractors. Successful negotiations will require effective communication or coordination both within the Government acquisition team and with contractors. The IP Evaluation Pilot Program data clearly demonstrated that the best time to conduct negotiations for IP-related license rights is prior to contract award.[73]

Figure 19. Important Information for Negotiations

- **Data requirements to achieve capability and program objectives.**
- **Understanding of the financial investment from both parties & expected ROI.**
- **Prioritization of use cases based on risk and opportunity analysis.**
- **IP Valuation for government and industry based on independent IP Valuation and market research.**
- **IP Evaluation approach based on contract strategy and program objectives.**

Considerations for SNLs: As noted in the introduction, there is a DoD policy preference for specially negotiated IP licenses rooted in statute.[74] Such special licenses may be incorporated in contract addenda (including access agreements[75]), public-private partnership agreements, patent and trademark licenses, and authorization to use Government-furnished TD or software under a Government contract.

A good special license departs from any applicable standard or default terms because doing so is in the better interests of both parties to the license; creativity for the sake of creativity is not desirable. In fact, there are usually extra administrative costs to the Government for managing

[73] *See* Appendix A – Key References (e.g., "Report to Congress on Pilot Program on IP Evaluation for Acquisition Programs for FY 2023, Pursuant to Sec. 801 of the NDAA for FY 2020 (P.L.116-92); Sec. 3.3.2 'Detailed Data Analysis' and Sec. 3.3.2.5.6 'Program Schedule Impacts Associated with Negotiated Licenses related to Technical Data and/or Software;' and Enclosure 3), Figure 5-7(b).'Timing of Negotiations Conducted for IP-Related LRs & Impacts to Program Schedules, By Comparable FY21 & FY23 Respondent Percentages.')"

[74] 3774, *supra* note 44.

[75] Access agreements permit the Government to view or access technical data or software in contractor-controlled repositories or facilities.

data with special or customized license terms. So, a special license that has the same effect as a standard license right but requires additional effort to understand or interpret is undesirable.

Additionally, the terms of special licenses are not just important at the time they are being negotiated and executed. Since those terms will govern Government handling and management of the licensed data often for years or even decades, the terms must be understandable and not create undue burdens on the Government or its employees, or third parties to whom the data may be provided.

The assessment of the SNL should be centered around the parties' interests, which may include ROI, mission needs, clarity and transparency, cost and ease of administration, compatibility with rights in similar data, etc. To determine whether the proposed license provides fair and reasonable value for each party, it is important to consider various aspects of the proposed license, including:

- The scope of the proposed license, including the scope of the TD and license rights provided under the proposed license compared to the scope of the standard license and to the Government's needs.
- The total amount of funding contributed or to be contributed by the Government for development, production, enhancement, refinement, or modification of the item or process to which the license pertains.
- The valuation of the IP and IP rights.
- Any other monetary and non-monetary consideration that the contractor will provide to the Government (including products, TD or software deliverables, lower prices, or broader license rights in other TD or software).

Understanding when a special license needs to be negotiated requires real understanding of the underlying foundational DFARS rights. To stay informed on evolving IP policies and tactics, DoD personnel need to review updates to DoD guidance, seeking DAU training opportunities, and consult dedicated IP SMEs (OSD IP Cadre, Service IP Cadres or local IP Legal SMEs).

In drafting and negotiating SNLs for noncommercial TD and CS, the DFARS specifies minimum required license rights — Limited Rights for TD[76] and Restricted Rights[77] for CS. Such special licenses may not go below these floors without approval of a DFARS deviation at the Office of the Secretary of Defense.[78] These rules on deviations from the FAR and DFARS do not apply to OTAs and other non-FAR agreements.

5.5.3 Award the contract.

At the completion of the solicitation process, the team should be confident that the program will receive the data, CS, and rights necessary not only to execute this phase of the program, but that the program is also postured to meet the life cycle capabilities required by the warfighter.

[76] *See* 7013, *supra* note 8, at (c)(4).
[77] *See* 7014, *supra* note 9, at (c)(4)(i).
[78] *See* DFARS 201.402(1)(ii) (2025); *see also*, for procedures DFARS 201.402(2) (2025).

A successful contract award is not measured simply as one that was awarded on time or on a pre-determined budget, but rather one that effectively meets the capability and program objectives, actively mitigates risk, creates opportunities, and allows flexibility for the dynamic needs of the mission.

As with all aspects of the contract, the IP portions require active management discussed in Section 6.

SECTION 6: MANAGING/MAINTAINING THE IPS

This section provides guidance on how to execute the IPS post-contract award in the daily execution of the program including inspecting and accepting deliverables, verifying markings, managing/maintaining data rights, and invoking data rights challenge procedures.

