Army Materiel Command

Army Guide for the Preparation of a Program Product Data Management Strategy (DMS)

8/31/2010

UNITED STATES ARMY
PRODUCT DATA & ENGINEERING
WORKING GROUP

DISTRIBUTION STATEMENT D. Distribution authorized to Department of Defense (DoD) and U.S. DoD contractors only. Administrative or Operational, 31 August 2010. Other requests may be referred to the **Headquarters, Army Materiel Command (AMCIO),** 9301 Chapek Road, Building 1, Fort Belvoir, VA 22060-5527

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Requirement for DMS 1
2 DMS Process 4
2.1 Step 1 - Data & Data Rights Determination 5
2.2 Step 2 - Data & Data Rights Acquisition 11
2.3 Step 3 - Data Management & Use 16
3 Data Management Strategy and the Life cycle 19
4 Data Management Strategy (DMS) Template 27
Appendices 32

Appendices

Appendix A - Program Life cycle Data Requirements A-1
Appendix B - Government Data Rights Procedures Background Information B-1
Appendix C - DFARS Contract Clauses for Data Rights C-1
Appendix D - Data Formats D-1
Appendix E - Data Delivery E-1
Appendix F - Data Storage and Maintenance F-1
Appendix G - Life cycle Access and Use of Data G-1
Appendix H - Required Resources and Risk Assessment H-1
Appendix I - DMS Worksheet Tool I-1
Appendix J - Acronyms J-1

List of Figures

Figure 1 - Data Management Strategy Development Process 3
Figure 2 - Complete DMS Creation Process 4
Figure 3 - Hierarchical Breakdown of Product Data 6
Figure 4 - Work Breakdown Structure (WBS) Levels of DMS Attention 12
Figure 5a - Noncommercial Technical Data Rights 13
Figure 5b - Noncommercial Software Rights 14

Figure 5c - Commercial Technical Data Rights 14
Figure 6 - Acquisition Life cycle and Data Management Reviews 20
Figure 7 - Relationships of Different Types of Data A-3
Figure 8 - Components of DMS Development I-2
Figure 9 - Data Rights Tool Introduction I-3
Figure 10 - Data Life cycle Management Tool Introduction I-4

1 INTRODUCTION

1.1 Purpose

This document provides the Program Manager (PM) and others involved in the acquisition and support of Army hardware and software, guidance in the proper preparation of a program-specific Data Management Strategy (DMS). In preparing the DMS, Congressional and Department of Defense (DoD) policy states the PM shall evaluate and plan for the long-term needs for product data necessary to develop, acquire, manufacture, operate, support, maintain and dispose of their acquisition program; and the appropriate data rights required to assure the Government can utilize the data to the maximum legal extent. An Excel spreadsheet support tool has also been developed to be used in conjunction with this guide as a "worksheet" for analyzing the data and data rights requirements of the total acquisition program and its major subsystems/components.

1.2 Requirement for DMS

The requirement to prepare program Data Management Strategies originated in Office of the Secretary of Defense (OSD) Policy Memo, "Data Management and Technical Data Rights", dated 19 July 2007. It has since been codified in the 8 December 2008 version of DoDI 5000.02, Enclosure 12, section 9, and in Department of Army Policy Memo, "Data Management and Technical Data Rights", dated 1 April 2008, and was reaffirmed in DA Memo, "Data Management, Technical Data Rights, and Competition", dated 8 January 2010.

These policy documents require ACAT I and II PMs to:

- assess the data required to design, manufacture, and sustain the system,
- assess the data required to support re-competition for production, sustainment or upgrade,
- prepare a DMS.

Historically product support or acquisition program operating sustainment costs are approximately 70% of the total ownership cost of the system over its entire "cradle to grave" lifecycle. Lack of technical data significantly impedes the Army's ability to maximize competition for both acquisition and sustainment of the acquisition program. It also severely impacts the government enterprise's ability to properly plan and execute effective and efficient sustainment strategies. This has led to the government's inability to reduce total ownership costs throughout its life cycle. Hence the value of the technical data across the government enterprise is critical for meeting key operating and sustainment Warfighter requirements.

To ensure maximum availability of competitive acquisition and product support alternatives throughout the life cycle of a system or component, PMs must make certain that all necessary product data and associated data rights are acquired at logical points in the life cycle process and are maintained for future use.

ACAT III PMs are not required to prepare DMSs for their programs, but are strongly encouraged to do so as it reflects a "best practice" for ensuring the Government understands what data, and associated

rights, are necessary to support the acquisition program throughout its life cycle. These same DMS issues arise in other common program documents such as a Justification and Approval (J&A).

The PM has primary responsibility for development and implementation of the DMS, but is encouraged to utilize a working level DMS Integrated Product/Process Team (IPT) to determine the long-term product data requirements of all functional areas that have roles in the weapon system life cycle. The DMS IPT should consist of personnel from the PM office, the associated Life Cycle Management Command (LCMC), associated Research, Development & Engineering Centers (RDECs), associated Software Engineering Centers, depots and other organizations as appropriate. A representative list of functional areas that should be represented in the DMS IPT include: engineering, logistics, environmental, Environmental Safety and Occupational Health (ESOH), contracting, legal, quality assurance, program management, and data management.

The DMS is to be integrated with the program Acquisition Strategy (AS), (or Technology Development Strategy (TDS) during the Materiel Solution Analysis phase), the Supportability Strategy (SS) (also referred to as the Life Cycle Sustainment Plan (LCSP)), the System Engineering Plan (SEP) and other program documents. Leveraging these program strategies, the PM and DMS IPT should use this guide and the companion DMS Worksheet (or equivalent) to conduct the detailed data, data rights, and data management analysis that will be synopsized in the DMS and submitted or updated for each Milestone Decision Review (MDR). Each DMS should be reviewed and approved by the same key program stakeholders that review and approve the AS and SS. DA Pamphlet 70-3 provides a list of these AS & SS stakeholders.

Figure 1 is a graphical depiction of the Data Management Strategy development process described above.

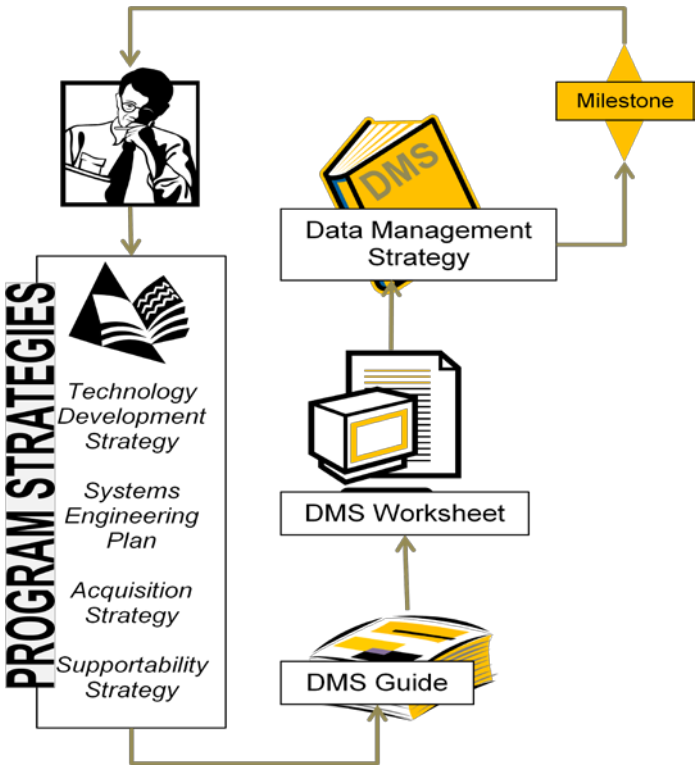


Figure 1 - Data Management Strategy Development Process

2 DMS PROCESS

Preparing a "good" DMS requires the PM and their staff to conduct a three step analysis.

Step 1 – Determination of the program's life cycle data requirements and associated data rights requirements.

Step 2 – Determination of the contractual actions (contract clauses, Contract Data Requirements Lists (CDRLs), Data Item Descriptions (DIDs), negotiations, contractor assertions, etc.) needed to acquire the above data and data rights from contractors.

Step 3 - Determination of the Information Technology (IT) repositories/environment, access controls, and configuration management actions that must be funded over the acquisition life cycle to manage the data and enable the various authorized Army users to access and use the data for product support purposes.

Figure 2 below graphically depicts and summarizes this three step process. The remainder of this section provides detailed guidance needed to accomplish these three steps.

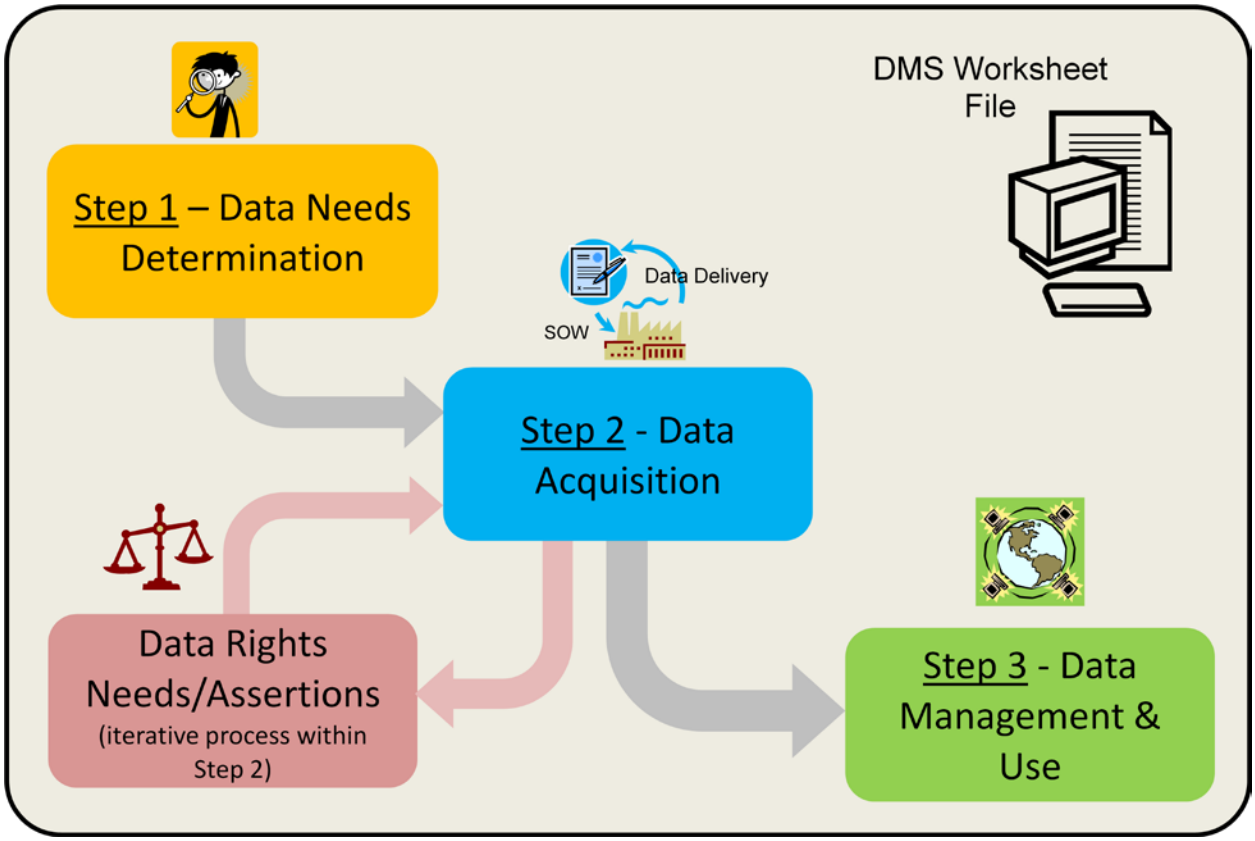


Figure 2 - Complete DMS Creation Process

2.1 Step 1 - Data & Data Rights Determination

Determination of the program's life cycle needs for data and data rights is dependent upon the program's Technology Development Strategy or Acquisition Strategy, Supportability Strategy, and the program System Engineering Plan. The TDS and SEP are usually generated prior to Milestone A, and the AS and SS are usually generated prior to Milestone B (see DoDI 5000.02, Enclosure 4, "Statutory and Regulatory Information and Milestone Requirements"). In all cases the program's plans for organic, sole source or competitive sourcing for life cycle functions and services will be a primary driver for determining the data and data rights required, so the DMS must be consistent with and support these other program management documents.