6.1. INSPECTING AND ACCEPTING DATA DELIVERABLES.

This subsection emphasizes the importance of proper delivery, access, and securing of IP rights for the Government. It outlines the critical steps for managing and maintaining the quality, integrity, security, and usability of the data. It also details the verification process for data rights markings and the handling of nonconforming markings, advising on best practices for personnel receiving data deliveries.

6.1.1 Acceptance of data.

To effectively use IP deliverables, it is critical that they are properly delivered, or sufficient access means are arranged, and that necessary IP rights are secured for the Government, usually by a license agreement. It is also critical that the program office ensures the acquired data and associated metadata are managed and maintained to preserve the quality, integrity, security, and usability of the data. This includes not just ensuring that the data is technically accessible, but also that the data is controlled based on licensing terms governing what data can be shared with whom and what must be kept confidential. Processes should be established to protect all data that contain critical technology information, as well as ensuring that limited distribution data, IP data or proprietary data are properly handled throughout the life cycle, whether the data are in hard-copy or digital format.

Designated data recipients should verify content, format, and quality of all contractually required data. Improper license rights markings are characterized as non-conforming or unjustified.[79] Before acceptance, designated data recipients should inspect contractually ordered data deliverables to ensure markings follow such requirements as:

- Data rights agreements, including DFARS clauses when applicable.
- Contractually imposed Government distribution statement instructions.
- Form DD-254 Security Agreement instructions (e.g., classification markings) or Controlled Unclassified Information (CUI) instructions.
- Export control marking requirements; and
- Marking instructions included in CDRLs and associated DIDs.

See DoDM 5010.12 for more information on data inspection and acceptance.

[79] *See* DFARS 227.7103-12 (2025) (technical data) [hereinafter 7103-12]; *see also* DFARS 227.7203-12 (2025) (computer software) [hereinafter 7203-12].

Table 11. Characteristics of Improper Markings

	(a). Nonconforming Markings	(b). Unjustified Markings
▪ **RIGHTS IN TD** (e.g., Other Than Commercial Products and Commercial Services)	(1) **Authorized markings** are identified in the clause at 252.227-7013[80], Rights in TD—Other Than Commercial Products and Commercial Services. ▪ All other markings that are directed to the Government's use and disclosure of the TD are **nonconforming markings**. ▪ An authorized marking that is not in the form, or differs in substance, from the marking requirements in the clause at 252.227-7013[81] is also a **nonconforming marking**. ▪ See also, DFARS 227.7103-12(a)(2)[82].	(1) An **unjustified marking** is an authorized marking that does not accurately reflect restrictions on the USG's use, modification, reproduction, release, performance, display, or disclosure of the marked TD, in accordance with the applicable data rights clause. ▪ For example, a Limited Rights legend placed on TD pertaining to items, components, or processes that were developed under a USG contract either exclusively at Government expense or with mixed funding (situations under which the Government obtains Unlimited or Government Purpose Rights) is an **unjustified marking**. ▪ See also, DFARS 227.7103-12(b)(2)[83].
▪ **RIGHTS IN CS** (e.g., Other Than Commercial CS and Other Than Commercial CS Documentation)	(1) **Authorized markings** are identified in the clause at DFARS 252.227-7014[84], Rights in Other Than Commercial CS and Other Than Commercial CSD. ▪ All other markings that are directed at the Government's use and disclosure of the software are nonconforming markings. ▪ An authorized marking that is not in the form, or differs in substance, from the marking requirements in the clause at 252.227-7014 is also a **nonconforming marking**. ▪ *See also*, DFARS 227.7203-12(a)(2)[85].	(1) An **unjustified marking** is an authorized marking that does not accurately reflects restrictions on the USGs use, modification, reproduction, release, or disclosure of the marked CS or CSD, in accordance with the applicable software rights clause. ▪ For example, a Restricted Rights legend placed on CS developed under a government contract either exclusively at Government expense or with mixed funding (situations under which the Government obtains Unlimited or Government Purpose Rights) is an **unjustified marking**. ▪ *See also*, DFARS 227.7203-12(b)(2)[86].

6.1.2 Conformance of restrictive markings.

Acceptance of delivered data that are not marked consistent with the marking requirements in the contract may result in the Government losing the opportunity to leverage its legal rights to TD, CS, or other data under the contract. Noncommercial TD and software under DFARS contracts have specified markings or legends that must be used to indicate restrictions on the use or

[80] 7013, *supra* note 8, at (g)-(i).
[81] *Id.*
[82] 7103-12, *supra* note 79, at (a)(2).
[83] *Id.* at (b)(2).
[84] 7014, *supra* note 9, at (g)-(i).
[85] 7203-12, *supra* note 79, at (a)(2).
[86] *Id.* at (b)(2).

distribution of the data. See Section 6.3 for a discussion of challenge procedures for handling improper markings.

The titles of the permitted data rights markings under the DFARS for noncommercial TD and software to restrict the rights of the Government are Government Purpose Rights, Limited Rights, Restricted Rights, Special License Rights, and SBIR/STTR Data Rights.[87] Any markings to restrict the rights of the Government other than those specified or altered versions of the specified markings are said to be "nonconforming markings." However, markings to provide notice of copyright as prescribed under 17 U.S.C. §§ 401 or 402 are allowable.

The DFARS clauses provide comparatively expeditious procedures to remove nonconforming markings. For either TD or CS, a contracting officer may notify a contractor of nonconforming markings and if the contractor fails to remove or correct the nonconforming markings within sixty days, the Government may ignore or, at the contractor's expense, remove or correct any nonconforming markings.[88]

It is a best practice for personnel receiving deliveries of data, data managers, or other personnel using contractor data to notify the appropriate contracting officer or Contracting Officer Representative promptly upon the discovery of nonconforming markings to permit timely corrective action.

6.2. MAINTAINING DATA RIGHTS.

Continuous attention to the scope and accuracy of restrictive markings on data is necessary to protect the Government's rights. Potential legal liabilities and program execution frustrations can arise from lost opportunities to secure rights to data. See DoDM 5010.12 for additional guidance on management of contractor-prepared data.

6.2.1 Importance of managing data rights records.

Continuous and diligent attention to the scope and accuracy of restrictive markings on data acquired by the Government is necessary to protect the Government's rights during the life of a program and until data is retired from use. Failure to properly handle data can lead to legal liability for the Government or individual Government employees and costly, time-consuming litigation may frustrate program and mission execution.

It is particularly critical that the details of specially negotiated licensing terms are maintained, connected with covered data, reflected in training and handling guidance to the workforce, and implemented into data management systems. If records of special licenses are lost, it may be impossible to reconstruct such terms. For IP licensing terms that have a fixed expiration date, it is critical to track license duration for those fixed-term licenses along with disposition instructions at termination. For data licenses of perpetual duration, it is critical that records of the license terms are maintained and provided to users of the data for as long as the data exists in Government custody.

[87] *See* 7013, *supra* note 8; 7014, *supra* note 9; 7018, *supra* note 18.
[88] *See* 7013, *supra* note 8, at (h)(2); 7014, *supra* note 9, at (h)(2); 7018, *supra* note 17, at (h)(2).

6.2.2 Preventing loss of rights in data.

Some programs have experienced the loss of Government rights to use data freely through intentional or inadvertent "capturing" of Government data as alleged contractor proprietary data. Anyone receiving deliverables and briefings from contractors should be on the looking for information provided as GFI that is submitted back to the Government marked as contractor proprietary information. These activities are typically when intentional or inadvertent "capturing" occurs.

Tolerance or acceptance of contractor claims to ownership of Government data or even publicly available information can establish precedents. They can also establish courses of dealing or create false impressions on the part of Government employees or support contractors regarding the source of data and who has rights to use or control it.

Maintenance of rights in data requires ongoing and continuous vigilance. Doing so is an essential practice for the Government to maintain its data rights and avoid any "capturing."

6.2.3 Complying with licensing obligations.

Complementary to maintaining Government rights in data is the necessity to comply with all agreed upon license obligations. Government license obligations are contractual obligations, which may substantially survive the contractor's period of performance. In fact, many licenses are perpetual in duration; meaning that any restrictive obligations must be tracked and enforced for as long as the data exists in Government hands and systems.

A lack of understanding about the types of IP license rights and how SNLs work can lead to frustration and breaching of contractual obligations.

When data subject to license restrictions is handled or distributed manually, handlers must be familiar with restrictive markings and all applicable license restrictions on the data. They must ensure that the information is only distributed to authorized recipients under authorized circumstances with proper safeguards.

When data subject to license restrictions is handled through automated information systems (e.g., databases systems and networks), it is important that the systems are properly configured. These systems and networks should be programmed to process metadata containing rights information, and to handle the data in accordance with the applicable restrictions.

SNLs and customized commercial licenses for software are often complicated and require workforce training, consultation, or both to properly implement the license restrictions in IT systems.

One special case is worthy of emphasis: namely, the case of Government Purpose Rights for noncommercial TD and software. A "Government Purpose" means any activity in which the Government is a party, including in cooperative agreements situations with international or multi-national defense organizations, or in situations involving sales or transfers by the

Government to foreign governments or international organizations.[89] Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose TD for commercial purposes, or authorize others to do so.[90] Before a contractor receives Government Purpose Rights data, it should be ensured that they will be using it for a Government purpose, not their own commercial purpose. Further, it should be ensured that the contractor has the applicable NDA in place.[91] Government Purpose Rights data should not be marked with Distribution Statement A, C, or D, which would authorize public release or distribution to contractors without checking for the necessary Government Purpose Rights conditions.[92]

6.3. VALIDATING RESTRICTIONS AND DATA RIGHTS CHALLENGES.

Challenging, verifying, or validating asserted restrictions generally refers to a statutory and regulatory process available to the Government after the award of a contract in which the Government may question contractor asserted data rights restrictions (e.g., improper markings) and request proof of contractor funding of development.[93] In simpler terms, data rights challenges are a DFARS process for questioning the factual basis of contractor asserted restrictions on the Government's rights to use and distribute TD and software (other than commercial software).