Life cycle functions can be divided into the basic categories of development, production, procurement, and sustainment. Since the Office of Management and Budget (OMB), Congress, and OSD have all called for increased use of competitive acquisition and logistics support approaches, the product data required for competition should be a primary (but not the sole) driver of data and data rights needs. The TDS or AS, SEP, and SS will describe which organization (organic Government, Original Equipment Manufacturer (OEM), or other contractor) is planned to perform those functions. Government organizational performance of life cycle functions should be further segregated such that the PM understands which specific organizations will have needs for weapon system product data and hence should be participants on the DMS IPT. Table 1 is a representational example of the type of life cycle function allocation between organizations that could exist for a hypothetical weapon system.

Table 1 – Representational Allocation of Life cycle Function Responsibilities

	Lifecycle Functions										
Organizations	Program Mgmt	Systems Engineering	Test	Integration	Provisioning	Inventory Mgmt	Contracting	Production	Sustainment Eng	Maint / Repair	Demil / Disposal
PM Office	X	X	X	X	X	X	X		X		X
OEM	X	X	X	X	X						
RDEC		X	X	X	X				X		
LCMC	X	X	X	X	X	X			X	X	X
ACC							X				
ATEC		X	X								
Prod Contractor								X			
Arsenal / Depot		X	X	X		X	X	X		X	
DLA					X	X	X				
Field Maintainers			X							X	
Log Supt Contractor										X	
Software Eng Center		X	X	X			X		X	X	

Acronyms:
ACC = Army Contracting Command
ATEC = Army Test & Evaluation Command
DLA = Defense Logistics Agency
LCMC = Life Cycle Management Command
LOGSA = U.S. AMC Logistics Support Activity
OEM = Original Equipment Manufacturer
PM = Program/Project Management
RDEC = Research, Development & Engineering Center

2.1.1 Data Categories / Definitions

The universe of product related data needed by the various organizations to support the weapon system throughout its life cycle can be categorized into the following three major groups: Product Definition Information, Product Operational Information, and Associated Information. Figure 3 is a graphical representation of the categories of product data as defined by the Army Product Data and Engineering Work Group (PEWG).

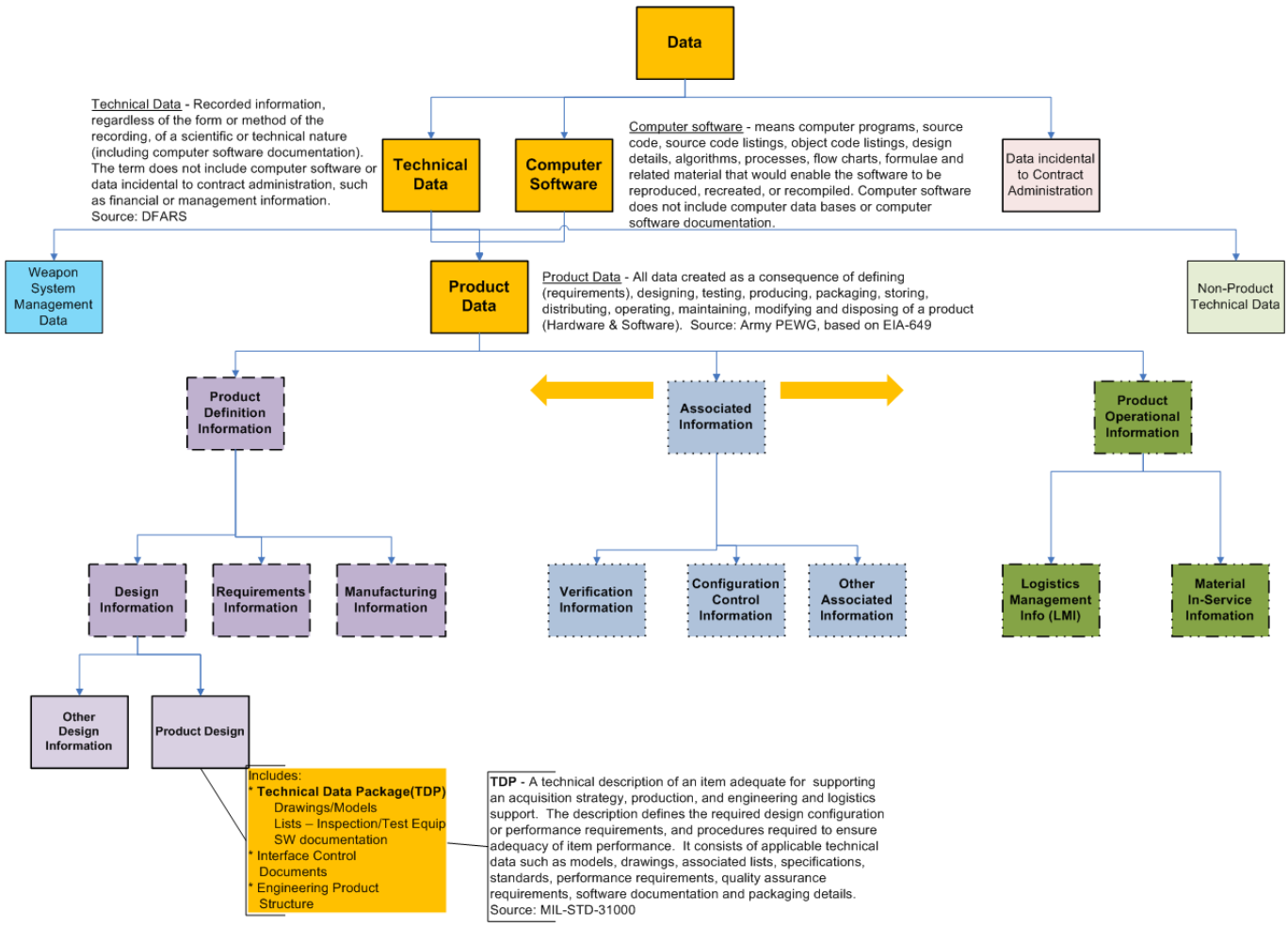


Figure 3 - Hierarchical Breakdown of Product Data

The definitions of the three major categories of product data are below:

- ***Product Definition Information*** – information that defines the product's requirements, documents the product's design and attributes, and is the authoritative source for configuration definition and control. Examples include: drawings, specifications, 3-D CAD models, analyses, trade studies, and information about designs not selected, requirements, manufacturing and depot overhaul/modification information.

- ***Product Operational Information*** – information that describes the operation and logistics support/sustainment of the weapon system. Examples include: field feedback information, records of maintenance actions, field deficiency reports, etc.), product identification information, technical manuals, ESOH/Hazardous Material information, and packaging, preservation, and transportation information.

- ***Associated Information*** – other product related data such as test results and proposed configuration changes that do not fit clearly into the other two categories

It is important to note that the types of product related data needed to support the weapon system throughout the life cycle extend beyond just the Technical Data Package (TDP). All elements of product data depicted in Figure 3 should be considered for their utility and need for each subsystem and major subcomponent of the weapon system.

Also note that computer software is included in Figure 3 as data to be considered and planned for in the program DMS. The Defense Federal Acquisition Regulation Supplement (DFARS) defines computer software as: computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer data bases or computer software documentation. While the DFARS segregates Computer Software and Technical Data as different entities, data rights are an important issue common to both.

The first step of the DMS analysis is for the PM and the DMS IPT to identify which elements of product data and computer software are needed by each organization to accomplish their mission functions. The "Data Management Sheet" tab of the DMS Excel support tool provides a checklist of product data elements to be considered in this step of the analysis.

More information about the categories and elements of product data is contained in Appendix A - Program Life cycle Data Requirements.

2.1.2 Data Rights Needs and Options

Any product data that is intended to be used by other than the Original Equipment Manufacturer (OEM) will require sufficient rights for Government or other use, so an assessment of required level of data rights for each set of product data must also be conducted. The options for data rights in noncommercial technical data and noncommercial computer software as defined within the DFARS are:

- Unlimited Rights
- Government Purpose Rights
- Limited Rights (or Restricted Rights for Non-commercial Computer Software)
- Special License Rights

When discussing the subject of Government data rights it must be remembered that the U.S. Government is entitled to certain automatic and default rights because of statute or regulation. In these cases the Government "secures" these rights. If the Government requires data rights beyond these entitlements, then the Government can attempt to "acquire" the additional rights through negotiations and possible additional cost. While recognizing this important distinction, the single term "acquire" is

used relative to data rights throughout the rest of this guide. Information about the DFARS treatment of automatic and default rights, commercial technical data, and commercial computer software is contained in Appendix B - Government Data Rights Procedures Background Information.

2.1.2.a Unlimited Rights (UR) in Technical Data and Computer Software

"Unlimited Rights" arise in certain types of data automatically upon contract award (e.g., Form, Fit, and Function (FFF) and installation, operation, maintenance, and training (IOMT)) and in most other data based upon exclusive (100%) Federal funding of development of the items, components, or processes (ICP) to which that data pertains. The Government may share this data with anyone for any reason.

2.1.2.b Government Purpose Rights (GPR) in Noncommercial Technical Data and Computer Software

If the Government provides some, but not 100% of the funding for the item, component, or process, then the Government receives by default a "Government Purpose Rights" license in all data pertaining to that ICP except that data in which it has received automatic Unlimited Rights. If neither party (Government or OEM contractor) proves exclusive (100%) funding then "Government Purpose Rights" are the default. The Government may share this data with third parties for any Government purpose after having that third party execute a DFARS Non-Disclosure Agreement (NDA).

2.1.2.c Limited Rights (LR) in Noncommercial Technical Data

When the contractor has exclusively (100%) funded the development of a non-commercial ICP, the Government receives "Limited Rights" in the data for which the Government has not received automatic "Unlimited Rights." With one exception for emergency repairs and overhaul, the Government may not share this data with third parties (to include support contractors).

2.1.2.d Restricted Rights (RR) in Noncommercial Computer Software

When the contractor has exclusively (100%) funded the development of non-commercial computer software, the Government receives "Restricted Rights" in that computer software for which the Government has not received automatic "Unlimited Rights." With very limited exceptions listed in the DFARS, the Government may not share this data with third parties (to include support contractors).

2.1.2.e Special License Rights (SLR) in Technical Data and Computer Software

Where the above DFARS defined categories are insufficient to properly define an agreement of the parties as to data rights allocations, the parties may specifically negotiate "Special License Rights" that are defined in the contract. The Government may always attempt to increase its rights by negotiation (without coercion) to "Government Purpose Rights", "Unlimited Rights" or even ownership rights. Always consult legal counsel when negotiating licenses.