Data rights challenges can take a long time due to the procedural rules and because challenges often involve analysis and arguments regarding complex accounting and technical issues, often requiring subject matter experts to help with these issues.

It is for these reasons that data rights challenge procedures may be invoked prior to contract award, but the DFARS advises the Government to "avoid challenging asserted restrictions prior to a competitive contract award unless resolution of the assertion is essential for successful completion of the procurement."[94]

However, if IP will not be evaluated in a competitive source selection or if awarding a contract that will be sole source for any reason, but especially if the sole source award is premised upon a lack of necessary data rights for competition, the DFARS guidance about pre-award challenges should be considered very carefully.

The DFARS permits questions about the validity of asserted restrictions to be postponed to post-award, but it is also clear that the USG has more leverage and freedom to maneuver prior to awarding a contract.

[89] *See* 7013, *supra* note 8, at (a); 7014, *supra* note 9, at (a); 7018, *supra* note 17, at (a).
[90] *Id.*
[91] *See* DFARS 252.227-7025 (2025); DFARS 227.7013-7 (2025).
[92] *See* U.S. DEP'T OF DEF. INSTR. 5230.24, DISTRIBUTION STATEMENTS ON DOD TECHNICAL INFORMATION, 11-14 (10 Jan. 2023).
[93] *See e.g.*, DFARS 227.7103-13 (2025) [hereinafter 7103-13]; DFARS 227.7203-13 (2025; DFARS 252.227-7019 (2025) [hereinafter 7019].
[94] 7103-13, *supra* note 93, at (b).

Sample Scenario

Suppose there are known and well-founded reasons to question the factual basis of asserted data rights restrictions such that a program and contracting officer firmly intend to initiate challenge procedures post-award. That means the USG is entering into a contractual relationship with a party knowing that it will be in a dispute with that party for what may be a substantial portion of the period of performance. Moreover, consider the possible outcomes of such a dispute. Challenge procedures are often protracted and end in compromise settlements without a clear answer to the question of whether development was performed at private expense. If a contractor fails to meet its burden of proving development at private expense at the end of the process, and the restrictions were part of the basis for the award, that means:

1. the contract was based on faulty premises;
2. the contractor still got the contract; and
3. the Government had to abide by the erroneous restrictions until the final unappealed decision.

If a contracting officer decision invalidating asserted restrictions is ultimately sustained, the markings shall be cancelled, corrected, or ignore, and the Government may be able to get reimbursement for costs of reviewing and challenging the restrictions.[95] However, if the contractor's asserted restrictions are validated, the Government's data rights position has not improved despite the administrative burden of the validation process. However, the Government does gain certainty with respect to its data rights, which may be valuable for the program.

Further, if a contracting officer decision invalidating asserted restrictions is ultimately not sustained, the Government will be bound by the asserted restrictions.

If the challenge is found not to have been made in good faith, the contractor may be able to get reimbursement for certain litigation costs if the decision was appealed.[96]

Accordingly, a decision on whether to try to challenge is important but suspect asserted restrictions pre-award and the risk of holding up a necessary contract or postponing any challenge of restrictions to post-award is often a choice between a "rock and a hard place." The answer will be very fact dependent. Program and contracting officials should consult with legal counsel and technical requirements SMEs.

The importance of getting a contract awarded for both the Government and the contractor and the consequences of delaying must be weighed against continued uncertainty, inability to fully utilize data consistent with the Government's view of development funding history, possible protracted litigation, and loss of leverage post-award.

When planning competitive awards, it is wise to consider avoiding difficult choices by properly using IP as an evaluation factor to obtain necessary IP rights without the challenge procedures. When in already sole source situations, this tough choice may well be unavoidable. In such cases, it should be an informed and thoughtful choice documented in contracting and program

[95] *See* 7019, *supra* note 93, at (h); *see also* DFARS 252.227-7037(h) (2025).
[96] *Id.*

records to mitigate later confusion or recriminations over earlier decisions that have substantial and long-term consequences.

6.4. REVIEWING AND UPDATING THE IPS.

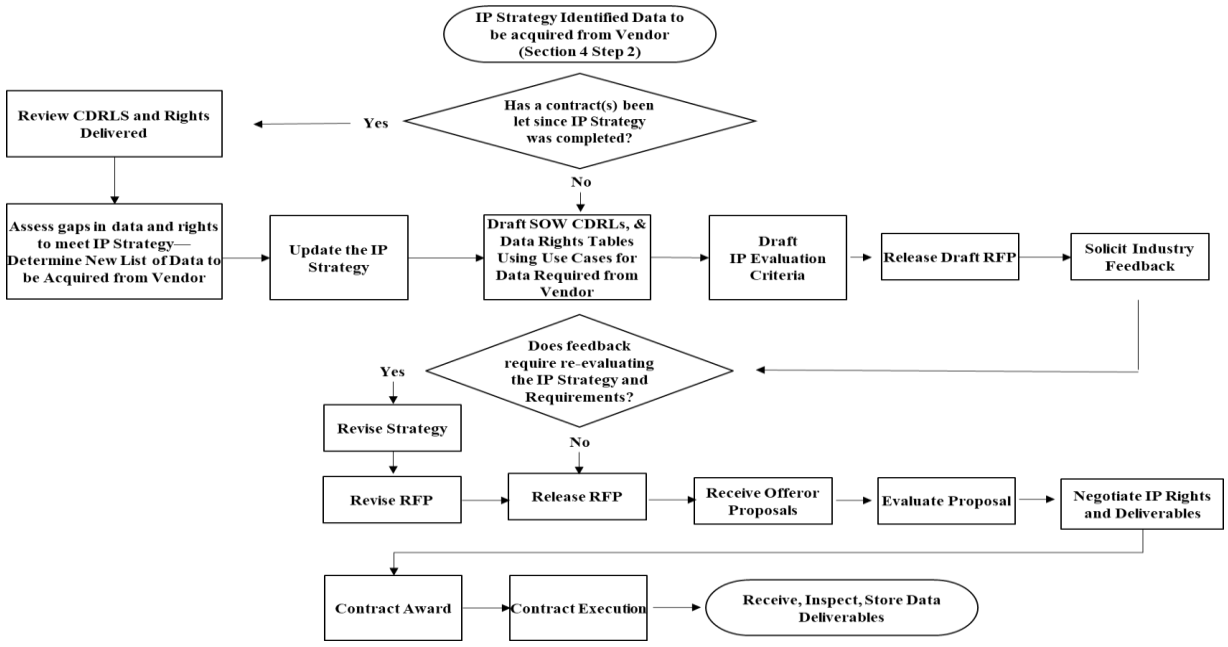
The IPS should be viewed as a living document and it should be reviewed and updated early and often over the course of the acquisition life cycle to reflect major program decisions, milestones, and direction, particularly when events and circumstances alter the assumptions in the strategy or produce results different from expected outcomes (e.g., IP negotiation does not produce the desired result). It should be continually referenced as a source of thorough program analysis to support decision making and mission objectives.

Events that may initiate reconsideration of an IPS can include:

- Receipt of data rights assertions contrary to expectations.
- Failure to receive and secure data deliveries in contract performance with expected rights.
- A change in mission or technical requirements that alters the needs for data and associated IP rights.
- Market changes that alter assumptions regarding the technical offerings or IP positions of prospective offerors in future contracts.
- Funding, appropriation, or other changes affecting a program that may alter ability or willingness to purchase data or IP rights.

Figure 2 represents the timing of IPS updates as they occur over the life cycle.

Figure 21. Implementing the IPS Through Contracts



SECTION 7: CONCLUSION

The effective management of IP is crucial for the DoD to maintain technological superiority and achieve its mission objectives. This guidebook outlined the fundamental concepts, strategies, and best practices for acquiring, managing, and utilizing IP within the DoD.

Key Takeaways:

- IP is critical to fostering innovation, competition, and collaboration with industry partners.
- The development of robust IP strategies ensures the DoD can secure the necessary data, CS, and rights to support its programs throughout their life cycle.
- Programs should continuously evaluate and adapt their IP strategies. As technology and market conditions evolve, so too must the DoD's approach to IP management. Regular reviews and updates to the IPS will help mitigate risks and capitalize on new opportunities.
- The successful implementation of IP strategies requires collaboration across various departments and stakeholders. By fostering a culture of communication and cooperation, the DoD can effectively leverage IP to enhance its capabilities and achieve its strategic goals.

In summary, the proactive and strategic management of IP is vital for the DoD's success. By adhering to the guidelines and best practices outlined in this guidebook, the DoD can navigate the complexities of IP management and secure a competitive advantage in the ever-evolving technological landscape.