2.1.3 Myths and Facts regarding Government Data Rights

The area of Government data rights is probably one of the most misunderstood areas within acquisition. Several key "myths and misconceptions" about Government data rights are listed in Table 2 below. Please see Appendix B – Government Data Rights Procedures Background Information for specifics related to the following "myths and misconceptions".

Table 2 -Myths and Facts about Data Rights

Myths	*Facts*
The Government must "own" the technical data in order to use it.	With few exceptions, the Government does not own data. The Government merely takes a license in the data that allows us certain use and release rights.
All technical data is costly and separate from the cost of acquisition program development.	The costs to acquire data required by a contract and certain standard license rights are priced into the cost of that contract. The only legitimate additional costs are for Government-unique media, reproduction and marking (distribution statements, export control, etc.) delivery requirements or to acquire "additional" rights in data that may be necessary or desirable. The Government "automatically" takes unlimited rights in certain categories of technical data (commercial and noncommercial) and in noncommercial computer software regardless of funding source. These categories of data include: Form, Fit, and Function (FFF); installation, operation, maintenance, and training (IOMT); computer software documentation and a few others.
All technical data is costly and separate from the cost of acquisition program development. (cont.)	Other rights in noncommercial technical data and noncommercial computer software are apportioned between the contractor and the Government according to who paid to develop the item, component, or process to which the technical data pertains, or the software.
Performance-based acquisition negates the need for technical data	While a performance specification may be the starting point for a system design, once the Government has paid for the system design and development, failure to secure the technical data effectively cedes much control of the system to the contractor. From a rights standpoint, if the Government is to establish and confirm its "automatic," "default," and "additional" rights in data, that data must always be scheduled for formal delivery regardless of performance based requirements. In addition, all such technical data (in the Government's possession) is available for use by third parties for emergency repairs and overhauls. From a logistics standpoint, design control efficiently maintains system qualification. Also, having detailed design data eliminates repair part proliferation: i.e., constrains the logistics footprint.

Myths	*Facts*
The contractor "said" the data was proprietary and too expensive	Generally speaking, the contractor must assert and be able to justify the data it claims as protected prior to each contract award. They also must make these assertions at the proper level of the product (top weapon system, subsystem, assembly, or component). The contractor has the burden of proving all assertions by maintaining and providing records showing funding allocations.
The data must be proprietary because it all had "proprietary" stamped on each page or file	Legends such as "PROPRIETARY" or "COMPANY CONFIDENTIAL" are nonconforming legends for data pertaining to a noncommercial ICP/software and should be ordered removed. Legends for which a proper assertion has not been made and incorporated into the contract also are "nonconforming." Upon receipt, all delivered data must be screened/sampled for nonconforming or unjustified markings and for conformance to other contract requirements and corrections required promptly. This is why "delivery" of the technical data is always recommended! Data should not be accepted prior to correction of technical and data rights defects. Doing so may waive Government rights.
The contractor modified some of the technical data we provided to them and now claim it is proprietary.	The Government has data rights in "corrections and changes" to Government Furnished Information (GFI) technical data or software provided to a contractor as Government Furnished Information (GFI), and retains its original rights in GFI. However, Government rights in "corrections and changes" in GFI that result from modification of an ICP or new development efforts may not be so straight forward.
Technical data "access" is sufficient	Mere access does not confirm rights! Formal delivery via CDRL is required to confirm Government rights and obtain correct markings on the data. By law, any enforceable right to see, access, or have a copy of data requires an OMB approved DID or FAR/DFARS Clause. By contract terms, only "deliverable" data is subject to the DFARS Part 227 clauses requiring assertions, markings, and justifications. Therefore, DoD cannot assume it has any useable rights in data that is informally provided unless such rights are explicitly granted by the contractor and reviewed by legal counsel. All data access provisions must be reviewed by counsel and the data rights in accessed information must be addressed in the contract.

Myths	*Facts*
The Government should only "buy" rights to technical data it has a current defined need for.	The Government should always aggressively pursue its "automatic" and "default" rights to certain technical data, as well as the other rights to which it is entitled at no additional cost. Since additional needs for the data may surface at a later time, there is no supportable rationale for "giving up" these rights to which the Government is legally entitled.
The Government agreed in the past to restrict its rights in the technical data and software.	These agreements should not be considered binding upon the Government's prior or future data rights until reviewed by legal counsel.

The result of the analysis will be an understanding of what product data (and associated rights) you need and why you need it. In nearly every case the Government's needs for using the product data can be met with Government Purpose Rights. The full analysis should be documented in the "Data Rights Sheet" tab of the DMS Excel support tool or something similar, and key results should be summarized and recorded in the DMS for Milestone Decision makers.

More information about the Government's data rights options and procedures can be found in Appendix B - Government Data Rights Procedures and Background Information.

2.2 Step 2 - Data & Data Rights Acquisition

Once the PM has completed the identification of the required product data and associated data rights needed to support the acquisition program throughout its life cycle, the next step is to identify actions to be taken to acquire the needed data and data rights. Generally recommended actions include:

- Use appropriate DFARS specified contract clauses (see Appendix C – DFARS Contract Clauses for Data Rights for a list of the clauses and types of contracts they should be used in)
- Determine the desired format for each set of product data ordered via contract. Information on data formats is located in Appendix D - Data Formats.
- Specify all requested data in the contract via the Contract Data Requirements List (CDRL) and appropriate Data Item Descriptions (DIDs)
- Require contractor to assert any intention to provide data with less than Unlimited Rights at time of proposal submission (this is automatically required in any contract containing DFARS 252.227-7017)
- Require documentation from the contractor to support all assertions
- Negotiate (if needed) to acquire additional data rights
- Reach agreement on all data costs and data rights by time of contract award
- Deliver to the Government of all contractually ordered data so it can be reviewed to determine compliance with contract requirements for data quality and data rights markings. Information on data delivery and verification can be found in Appendix E - Data Delivery.

Again, the "Data Management Sheet" tab of the DMS Excel support tool provides a place to document the program's plans for many of these data acquisition decisions.

2.2.1 Data Rights Assertions

DFARS 252.227-7017 requires that, as part of their proposal, contractors provide assertions regarding any data identified in the Government's Solicitation in which the contractor asserts the Government should take less than Unlimited Rights. These assertions should be identified at the appropriate Work Breakdown Structure (WBS) level (top system, subsystem, assembly, or component) and substantiated as appropriate. Figure 4 below shows a notional WBS for a generic acquisition program. The WBS provides a framework for specifying program objectives. It defines the program in terms of hierarchically related, product-oriented elements and includes "other Government" elements (i.e., Program Office Operations, Manpower, Government Furnished Equipment (GFE), and Government Testing). Each element provides logical summary levels for assessing technical accomplishments, supporting the required event-based technical reviews, and measuring cost and schedule performance. Usually the Government develops the top three levels of the Program WBS and includes it in the solicitation. Bidding contractors build upon the Government program WBS and propose detailed WBS structures (known as Contract WBS) based on their development approach. The winning contractor's Contract WBS together with the Government's Program WBS becomes the complete WBS for the acquisition program. MIL-HDBK-881A "Work Breakdown Structures for Defense Materiel Items" provides more information about the proper development and uses of WBSs.

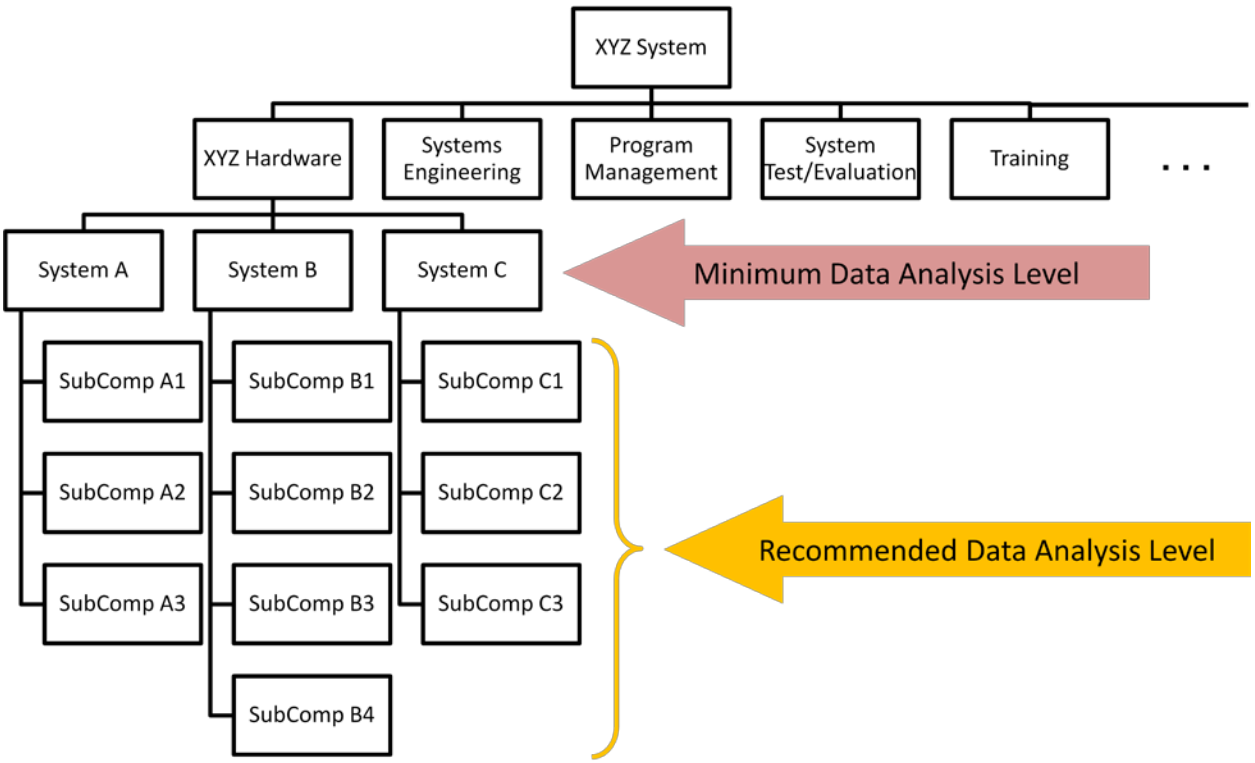


Figure 4 - Work Breakdown Structure (WBS) Levels of DMS Attention

When evaluating OEM assertions of limitations on Government rights, the Government must compare the contractor claims against the guidance contained in the DFARS. Figures 5a, 5b, and 5c below visually demonstrate the relationship between the Government's license rights levels and certain categories of data. The initial DMS assumption as to existing and future data rights should be based upon the categories, levels and relationship shown in these figures. Refer to Appendix C – DFARS Contract Clauses for Data Rights for a better understanding of the DFARS clauses called out in the following figures.