SECTION 8: GLOSSARY

Term	Definition
Acquisition	The conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support (LS), modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions. Source: DAU Glossary
Acquisition Strategy (AS)	A business and technical management approach designed to achieve program objectives within the resource constraints imposed. It is the framework for planning, directing, contracting for, and managing a program. It provides a master schedule for research, development, test, production, fielding, modification, post-production management, and other activities essential for program success. The AS is the basis for formulating functional plans and strategies (e.g., Test and Evaluation Master Plan (TEMP), Acquisition Plan (AP), competition, Systems Engineering Plan (SEP), etc.). Source: DAU Glossary
Black Box	A system or process that takes inputs, performs a function, and generates outputs, but the inner operations of the system or process are unknown to the user.
Commercial	(1) Any item, other than real property, that is of a type customarily used by the general public or by non-governmental entities for purposes other than Governmental purposes, and— (i) Has been sold, leased, or licensed to the general public; or (ii) Has been offered for sale, lease, or license to the general public. *(abridged definition) Complete definition at* FAR Definitions
Competition	"An AS whereby more than one contractor is sought to bid on a service or function; the winner is selected based on criteria established by the activity for which the work is to be performed." Source: DAU Glossary
Competition in Contracting Act	1984 Federal law requiring the use of competition for Government acquisitions. Source: Federation of American Scientists (fas.org) presentation: Competition in Federal Contracting: An Overview of the Legal Requirements, DPAP Memo (27 Apr 11): Improving Competition in Defense Procurements - Amplifying Guidance
Computer Software (CS)	Information consisting of "…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. CS does not include computer databases or CSD." Sources: DFARS 227.72, 252.227-7013, -7014, -7015, and -7018
Computer Software Documentation (CSD)	"...owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the CS or provide instructions for using the software." Source: DFARS 252.227 - 7014
Configuration	The functional and physical characteristics of existing or planned hardware, firmware, software or a combination thereof, as detailed in requirements and technical documentation and ultimately achieved in a product. Source: MIL-STD-3046
Configuration Management (CM)	A process for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design and operational

Term	Definition
	information throughout its life. The five elements of Configuration Management and their descriptions are listed below. **Configuration Management Planning** - The planning and preparation for all CM activities to be performed for the program. **Configuration Identification** - The selection and identification of Configuration Items and the associated documentation and data that describes the item configuration. **Configuration Change Control** - The control of changes to the configuration of an item to assure that only beneficial changes are made, and that all associated documentation is also changed accordingly to reflect the actual item configuration change. **Configuration Audits** - Verification that the item meets its performance requirements and that the associated documentation and data matches the item configuration. **Configuration Status Accounting** - The historical record of the original product configuration and all approved changes that have occurred since. Source: MIL-HDBK-61A(SE) Configuration Management Guidance
Contract Clause	"Contract clause" or "clause" means a term or condition used in contracts or in both solicitations and contracts and applying after contract award or both before and after award. FAR 2.101 Definitions
Contract Data Requirements List (CDRL)	A list of contract data requirements using DD Form 1423 that are authorized for a specific acquisition and made a part of the contract. Source: DAU Glossary
Cooperative Research and Development Agreement (CRADA)	An agreement between one or more Federal laboratories and/or technical activities and one or more non-Federal parties. Under a CRADA, the Government laboratories and/or technical activities shall provide personnel, services, facilities, equipment, or other resources with or without reimbursement (but not funds to the non-Federal parties). CRADAs are instruments that may be used in all aspects of a product and/or system life cycle where RDT&E activities occur. The non-Federal parties shall provide funds, personnel, services, facilities, equipment, or other resources toward the conduct of specified R&D efforts that are consistent with the missions of the laboratory. The CRADA partners shall share in the IP developed under the effort. Source: DAU Glossary
Data	Recorded information, regardless of form or the media on which it may be recorded. The term includes TD and CS. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information. Source: FAR 52.227-14
Data Item Description (DID)	A completed document that defines the data required of a contractor. The document specifically defines the data content, format, and intended use. Source: MIL-STD-963
Defense Federal Acquisition Regulation Supplement (DFARS)	DoD supplement to FAR. Contains additional regulations specific to DoD acquisition needs. Source: D&DR Guide FAR and DFARS Overview
Federal Acquisition Regulation (FAR)	The principal set of rules governing Federal acquisitions of supplies and services. It contains 53 parts, and more than 1,800 pages of standardized policies and procedures used or referenced in federal contracts. Source: D&DR Guide FAR and DFARS Overview

Term	Definition
Form, Fit, and Function Data (FFF)	Information that describes "...the required overall physical, functional, and performance characteristics (along with the qualification requirements, if applicable) of an item, component, or process to the extent necessary to permit identification of physically and functionally interchangeable items." Sources: DFARS 252.227-7013, -7014, -7015, -7018
Framing Assumptions	Fundamental beliefs about program conditions that we expect to be true in the future. These are items that will cause program failure if they turn out to be false.
Intellectual Property (IP)	Information, products, or services that are protected by law as a type of intangible property, including data (e.g., TD and CS), technical know-how, inventions, creative works of expression, trade names.
IP Acquisition	IP in DoD acquisitions is critical for ensuring return on technology investment, promoting technical innovation, and enhancing competition, supportability, technical refresh, and affordability. Acquiring and licensing the appropriate IP is vital for ensuring the systems will remain functional, sustainable, upgradable and affordable.
IP Deliverables	Products or services (including information products and services) that are required to be delivered or provided to the USG by contract or another legal instrument and that include or embody IP (e.g., TD and CS).
IP Rights	The legal rights governing IP, including ownership as well as license or other authorization to engage in activities with IP (e.g., make, use, sell, import, reproduce, distribute, modify, prepare derivative works, release, disclose, perform, or display IP). When the IP involves access to classified information, DoD Directive 5535.02, DoDI 2000.03, and Volume 2 of DoDM 5220.22 may apply.
IP Strategy (IPS)	Strategy to identify and manage the full spectrum of IP (e.g., TD and CS deliverables, patented technologies, and appropriate license rights) from program inception and throughout the life cycle. The IPS will describe how program office will assess program needs for, and acquire competitively, when possible, IP deliverables and associated license rights needed for competitive, affordable acquisition and sustainment over the life cycle. The IPS is updated throughout the life cycle, summarized in the AS, and in the LCSP during the Operations and Support Phase. The PM is responsible for evaluating and implementing open systems architectures, where cost effective, and implementing a consistent IPS. This approach integrates technical requirements, contracting mechanisms, and legal considerations to support continuous multiple competitive alternatives throughout the life cycle. Source: DAU Glossary
TD necessary for Operation, Maintenance, Installation and Training Data (OMIT)	Information that is "necessary for installation, operation, maintenance, or training purposes (other than detailed manufacturing or process data)." Sources: DFARS 252.227-7013, -7014, -7015, and -7018

APPENDIX A: REFERENCES

Statutes

Statute Number	Statute Title	Link
10 U.S.C. § 3771	Rights in TD: Regulations	10 U.S.C. § 3771
10 U.S.C. § 3772	Rights in TD: Provisions Required in Contracts	10 U.S.C. § 3772
10 U.S.C. § 3774	Major Weapon Systems and Subsystems: Long-term TD Needs	10 U.S.C. § 3774
10 U.S.C. § 3781	TD: contractor justification for restrictions; review of restrictions	10 U.S.C. § 3781
10 U.S.C. § 3791	Management of IP Matters Within the DoD	10 U.S.C. § 3791
10 U.S.C. § 1707	Cadre of IP experts	10 U.S.C. § 1707
10 U.S.C. § 2464	Core Logistics Capabilities	10 U.S.C. § 2464
10 U.S.C. § 4211	AS	10 U.S.C. § 4211
10 U.S.C. § 4324	Life Cycle Management and PS	10 U.S.C. § 4324
10 U.S.C. § 4236	Negotiation of price for TD before development, production, or sustainment of major weapon systems	10 U.S.C. § 4236
10 U.S.C. § 4401	Requirement for MOSA in major defense acquisition programs; definitions	10 U.S.C. § 4401
10 U.S.C. § 4576	Requirement for consideration of certain matters during acquisition of noncommercial CS	10 U.S.C. § 4576
35 U.S.C. §§ 201-204	Bayh-Dole Act	35 U.S.C. §§ 201-204

Policy and Regulations

Policy or Regulation Number	Description	Link
DoDI 5010.44	IP Acquisition and Licensing. Establishes policy, assigns responsibilities, and prescribes procedures for the acquisition, licensing, and management of IP	DoDI 5010.44
DoDM 5010.12-M	Procedures for the Acquisition and management of TD	DoDM 5010.12-M
DFARS 252.227-7013	Rights in TD - Other Than Commercial Products and Commercial Services	DFARS 252.227-7013
DFARS 252.227-7014	Rights in Other Than Commercial CS and Other Than Commercial CSD	DFARS 252.227-7014
DFARS 252.227-7015	TD – Commercial Products and Commercial Services	DFARS 252.227-7015

DFARS 227.7202-1, -3, and -4	Commercial CS and Commercial CSD. No specific clause prescribed, policy prefers use of commercial license, adapted by negotiation if/as necessary	227.7202-1 227.7202-3 227.7202-4
DFARS 252.227-7018	Rights in Other Than Commercial TD and CS—Small Business Innovation Research Program and Small Business Technology Transfer Program	DFARS 252.227-7018
DFARS 252.227-7104	Contracts Under the Small Business Innovation Research Program and Small Business Technology Transfer Program	DFARS 252.227-7104
DFARS 252.227-2017	Identification and Assertion of Use, Release, or Disclosure Restrictions	DFARS 252.227-2017
DFARS 252.227-7019	Validation of Asserted Restrictions – CS	DFARS 252.227-7019
DFARS 252.227-7037	Validation of Asserted Restrictions on TD	DFARS 252.227-7037
DFARS 252.227-7026	Deferred Delivery of TD or CS	DFARS 252.227-7026
DFARS 252.227-7027	Deferred Ordering of TD or CS	DFARS 252.227-7027