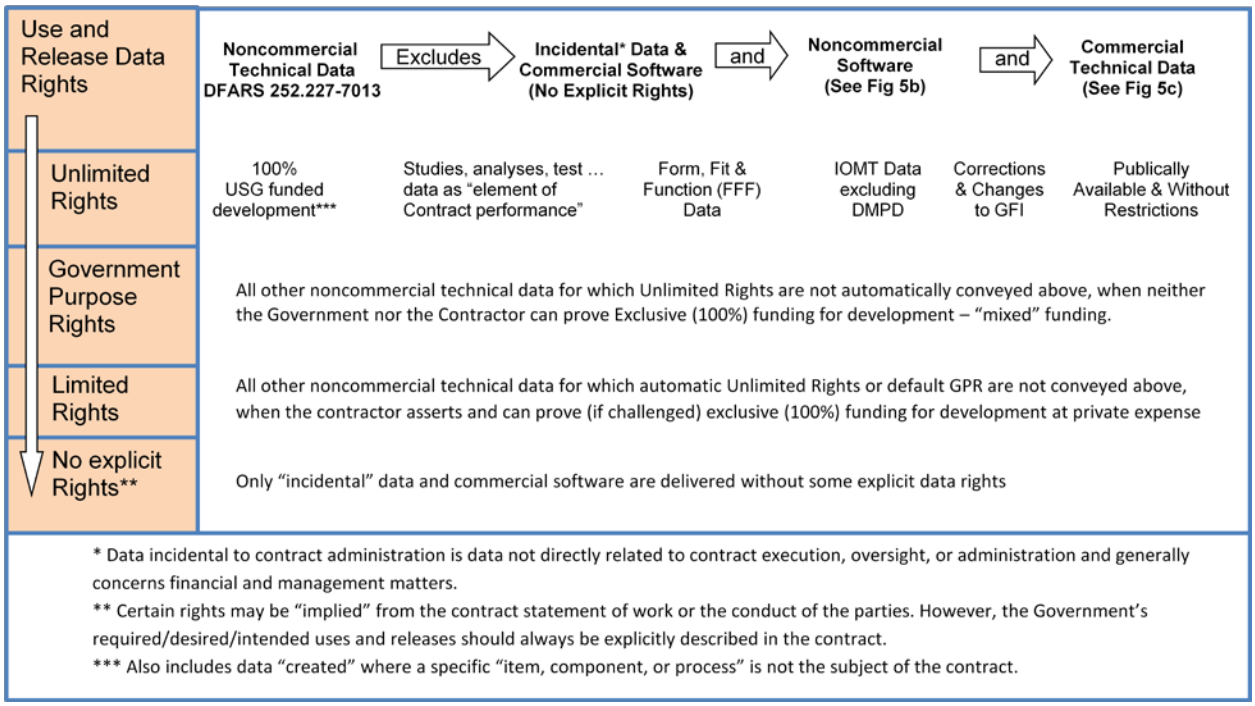


Figure 5a - Noncommercial Technical Data Rights

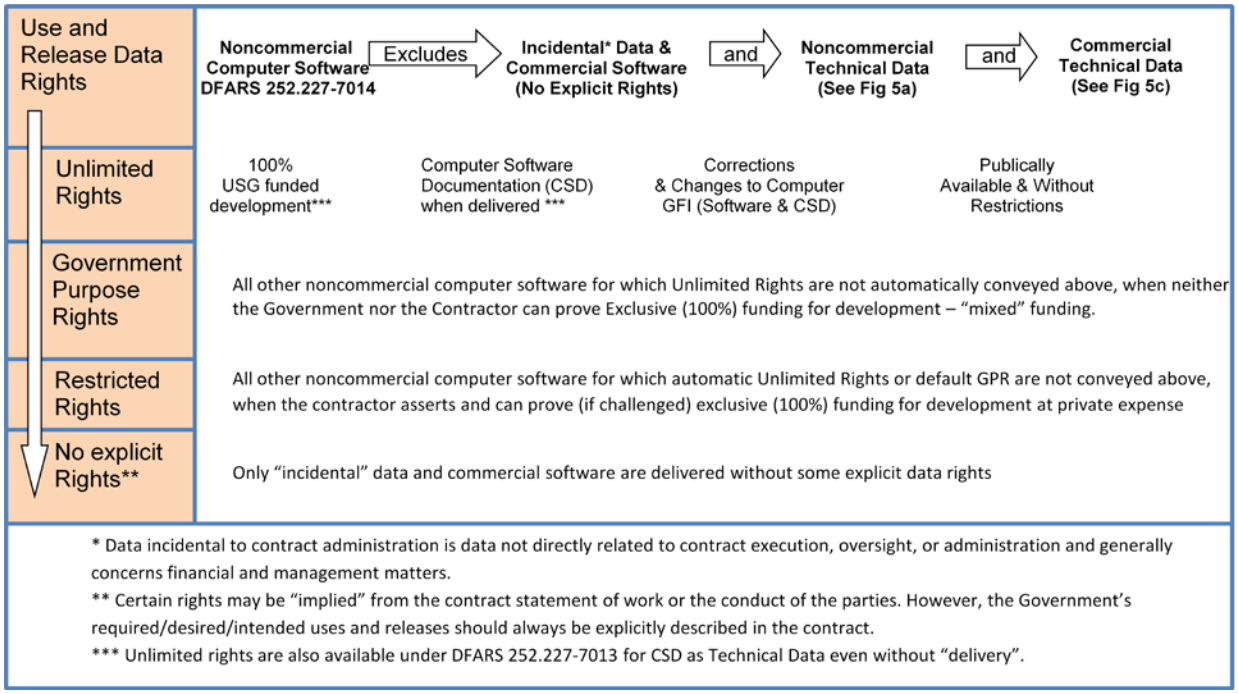


Figure 5b - Noncommercial Software Rights

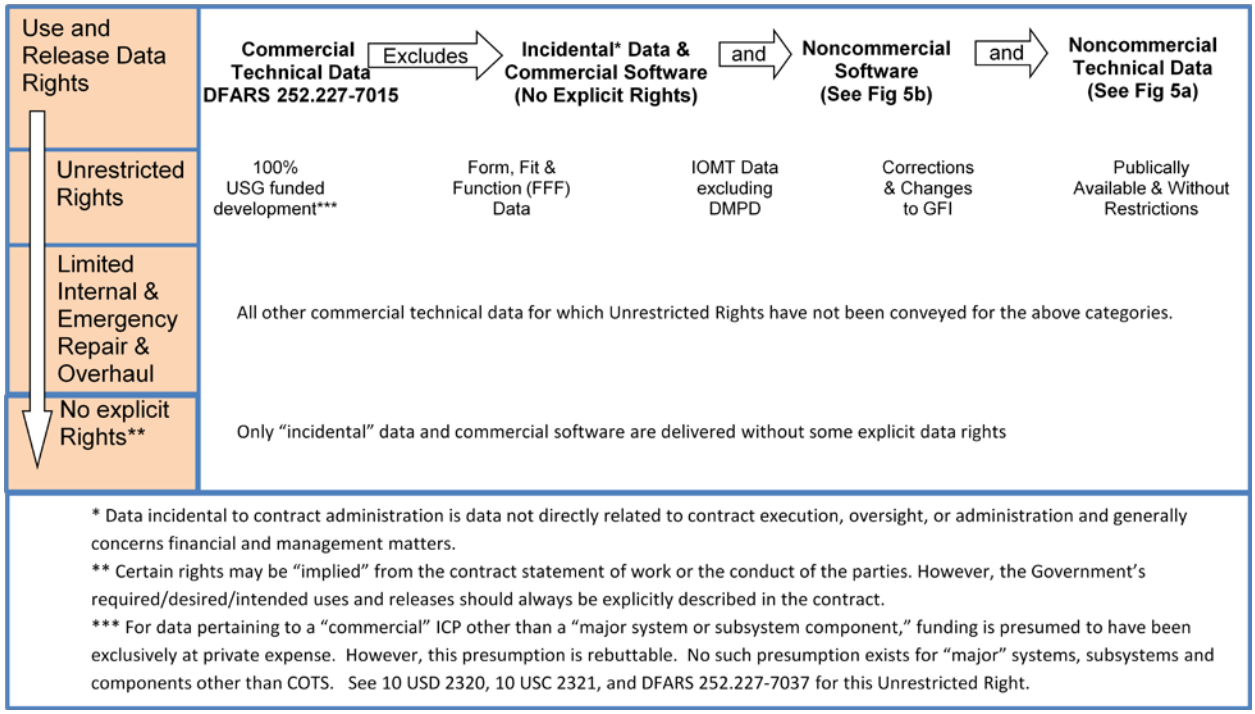


Figure 5c - Commercial Technical Data Rights

If the contractor's assertions are determined to be valid, then the Government must compare those limited rights usages to the data rights and planned usages determined in Step 1 to identify any gaps between what is required and what the Government is legally entitled to at no additional cost.

For each gap identified, appropriate actions must be planned to close the gap. Negotiations and discussions will be required with the OEM to finalize the Government's data rights situation. The results of the OEM assertions should be documented in the "Data Rights Sheet" tab of the DMS Excel support tool (or equivalent).

2.2.2 Risk Assessment / Risk Management – Part 1

Since it may not be possible to acquire all of the required product data and associated data rights at no additional cost to the Government, the PM should conduct a Risk Assessment & Management approach to the their data needs. The PM should:

- Assess the risks to the program and to the Army of not acquiring the desired product data or data rights due to cost or other considerations. See Appendix H - Required Resources and Risk Assessment for more details.
- Explore alternatives for acquiring the needed data rights for life cycle support from the OEM. Some, but not all, of the alternative actions include:
    - Additional rights negotiations (ARN). The parties may negotiate for data rights beyond the automatic and default rights conveyed by the DFARS clauses. Such negotiations are subject to a statutory prohibition that the contractor cannot be compelled to relinquish such additional rights as a condition of being responsive to the solicitation or as a condition of award. In a competition, such negotiations within this prohibition are difficult and usually take the form of a voluntarily priced option (often a not-to-exceed price) to deliver all required data (commercial and noncommercial) with not less than GPR. Generally, a competitive evaluation of such options is limited to the life cycle cost impacts to the program.

    - Change Program Strategy(s). Adjust one or more of the program strategies to be consistent with the expected data rights.

    - Use of Competitive Sourcing Proposals (CSP). This approach is unique to major systems and it authorizes a mandatory requirement in the solicitation for competitive sourcing proposals. A CSP does not require (nor prohibit) that the contractor offer additional data rights, but does require that the contractor propose a method by which the Government may competitively re-procure the system. The exact method for achieving such competition is left to the contractor to propose. One possible method to achieve this would be for the contractor to license additional suppliers.

    - Physically and Functionally Interchangeable (PFI) ICPs. When the Government lacks sufficient data rights to competitively re-procure an item (or any sublevel of that item), the Government may describe a new replacement item by the use of Form Fit and Function (FFF) data. Such FFF for commercial and noncommercial items is "automatically" provided with unlimited rights.

- Reverse Engineering by or at the direction of the Government (REG). To fill in for missing data or insufficient data rights, an item may be reverse engineered to develop either a data package or a performance specification. By policy, such reverse engineering is to be used as a last resort and only after obtaining Head of the Contracting Activity (HCA) approval.

- Reverse Engineering by a third party (RET). The above noted policy and HCA approval regarding a Government effort to reverse engineer an item do not apply to such efforts by a contractor. There is a statutorily authorized program (See DoDI 4140.57) by which contractors can purchase or borrow such items for this purpose.

- Internal Government Use (IGU) of Limited Rights data. Many authorized uses of Limited Rights data can enable competition without disclosing or releasing Limited Rights/Restricted Rights data to third parties. This internal Government only use of data may be helpful in connection with reverse engineering efforts by the Government or another contractor. Such uses include:
  - Comparative purposes and evaluating the first article of another contractor;
  - Internal evaluation of third party applications to a Government agency;
  - Validating a competitive copy or reverse engineering effort; and
  - Government oversight of another contractor's performance.

  Always consult with legal counsel when considering use of Limited Rights/Restricted Rights data to facilitate competition.

- Periodic competitions for subsystem upgrades where it employs one of the above solutions to conduct the new competition. The new competition may itself not lead to competitive rights.

- Discuss the risks of not acquiring product data and data rights that are not forecasted to be needed for the current TDS, AS and SS, but may be required if changes occur to any of these. For example, what are the risks to the Government of not acquiring certain product data and rights if the current planned AS calls for sole source procurement of all end items and spares from the OEM, and later a decision is made to break-out various spares for competitive procurement? By not acquiring the data and rights, has the program locked the Government into a course of action that would be costly or impossible to change at a later date.

More information about alternative ways to enable competition without having the desired level of data rights can be found in the Appendix B - Government Data Rights Procedures and Background Information.

It is recommended that the DMS should report the key results of the OEM assertions and data rights gap analysis through level 3 of the WBS, with the entire detailed analysis included as an appendix.

2.3 *Step 3 - Data Management & Use*

In the final step of the DMS analysis process, the need for various Government (and possibly contractor) organizations to access and use the product data over the life cycle of the acquisition program must be

considered and planned for. The Defense Acquisition Guide (DAG), Sections 2.3.14.2 and 4.2.3.1.7, recommends PMs establish an Integrated Data Environment (IDE) that allows every activity involved with the program to cost-effectively create, store, access, manipulate, and exchange digital data. PMs are also encouraged to use existing IDE infrastructure (such as repositories operated by AMC LCMCs and/or RDECs) as appropriate. United States Code (U.S.C.) Title 40 subtitle III, U.S.C. Title 10 Sections 2223 and 3014, and U.S.C. Title 44 chapters 35-36 drive the DoD and Army policies for Information Resource Management and Information Technology. Army Regulation (AR) 25-1 applies to information technology contained in both business systems and national security systems (except as noted) developed for or purchased by the DA. This regulation implements the above Public Law as well as DoDD 8000.01 and sets the strategic path for Information Technology (IT) use.

The key considerations in developing a data management approach are:

- The Information Technology (IT) environment that will be used to store and manage the data. The choices are:
    - Government repositories – a combination of command specific repositories usually provided by the acquisition program's Life cycle Management Command (LCMC) or Research, Development and Engineering Center (RDEC), and AMC or Army-wide enterprise repositories such as the Logistics Modernization Program (LMP) and Logistics Information Warehouse (LIW).
    - Contractor repository – provided by either the OEM or a third-party contractor via an existing contract vehicle and a commensurate level of funding provided by the PM for the storage, maintenance and providing the Government access to the data.

  Program-unique repositories are discouraged as long-term product data IT environments due to the high cost to the Army if multiple PMs establish and fund separate IT environments. They may also represent possible violations of the Clinger-Cohen Act if a program unique repository represents a duplication of an existing IT capability within the DoD and have not been certified by the appropriate Investment Review Board and the Defense Business System Management Council (DBSMC) (if $1M or more in cost). Program unique repository approaches also inhibit data access, sharing and reuse across the Army.

- Budgeting for maintenance and upkeep of the product data throughout the life cycle. Such maintenance activities include:
    - Incorporation of configuration changes (to include changes due to obsolete parts or materials)
    - Technology or format refresh

- Access for Army users throughout the life cycle. This includes methods to be used to inform the organizations that will be involved in the various life cycle support activities what product data exists, where the authoritative copies are stored and maintained, and how they can access the data.

More information about considerations to store and maintain the product data throughout the life cycle of the acquisition program and make it available for use by others can be found in Appendix F - Data Storage and Maintenance and Appendix G - Life cycle Access and Use of Data.

2.3.1 Risk Assessment / Risk Management – Part 2

The PM should continue their risk assessment & management approach in this step by assessing the risks to the program and to the Army of not budgeting and providing sufficient recurring funds for data maintenance and management. Information on considerations for resource requirements and risk assessments can be found at Appendix H - Required Resources and Risk Assessment.

3 DATA MANAGEMENT STRATEGY AND THE LIFE CYCLE

Before the actual DMS format and content is discussed there are some key points that should be understood.

First, the DMS will only be a summary of the results of the detailed data, data rights, and data management needs analysis described above. The full analysis should be documented in the DMS worksheet, but the DMS itself will identify that the full analysis was performed, provide an overview of the results of each step of the analysis, and highlight any risk issues that were identified and any actions required by decision authorities to mitigate those risks.

Second, a DMS is required for each Milestone Decision Review (MDR) and the Full Rate Production (FRP) Decision Review (DR), but the contents and focus of the DMS are different for each. As the program moves from Milestone (MS) A through MS C and FRP DR there is an escalating amount of data to be addressed in the DMS. Though not an official MDR point, the transition within the Engineering and Manufacturing Development Phase from the Integrated System Design effort to the Systems Capability and Manufacturing Process Demonstration effort may be a good time to re-assess and update the program DMS.

After MS A, each successive DMS takes on a dual nature. It will both:

1) Describe the planned approaches and actions for the upcoming life cycle phase, and
2) Report on the actual results of the actions from the just completed phase

The latter information is necessary to inform MS decision makers of any changes to the DMS that may have occurred from the strategy approved at the prior MS. For example, at MS A a program's DMS may have indicated an intent to acquire Unlimited Rights to the required data sets, but as a result of the Technology Development Phase contract negotiations the contractor may have asserted legitimate claims to proprietary data which now limit the Government's data rights. As a result, the DMS for the next MS should identify these occurrences and describe the new data strategy and any risk mitigation approaches.

Figure 6 depicts required and recommended review points in the life cycle of a program.

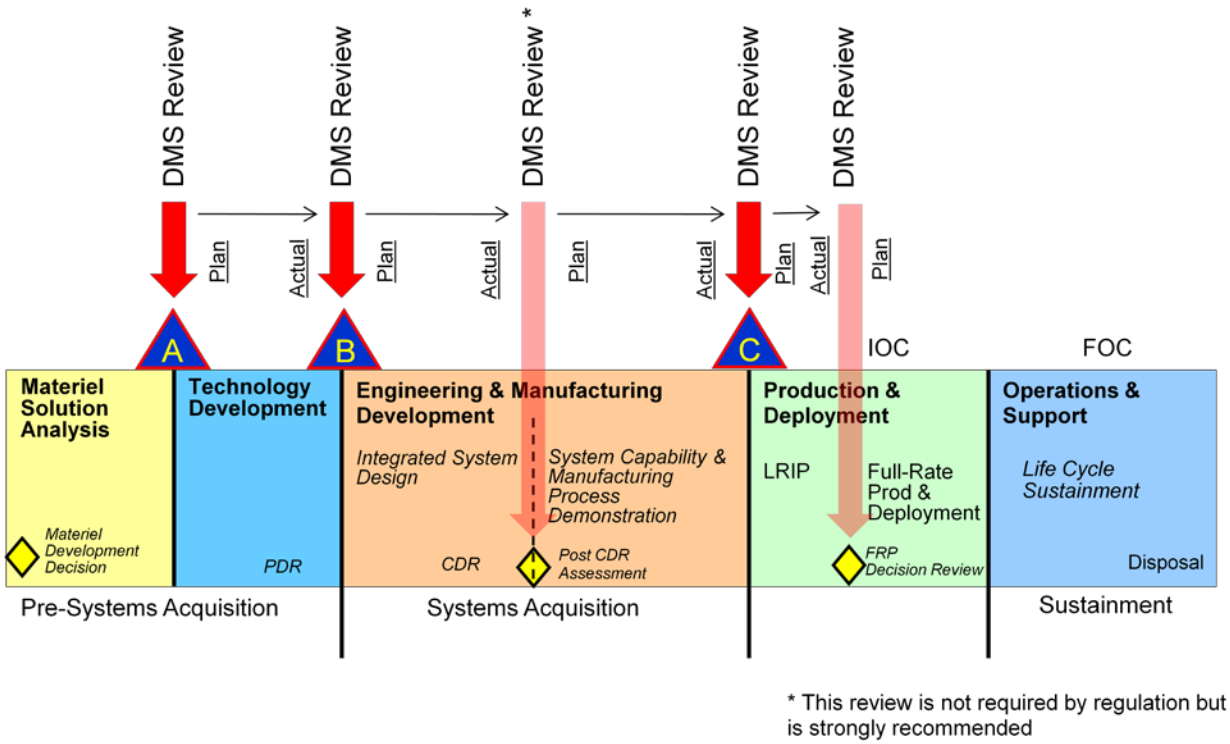


Figure 6 - Acquisition Life cycle and Data Management Reviews

Below are excerpts from DoDI 5000.02 that highlight key activities to be accomplished at each life cycle phase and the resulting product data from each activity.

Materiel Solution Analysis Phase

Phase Activities:	*Resulting data for consideration of acquisition and associated rights:*
Identify and document the recommended materiel solutions to move forward in development	Descriptions of each potential materiel solution considered

Technology Development Phase

Phase Activities:	*Resulting data for consideration of acquisition and associated rights:*
Develop technology approaches and associated prototypes (preferably two or more) to reduce technical risk, validate designs and cost estimates, evaluate manufacturing processes, and refine requirements. • Technology developed in S&T • Technology procured from industry	Product definition information associated with each design/technology under consideration. This includes: • Design information (drawings, specifications, CAD models, engineering studies, engineering analyses, trade studies, simulations and models) • Requirements • Preliminary Manufacturing information (preliminary manufacturing process planning and evaluations)
Plan for life cycle sustainment of each proposed technology (follow and adjust Life-Cycle Support Planning). Life cycle sustainment considerations include: supply, maintenance, transportation, sustaining engineering, data management, configuration management, Human Systems Integration (HSI), environment, safety (including explosives safety), and occupational health, protection of critical program information and anti-tamper provisions, supportability, and interoperability.	Planning for life cycle sustainment of each candidate technology (logistics management information (LMI))
Conduct Preliminary Design Review (PDR) of all candidate designs to select the recommended design & technology approach. • Successful PDR establishes the Allocated Design Baseline for that design	Acquisition program Allocated Configuration Baseline (total system and major component level specifications, drawings and interfaces)

Engineering & Manufacturing Development (EMD) Phase

Phase Activities:	*Resulting data for consideration of acquisition and associated rights:*
Develop a system or an increment of capability • Define system and system-of-systems functionality and interfaces, complete hardware and software detailed design, and reduce system-level risk. • Integrated System Design activities shall include the establishment of the product baseline for all configuration items.	Acquisition program Product Configuration Baseline (PCB) and documentation of EMD efforts. This includes: • Design information (drawings, specifications, CAD models, engineering studies, engineering analyses, trade studies, simulations and models) • Requirements documents • Manufacturing information (manufacturing process planning) • LMI • Test & QA information (test reports, test plans) • Configuration Control information (ECPs, Waivers, ERRs) • Other associated information
Ensure operational supportability with particular attention to minimizing the logistics footprint.	LMI
Conduct successful Developmental Test and Evaluation (DT&E) and Operational Test & Evaluation (OT&E).	Test Reports
Conduct CDR to establish the acquisition program product configuration baseline.	Acquisition program Product Configuration Baseline (total system specifications, drawings, models and interfaces) plus the studies and analyses that supported the design