Regulatory Reform

DFARS Case	Description & Status	Links
DFARS 2019-D069, Validation of Proprietary and TD	Streamlined Challenges/Validation for Commercial Tech Data – Final Rule	DFARS Case No. 2019-D069
DFARS 2018-D018, Noncommercial CS	Ensuring Needed Software Delivery During Program Life Cycle – Final Rule	DFARS Case No. 2018-D018
DFARS 2021-D005, MOSAs	Enabling MOSA – Proposed Rule	DFARS Case No. 2021-D005
DFARS 2019-D044, Rights in TD	Enhanced Deferred Ordering for Tech Data & Software – Proposed Rule	DFARS Case No. 2019-D044
DFARS 2019-D043, Small Business Innovation Research Program Data Rights	Full Implementation SBIR/STTR Data Rights Policy Updates – Final Rule	DFARS Case No. 2019-D043
DFARS 2018-D071, Negotiation of Price for TD and Preference for SNLs	Flexible, tailored, business-case supported Negotiations for IP – Proposed Rule	DFARS Case No. 2018-D071
DFARS 2022-D016, Update of Challenge Period for Validation of Asserted Restrictions on TD and CS	Doubling the Challenge Period (from 3 to 6 years) for DR Validations – Final Rule (awaiting publication)	DFARS Case No. 2022-D016

Key References

Reference	Description	Link
DoD Other Transactions Guide	Introduces all three OTAs (research, prototype, and production) and strategy for planning, execution, and administration of them.	DoD Other Transactions Guide
DoD MOSA Implementation Guidebook	Provides comprehensive guidance on implementing MOSA principles across the DoD acquisition life cycle. It emphasizes using modular design, open standards, and widely supported interfaces to develop and acquire affordable, adaptable, and evolvable systems.	DoD MOSA Implementation Guidebook
Sec. 813 Report	Government-Industry advisory panel on TD rights, (Nov 2018)	Sec. 813 Report
Sec. 875 Report	DoD access to IP for weapon systems sustainment, (May 2017)	Sec. 875 Report
DoD Response to Sec. 813 & 875 Reports from USD(A&S)	Response to Sec. 813 & 875 Reports from USD(A&S), (Feb 2019)	USD(A&S) Response to Sec. 813 & 875
Sec. 801 Report FY20	First Annual Report to Congress on Pilot Program on IP Evaluation for Acquisition Programs Section 801 of FY20 NDAA (March 2021)	First Annual Sec. 801 Report
Sec. 801 Report FY21	Second Annual Report to Congress on Pilot Program on IP Evaluation for Acquisition Programs Section 801 of FY20 NDAA (Feb 2022)	Second Annual Sec. 801 Report
Sec. 801 Report FY22	Third Annual Report to Congress on Pilot Program on IP Evaluation for Acquisition Programs Section 801 of FY20 NDAA (Nov 2022)	Third Annual Sec. 801 Report
Sec. 801 Report FY23	Fourth Annual Report to Congress on Pilot Program on IP Evaluation for Acquisition Programs Section 801 of FY20 NDAA (Nov 2023)	Fourth Annual Sec. 801 Report
Additional Congressional Reports	Significant IP & Sustainment-planning content in both DoD Reports to the White House Competition Council, required by Section 5 of Executive Order 14036, Promoting Competition in the American Economy (09 Jul 2021)	"State of Competition within the Defense Industrial Base" (15 Feb 2022) "DoD Life cycle Sustainment Efforts in Support of Organic Repair" (25 June 2023)
OSD IP Cadre Website	Provides the focus and structure of the OSD IP Cadre as well as additional inks and references relevant to IP in DoD acquisitions.	IP Cadre Website

APPENDIX B: TOOLS AND RESOURCES

Tools and Resources	Web Link
▪ Foundational IP Credential	▪ https://www.dau.edu/credentials/cacq-008
▪ The IP & Data Rights (DR) Community of Practice	▪ https://www.dau.edu/cop/IPDR
▪ DAU IPDR CoP Sub-Page: The IP Cadre	▪ https://media.dau.edu/channel/Contracting/62925211
▪ Online DAU Training Videos	▪ https://www.dau.edu/cop/IPDR/Pages/Topics/IPDR-Cadre.aspx
▪ DFARS Procedures, Guidance and Information (PGI)	▪ https://www.ecfr.gov/
▪ Life Cycle PS Planning: IP for PS Toolkit	▪ https://www.dau.edu/tools/intellectual-property-ip-product-support-ps-toolkit
▪ OSD IP Cadre Website	▪ https://www.acq.osd.mil/asda/dpc/api/ip-cadre.html
▪ LCSP Version 3.0, Figure 2-2: PSS for Reference Design Concept	▪ https://www.dau.edu/sites/default/files/Migrated/ToolAttachments/LCSP%20Outline%20Version%203.0%2013_October_2022%20v1.pdf
▪ IP: Navigating Through Commercial Waters (This guidebook replaces and supersedes "Navigating Through Commercial Waters")	▪ https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Intellectual%20Property-Navigating%20through%20Commercial%20Waters.PDF