Production & Deployment Phase

Phase Activities:	*Resulting data for consideration of acquisition and associated rights:*
Conduct Low Rate Initial Production (LRIP) (if part of the approved Acquisition Strategy) • The purpose of LRIP is to complete manufacturing development in order to ensure adequate and efficient manufacturing capability and to produce the minimum quantity necessary to provide production or production-representative articles for IOT&E, establish an initial production base for the system; and permit an orderly increase in the production rate for the system, sufficient to lead to full-rate production.	Manufacturing information (manufacturing process plans, work instructions, statistical process control metrics, process capability studies, but only if required for organic manufacturing or rebuild activities) Adjustments to the Acquisition program Product Configuration Baseline as a result of LRIP or production activities. • Configuration Control information (ECPs, Waivers, ERRs) • Design, manufacturing and logistics information from the Engineering and Manufacturing Development Phase needs to be updated.
Begin Full Rate Production	Final Acquisition program Product Configuration Baseline Adjustments to the Acquisition program Product Configuration Baseline as a result of production activities. • Configuration Control information (ECPs, Waivers, ERRs) • Design, manufacturing and logistics information from the Engineering and Manufacturing Development Phase needs to be updated.
Apply Item Unique Identification (IUID) to all applicable acquisition program components.	Materiel In-Service information (IUID, “as produced” configuration information)

Operations & Support Phase

Phase Activities:	*Resulting data for consideration of acquisition and associated rights:*
Operate, support, and sustain the system in the most cost-effective manner over its total life cycle.	Materiel In-Service information (system maintenance and reliability information, system Condition-Based Maintenance (CBM) data, "as maintained" unit configuration information)
Initiate system modifications, as necessary, to improve performance and reduce ownership costs.	PCB
At the end of its useful life, a system shall be demilitarized and disposed of in accordance with all legal and regulatory requirements and policy relating to safety (including explosives safety), security, and the environment.	Disposal and item characterization information

For a "new start" acquisition program, its first DMS will support the MS A decision and explain the product data and data rights needed and why they are needed, the actions planned to be taken to acquire the data and data rights, and the planned approach for long-term access and use of the data in its IT environment. The primary focus of the MS A DMS will be the actions to be taken in the Technology Development phase.

It should be noted that the types of product data of probable interest at MDR A will be very limited – focused on design related information to be acquired from contractors in the Technology Development phase of the life cycle. This includes proposed preliminary design approaches and the results of their requirements allocation process that will result in the approved Allocated Configuration Baseline at the end of the Preliminary Design Review (PDR). Since MDR B is the lead-in for the Engineering and Manufacturing Development (EMD) phase of the life cycle, where most of the detailed design and logistics support analysis will be conducted, the types of product data the PM has to consider and plan for is greatly increased. Midway through EMD, after successful completion of the Critical Design Review (CDR) occurs, a Post-CDR Milestone Review occurs to approve transition from the Integrated System Design sub-phase to the System Capability and Manufacturing Process Demonstration sub-phases of EMD. At MDR C, most of the development activities should be nearly completed, and the product related data and associated data rights already specified in the EMD contract. At this point the DMS should be focused on confirming the completion of the data activities described in the MDR B DMS, and specifying any new activities that may be required, such as handling of engineering change proposals (ECPs) and field feedback information.

Table 3 summarizes how the depth and breadth of the DMS product data analysis increases through the MDRs. Each cell marked "X" represents a type of product data that is recommended for analysis for that particular MDR.

Table 3 - DMS Data Objects over Life cycle

	Milestone A	Milestone B	Milestone C / FRP
1.0 Product Definition Information	-	-	-
1.1 Design Information	X	X	X
1.1.1 Product Design	X	X	X
Technical Data Package (TDP) - General	X	X	X
Interface Control Document	X	X	X
Engineering Product Structure	X	X	X
1.1.2 Other Design Information	X	X	X
Functional Breakdown Descriptions	X	X	X
Trade Study Reports (Trade-Offs)	X	X	X
Design Selection Decision Document	X	X	X
Engineering Analyses	X	X	X
Models & Test Cases (Simulation)	X	X	X
1.2 Requirements	X	X	X
Capabilities Development Document (CDD)		X	X
Capabilities Production Document (CPD)			X
TDP - System Specifications	X	X	X
1.3 Manufacturing Information		X	X
Manufacturing Instructions		X	X
Manufacturing Process Routings		X	X
Depot Maintenance Work Requirements (DMWRs) and National Maintenance Work Requirements (NMWRs)			X
2.0 Product Operational Information	-	-	-
2.1 Logistics Management Information	X	X	X
2.1.1 Maintenance Planning Information/Technical Publications	X	X	X
2.1.2 Support & Test Equipment Information		X	X
2.1.3 Supply support Information		X	X
2.1.4 Manpower, Personnel & Training Information		X	X
2.1.5 Packaging, Handling, Storage, and Transportation (PHST) Information		X	X
2.1.7 Environmental, Safety & Occupational Health (ESOH) Information		X	X

	Milestone A	Milestone B	Milestone C / FRP
2.2 Material In-Service Information			X
Field Feedback information (Maintenance Incidences)			X
Demand Data from Field Requisitions			X
Item Prognostics & Diagnostics Information			X
Field Quality Deficiency Report Data			X
Field Supply Deficiency Report Data			X
Product Unit Configuration Information			X
3.0 Associated Information	-	-	-
3.1 Verification Information		X	X
Test Reports		X	X
Physical Configuration Audits		X	X
Functional Configuration Audits		X	X
3.2 Configuration Control Information		X	X
Request for Change		X	X
Request for Variance			X
Configuration Control Board Decision		X	X
Product Configuration Management Status Accounting Data			X
3.3 Other Associated Information			X
Government Industry Data Exchange Program (GIDEP) Notices			X
Supplier Notices of Obsolete Parts			X
Disposal and Demilitarization Information			X

4 DATA MANAGEMENT STRATEGY (DMS) TEMPLATE

The following template is recommended for use by all Army programs preparing DMSs. More detailed guidance for generating most of the DMS sections can be found in the appendices to this DMS Guide.

Date

Data Management Strategy for the *XXXXX* Program

This document, together with the accompanying Excel worksheet support tool, constitutes the DMS for the (*XXXXXX)* program.

1. Description of Program

2. Program Acquisition and Logistics Support Strategies.

The (*XXXXX*) system will be entering the (*XXXXX*) life cycle phase.

The program's planned acquisition strategy is:

The program's planned logistics support strategy is:

3. Assessment of Program Life cycle Data Requirements.

The following types of product data will be required by the specified organizations to perform their respective life cycle functions:
(*Specify each organization in a separate row below the major categories of product data along with their corresponding life cycle functions and data needs. Some typical ones are provided in the list below, but add or delete to this list as required. Specify the product data required by each organization only to the 3rd level "X.X.X" of the product data hierarchy in the Excel Worksheet Support Tool.*)

Organization needing the data	Their life cycle mission functions	Required Product Data
PM Office		
R&D Center(s)		
LCMC		
OEM		
Production contractors		
Government Arsenals/Depots		
Other Army Programs		
ATEC		
LOGSA		
Field Maintenance personnel		
Performance Based Logistics (PBL) Providers		
Software Engineering Centers		

4. Data Rights Approach and Gap Analysis.

The Government will need certain types of data rights for the product data associated with all weapon system subsystems and components in order to support the planned Acquisition Strategy and Supportability Strategy.

The PM will require the development contractor(s) to assert any claims of limited or restricted rights for the Government as part of their contract proposal for this life cycle phase. All such assertions will be required to be substantiated by evidence of funding allocations and guided by DFARS requirements for types of technical data to which the Government will have “automatic” or “default” rights.

Based on existing knowledge and/or actual contractor data rights assertions, we anticipate or know of (check the appropriate choice below):

_____ No gap between the data rights required and the data rights expected to be agreed to in the contract.

_____ The following gaps between the data rights required and the data rights expected to be agreed to in the contract.

The DFARS defined categories of data rights are:

Unlimited Rights (UL)
Government Purpose Rights (GPR)
Limited Rights (for Technical Data) (LR)
Restricted Rights (for Computer Software) (RR)
Special License Rights (SLR)

Acquisition program Subsystem or Component	**Type of Government Data Rights Expected**	**Rationale for less than Government Purpose Rights**

5. Risk Mitigation Approaches.

Based on the above anticipated mismatches, the following actions will be taken by the program to enable consistency between the program's TDS or AS, SS, SEP, and DMS, and the data and data rights being acquired by the program:

6. Data Formats.

In order to minimize the costs of unique software applications, data maintenance, and data reformatting, and to enhance long-term data usage, the program has selected the following data format approaches: *(Note: Examples of data format approaches would be specifying data formats that your organization (or others) is set up to deal with, or use of neutral file formats that can be read or used by multiple applications.)*

7. Data Delivery and Review.

In order to assure the content and quality of all contractually ordered data, and adherence to contractual agreements for data rights markings, the program has scheduled formal delivery of the specified contractor generated product data to occur at the following points in the life cycle:

The method of delivery will be:

The delivered data will be reviewed via (design reviews, configuration audits, sample inspection at time of delivery, other (describe)) to ensure it meets content and quality requirements, to include data markings.

8. Data Storage and Maintenance for Life cycle Use.

Since the organizations identified in Section 3 of the DMS have needs for access and use of the acquisition program product data, the following types of product data will be stored and maintained in the indicated IT systems with appropriate access provided.

Type of Product Data	**IT Storage & Management System**

The maintenance of the data is expected to require an annual expenditure of $(*XX,XXX*) to keep the data current and accurate as a result of ECPs and other needs. This funding is a part of the current program budget.

9. Resource Requirements.

We require $ (*XX,XXX*) additional funds to acquire necessary rights to acquisition program product data needed for:

We require $ (*XX,XXX*) additional funds annually to manage and maintain the acquisition program product data over the life cycle. This includes funding required to store the data and maintain its currency.

If these funds are not provided the program will incur the following risks:

10. Merits of Priced Contract Option for later Acquisition of Data

(*If applicable. If not applicable then use N/A*)

Based on the data rights gap analysis assessment performed in Section 4 of the DMS it has been determined that the Government's "automatic" and " default" rights in data (confirmed prior to award) are insufficient to fully enable the preferred acquisition and/or logistics support strategy. Additional funding necessary to acquire the needed additional level of data rights is not currently available, and other negotiation options are insufficient, so a priced option for purchasing "additional" data rights at a later point in time when more funding may be available is considered the only viable option.

The merits of this approach include:

The risks of this approach include:

11. Program DMS POCs. The following POCs should be contacted if there are any questions about the information contained in this DMS:

POC Name	Organization	Phone	E-Mail

Appendix – DMS Worksheet (or equivalent)

APPENDICES

The following appendices provide additional guidance to assist PM offices and others in the proper preparation of a program DMS.

Appendix A - Program Life cycle Data Requirements A-1
Appendix B - Government Data Rights Procedures Background Information B-1
Appendix C - DFARS Contract Clauses for Data Rights C-1
Appendix D - Data Formats D-1
Appendix E - Data Delivery.....E-1
Appendix F - Data Storage and Maintenance F-1
Appendix G - Life cycle Access and Use of Data G-1
Appendix H - Required Resources and Risk Assessment H-1
Appendix I - DMS Worksheet Tool.....I-1
Appendix J - Acronyms J-1

Appendix A - Program Life cycle Data Requirements

PMs must develop an estimate for the data needed to support both short-term and long-term program needs to design, manufacture, and field the item, and then to sustain it throughout its life cycle. Included will be identification of the data needed to ensure that all future life cycle needs can be achieved by enabling competitive contracting strategies whenever possible.

Definition of Product Data

The OSD requirement for DMSs in the DoDI 5000.02, Encl 12, states the DMS must "*assess the data required to design, manufacture, and sustain the system, as well as to support re-competition for production, sustainment, or upgrades.*" This definition of the scope of technical data to be addressed within the DMS matches well with the definition for product data developed by the Army Product Data and Engineering Working Group (PEWG). The PEWG definition for Product Data (data related to a product) is "*All data created as a consequence of defining (requirements), designing, testing, producing, packaging, storing, distributing, operating, maintaining, modifying and disposing of a product.*" The PEWG has further delineated product data into segments containing:

- **Product Definition Information -** information that defines the product's requirements, documents the product's attributes, and is the authoritative source for configuration definition and control. Examples include:
  - Actual product definition information (drawings, specifications, 3-D CAD models, (aka: the Technical Data Package (TDP)), etc. – the "As Designed" product configuration)
  - Design concept information (analyses, trade studies, and information about designs not selected for use should be captured, retained and managed)
  - Requirements (Performance and Logistics Support)
  - Manufacturing information (the "As Built" product configuration)
  - Depot overhaul/modification information (the "As Modified" product configuration)

- **Product Operational Information -** information used to operate, maintain and dispose the product. Examples include:
  - Field Feedback information (records of maintenance actions, depot overhauls / modifications, field deficiency reports, etc. – the "As Maintained" product configuration)
  - Product identification information (part and unit identification)
  - Technical manuals
  - ESOH/Hazardous Material information,
  - Distribution information (packaging, preservation, transportation)

- **Associated Information -** information generated as part of the product development and life cycle management process, but isn't clearly definable as either of the other two categories. Examples include:
  - Configuration control information (ECPs, Waivers)
  - Test & QA information

Unfortunately, the definition of “technical data” used in the original OSD policy memo and DoDI 5000.02 citation does not match the definition contained in the Defense FAR Supplement (DFARS). Figure 7, below, shows a graphical representation of the relationship between the DFARS definition of “technical data”, the PEWG definition of Product Data, and a common misperception that the term “technical data” is really equivalent to just a TDP.

Due to the similarity in definitions between the OSD DMS policy memo and the PEWG definition of product data and the inconsistency with the DFARS definition of “technical data”, the term “product data”, as defined above, shall be used in lieu of the term “technical data” used in the OSD guidance.

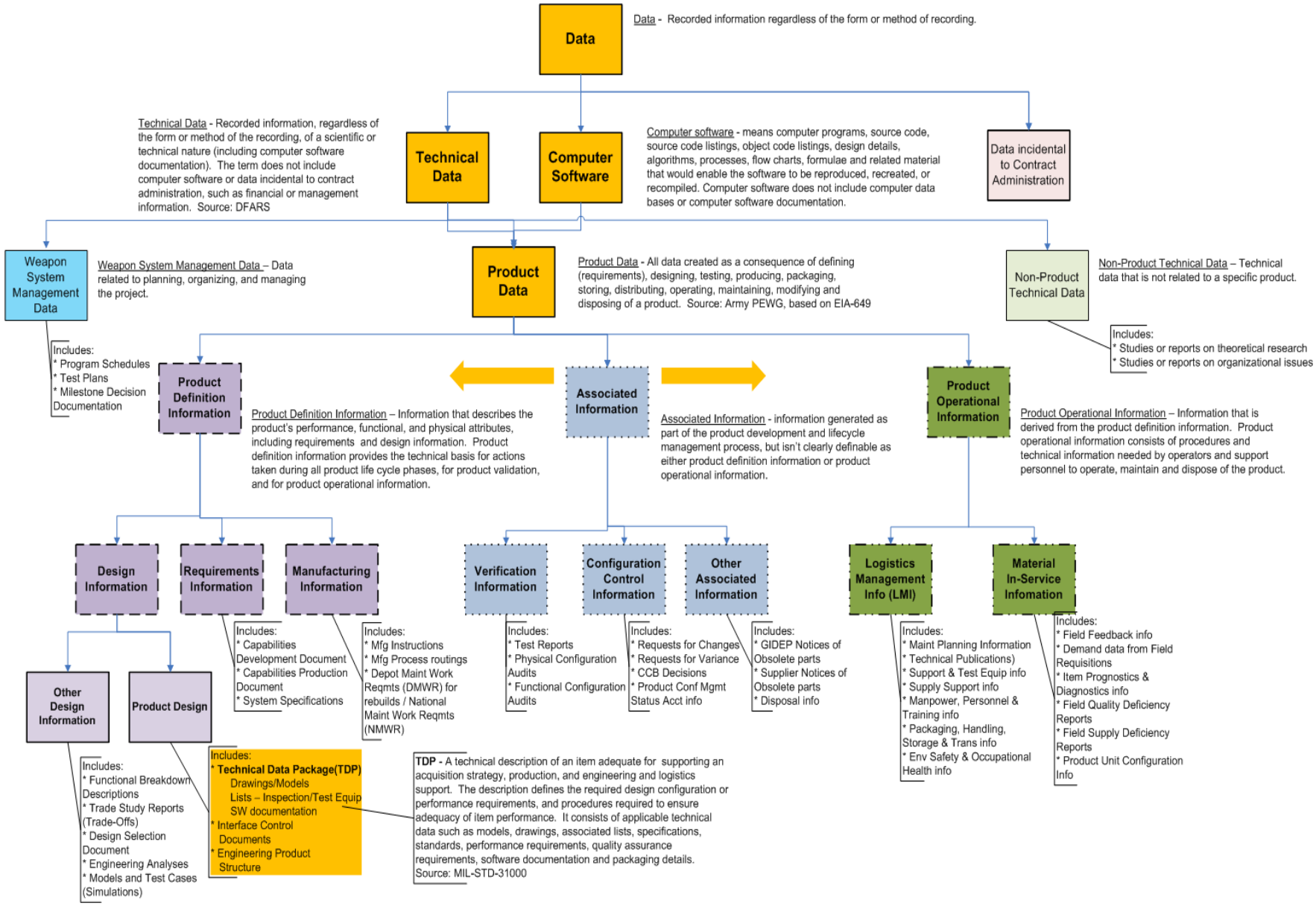


Figure 7 - Relationships of Different Types of Data

Life cycle functions can be divided into the basic categories of development, production, procurement, and sustainment. Since the Office of Management and Budget (OMB), Congress, and OSD have all called for increased use of competitive acquisition and logistics support approaches, the product data required for competition should be a primary (but not the sole) driver of data and data rights needs. The TDS or AS, SEP, and SS will describe which organization (organic Government, OEM, or other contractor) is planned to perform those functions. Government organizational performance of life cycle functions should be further segregated such that the PM understands which specific organizations will have needs for acquisition program product data and hence should be participants on the DMS IPT. Table 4 is a representational example of the type of life cycle function allocation between organizations that could exist for a hypothetical weapon system.

Table 4 – Representational Allocation of Life cycle Function Responsibilities

	Lifecycle Functions										
Organizations	Program Mgmt	Systems Engineering	Test	Integration	Provisioning	Inventory Mgmt	Contracting	Production	Sustainment Eng	Maint / Repair	Demil / Disposal
PM Office	X	X	X	X	X	X	X		X		X
OEM	X	X	X	X	X						
RDEC		X	X	X	X				X		
LCMC	X	X	X	X	X	X			X	X	X
ACC							X				
ATEC		X	X								
Prod Contractor								X			
Arsenal / Depot		X	X	X		X	X	X		X	
DLA					X	X	X				
Field Maintainers			X							X	
Log Supt Contractor										X	
Software Eng Center		X	X	X			X		X	X	

Acronyms:
ACC = Army Contracting Command
ATEC = Army Test & Evaluation Command
DLA = Defense Logistics Agency
LCMC = Life Cycle Management Command
LOGSA = U.S. AMC Logistics Support Activity
OEM = Original Equipment Manufacturer
PM = Program/Project Management
RDEC = Research, Development & Engineering Center

Appendix B - Government Data Rights Procedures Background Information

General. Government license rights in technical data and computer software, as defined by DFARS and hereafter referred to as "Data," are a bundle of "intellectual property" license rights which specifies what uses and releases the Government is authorized to make. The allocation of these rights between a Government contractor and the Government is specified in the standard DFARS contract clauses. The Government's "automatic" and "default" rights in those DFARS clauses may be enlarged or decreased by specific negotiations recorded in the contract. With few exceptions, the Government does not own data. The Government obtains license rights in the data. This remains true even when the Government exclusively funds development costs. All standard DFARS licenses to technical data and software include the right of the Government to make modifications.

Data license rights: Automatic and Default (based on funding). Certain license rights in data arise automatically upon contract award and performance regardless of funding issues. These "automatic" rights in data include "unlimited rights" in: form, fit, and function (FFF) data; computer software documentation; and installation, operation, maintenance, and training (IOMT) data. Other "default" license rights (e.g., Unlimited and Government Purpose Rights) are created by direct Federal funding for the development of related items, components, or processes (ICPs).

Delivery of data and contract procedures. The contract requirement for a formal delivery obligates the contractor to comply with three critical contract procedures regarding data rights: asserting; marking; and justifying. These procedures force the contractor to clarify its positions on data rights and highlight any areas of disagreement between the parties. Formal delivery of data is a critical step for securing the Government's rights in data. This delivery must be scheduled in the contract by use of an approved Data Item Description (DID) or FAR/DFARS clause to be legally enforceable and to invoke critical contract procedures.

Data license rights categories. There are six potential data rights categories which are subject to the contract clauses that define and allocate data rights. Commercial computer software and certain data incidental to contract administration are not subject to these DFARS clauses and procedures. Government rights in commercial computer software must be separately negotiated using language which is consistent with a DFARS contract and Federal Procurement laws (See DFARS 227.7202-1 and Subpart 208.74). All such special negotiations should be reviewed by Government legal counsel. In all categories below, a basic copyright marking (name, year and symbol/word for copyright) by the contractor is allowed and such marking is not inconsistent with the stated license rights.

1. **Unlimited Rights (UR) in Technical Data and Computer Software.** There is presently no mandatory marking/legend for "Unlimited Rights" data. Data which is required to be delivered under the contract and which is unmarked (or marked only with a copyright) at delivery is generally presumed to provide "Unlimited Rights" to the Government. However, it is always best to have the status of unmarked data confirmed with the contractor or reviewed by Government legal counsel. "Unlimited Rights" arise in certain types of data automatically upon award (e.g., FFF and IOMT) and in most other data based upon exclusive (100%) Federal funding of the ICP to which that data pertains. The automatic unlimited rights in certain types of

data (e.g., FFF, IOMT) apply to commercial AND noncommercial technical data. The term "unrestricted" is used in the DFARS 252.227-7015 clause for the automatic rights which are independent of funding and appropriate to commercial technical data under that clause. The Government may share commercial or noncommercial UR data with anyone for any reason.

2. Government Purpose Rights (GPR) in Noncommercial Technical Data and Computer Software. If neither party proves either exclusive (100%) Government or Private funding, then the development of an ICP is generally presumed to have been with "mixed funding." Unless otherwise explicitly negotiated, the Government receives a GPR license in all data pertaining to ICPs developed with "mixed funding." The Government may share this data with third parties for any Government purpose after having that third party execute a DFARS Non-Disclosure Agreement (NDA). There is only one contractually authorized marking for such data. If the contractor fails to procedurally protect these rights (assert/mark/justify), additional rights should vest in the Government.

3. Limited Rights (LR) in Noncommercial Technical Data. When the contractor has exclusively (100%) funded the development of a non-commercial ICP, the Government receives "Limited Rights" in the data for which the Government has not received automatic "Unlimited Rights." Usually, such data subject to Limited Rights is detailed manufacturing or process data (DMPD). The Government may NOT share this data with third parties (to include support contractors). There is only one contractually authorized marking for such data. If the contractor fails to procedurally protect these rights (assert/mark/justify), additional rights should vest in the Government.

4. Restricted Rights (RR) in Noncommercial Computer Software. When the development of computer software is 100% privately funded, the Government receives "Restricted Rights" in that computer software for which the Government has not received automatic "Unlimited Rights." Automatic URs include all delivered computer software documentation. This category applies only to noncommercial computer software. With very limited exceptions listed in the DFARS, Government may NOT share this data with third parties (to include support contractors). There is only one contractually authorized marking for such software. If the contractor fails to procedurally protect these rights (assert/mark/justify), additional rights should vest in the Government.

5. Special License Rights (SLR) in Technical Data and Computer Software. Where the above DFARS defined categories are insufficient to properly define an agreement of the parties as to data rights allocations, the parties may specifically negotiate those rights and designate them with a marking/legend of "Special License Rights." That marking directs the reader to the contract for a full definition. The Government may always attempt to increase its rights by negotiation (without coercion) to "Government Purpose Rights", "Unlimited Rights" or even ownership rights. The DFARS contract clauses prohibit the Government from negotiating/accepting less than "Limited Rights" in noncommercial technical data or "Restricted Rights" in noncommercial computer software. Two statutes (10 U.S.C. 2304 and 10 U.S.C. 2320(a)(2)(G)(ii)) prohibit the relinquishment of certain competitive or accorded rights. Government legal counsel should always be consulted before relinquishing Government rights in data.

The DFARS 252.227-7015 clause for technical data regarding commercial items also refers to a "special license agreement" which may be negotiated to attempt to obtain "additional rights" in technical data when the Government desires more than the "unrestricted rights" in certain data provided under that clause. There is no DFARS mandated marking for data covered by these additional rights. A marking scheme that distinguishes the data as commercial and clearly indicates the Government's rights and obligations, if any, would be prudent.

6. Small Business Innovative Research (SBIR) Data Rights. Within DoD, SBIR data rights are uniquely defined by DFARS. SBIR data rights may be marked as such by the contractor at the time of delivery (no advance assertion is required) and they do not expire until 5 years after completion of the "project" which may differ from completion of the contract. The Government may use SBIR data rights similar to GPR except that ONLY "support services contractors" may have access for an authorized Government Purpose. SBIR data rights attach to noncommercial technical data and noncommercial computer software first created and then delivered under a SBIR contract. The unique features of such SBIR data rights and differing policies from the Small Business Administration at present normally dictate obtaining legal support prior to use. There is only one contractually authorized marking for such data. If the contractor fails to procedurally protect these rights (assert/mark/justify), the Government takes additional rights.

Procedural processes – critical contract rights. The following procedures do NOT apply to commercial data. There are three contract procedures with which the contractor must comply or risk losing the ability to limit/restrict the Government's use or release of the data: asserting; marking; and justifying the assertion/marking.

1. Asserting. A proper assertion is one made before award or made prior to delivery (and justified as a "new" or "inadvertent omission" not affecting source selection) and incorporated into the contract. It should specifically identify pieces of data (not documents which might contain such data) and the related ICP. Without a proper assertion in the contract, data must be delivered unmarked (except for a copyright notice) and with "Unlimited Rights."

2. Markings. Noncommercial technical data and noncommercial computer software may be delivered only with the following contractually authorized markings:

- Copyright notice (only the three basic elements of year, owner, and copyright word/symbol);
- Unlimited Rights (no marking currently authorized by DFARS);
- Government Purpose Rights;
- Restricted Rights (computer software);
- Limited Rights (technical data);
- Special License Rights.

The restrictive/limiting markings (Government Purpose Rights, Restricted Rights, Limited Rights and Special License Rights) when applied to delivered data must be limited to the data on each page (by circling, underlining, or other method of identifying) which is subject to that

asserted limitation or restriction. An entire page (or document) may not be marked unless every piece of data on the page or within the document is subject to the asserted limitation or restriction.

3. Justifying. The contract places the burden upon the contractor to maintain sufficient business records to justify any assertion or marking and to provide those records to the Government upon request.

Correcting Assertions and Markings Regarding Data Rights. "Unauthorized" (also labeled "nonconforming") assertions and markings are those which are not covered by a current assertion in the contract or which are not in the contractually specified format. The Contracting Officer may order these unauthorized markings to be removed and corrected, usually within 60 days of notification. "Unjustified" assertions and markings are those which the Government doubts the facts will support. These unjustified assertions/markings may be challenged by the Government by means of a contractually specified validation process. Pending completion of the validation process, a suspected "unjustified" marking is usually honored.

Data Rights and Competition. Whenever the success of a competitive procurement depends upon the competitors' access to Government furnished data, the PM must determine the Government's rights in such data. Data generated solely by Government employees (no use of support contractors) will be subject to only internal Government controls indicated by the assigned Distribution Statement IAW DoDD 5230.24. Data which is not newly generated, but which is reused from other programs or sources should have been obtained by the PM with proper markings as to the Government's rights in that data. (Any uncertainty or doubt about the Government's rights in such reused data must be resolved.) The Government's rights in data created or delivered by a Government contractor must be determined under the terms of the appropriate contract or funding agreement. The Government's automatic rights based upon proper theory are noted above. The Government's actual and immediately useable rights will depend upon the contractor markings placed upon delivered data. Such initial contractor markings are subject to Government rejection (if nonconforming) or challenge (if unjustified).

Contractor markings are NOT assumed to be correct, but are honored until removed or corrected IAW contract procedures. This discussion addresses rights in data delivered under a contract containing the appropriate DFARS clauses. Data furnished or made available to the Government outside such contracts are not subject to the same rules and require a case-by-case review.

Data Rights needed to compete. The following lists the most common areas for competition and the standard DFARS data right licenses which would support such a competition. These standard licenses sometimes provide too little or more than is needed for a specific competition. What is actually required for a specific competition is the right to release all the data necessary for use by those third parties who will be competing. Typically, that would be GPR and UL rights. This release and use right (if not covered by the standard licenses) may be the subject of non-coercive negotiations with the owner of the data or an alternative to obtaining data rights considered. Whenever the Government's data rights in the data to be released are less than what is shown below, those rights may be insufficient to enable competition.

1. **Re-procurement of the system or ICPs/software.**
   - Noncommercial Technical Data: UL or GPR
   - Commercial Technical Data: Unrestricted Rights as defined in 252.227-7015(b)(1)
   - Noncommercial Computer Software: UL or GPR
   - Commercial Computer Software: no standard rights - additional rights must be negotiated.

2. **Sustainment of the system or ICPs: UL or GPR.**
   - Noncommercial Technical Data: UL or GPR
   - Commercial Technical Data: Unrestricted Rights as defined in 252.227-7015(b)(1)
   - Noncommercial Computer Software: UL or GPR
   - Commercial Computer Software: no standard rights - additional rights must be negotiated.

3. **Emergency repair and overhaul of ICPs or software.**
   - Noncommercial Technical Data: any level will suffice for such emergencies – UL/GPR/LL
   - Commercial Technical Data: Unrestricted Rights IAW 252.227-7015(b)(1) or rights IAW 252.227-7015(b)(2)(ii)
   - Noncommercial Computer Software: any level will suffice for such emergencies – UL/GPR/RR
   - Commercial Computer Software: no standard rights - additional rights must be negotiated.

4. **Government Support Contractors (GSC).**
   GSCs are those contractors who provide independent analysis and advice to the Government regarding a system and do not directly compete for or provide any portion of the system. Until special statutory authority (newly passed into law) is implemented in a DFARS case, without specific authorization from the data owner, such GSCs may receive access to only UL and GPR data. GSCs may also receive access to Specifically Negotiated License Rights data where explicitly authorized by a special license. Additional authority may be granted by the owner of the data via special contract agreements or written authority from someone authorized to bind the contractor.

Obtaining sufficient rights in data to enable competition.

When the Government's automatic or standard rights in data pursuant to the DFARS clauses are insufficient to enable competition (limited or full), there are a variety of methods for resolving this gap between what is needed and what is presently (or anticipated to be) available regarding data rights.

1. **Additional rights negotiations (ARN).** The parties may negotiate for data rights beyond the automatic and default rights conveyed by the DFARS clauses. Such negotiations are subject to a statutory prohibition that the contractor cannot be compelled to relinquish such additional rights as a condition of being responsive to the solicitation or as a condition of award. In a competition, such negotiations within

this prohibition are difficult and usually take the form of a voluntarily priced option (often a not-to-exceed price) to deliver all required data (commercial and noncommercial) with not less than GPR. Generally, a competitive evaluation of such options is limited to the life cycle cost impacts to the program.

This solution has great appeal in its simplicity; however, it has not been generally successful in the past. A great deal of evaluation weight must be placed upon the life cycle costs (i.e., the impact of not having competitive rights such as GPR) in order to provide sufficient incentive for the contractors to voluntarily price such options. However, placing too much weight upon long-term life cycle costs may distort the true near-term value of the competing proposals. It may eventually be recognized by contractors that pricing GPR to the Government at a reasonable price represents an immediate and certain profit from those data rights while that contractor still has a likely (fair) competitive advantage in any competition. This can be a win-win for contractors with reasonable profit incentives in the near and long terms.

2. **Competitive Sourcing Proposals (CSP).** This approach is unique to major systems and is authorized by 10 U.S.C. 2305(d) and DFARS 227.7103(e). Use of this authority is subject to certain approvals. While the language is quite complex, it authorizes a mandatory requirement in the solicitation for competitive sourcing proposals (CSP). A CSP does not require (nor prohibit) that the contractor offer additional data rights. A CSP does require that the contractor propose a method by which the Government may competitively re-procure the system. If the Head of the Agency makes a special finding, then the CSP may mandate a proposal that "enables the United States to acquire competitively in the future an identical item [even] if that item was developed exclusively at private expense…" The exact method for achieving such competition is left to the contractor to propose. The relinquishment of data rights is one possible method. Others could include a proposal to qualify one or more additional sources or to reuse an existing subsystem to which the Government has competitive rights. When the special authority for "identical items" is not invoked, the CSP proposal might be for a physically and functionally interchangeable ICP as noted below.

   A special and very useful example would include a requirement that IOMT be delivered with any asserted/marked LR/RR DMPD placed into a separate annex. The solicitation could require a CSP that replaced the gaps in the IOMT data/documents (caused by the omitted DMPD) with data sufficient to competitively "sustain" the system as opposed to re-procurement. One obvious solution is to substitute data that is detailed enough to conduct maintenance, repairs, and replacements but not detailed enough to actually manufacture the item.

3. **Physically and Functionally Interchangeable (PFI) ICPs.** When the Government lacks sufficient data rights to competitively re-procure an ICP (or any sublevel of that ICP), the Government may describe the replacement ICP by the use of FFF data. The obvious negatives for this approach are the added time for design development and qualification, expansion of the logistic footprint, and assigning responsibility when the interchangeable ICP does not function properly.

4. **Reverse engineering by or at the direction of the Government (REG).** To fill in for data in which the Government is lacking sufficient data rights, an ICP may be reverse engineered to develop either a data package or a performance specification. By policy,[1] such reverse engineering is to be used as a last resort and only after obtaining Head of the Contracting Activity (HCA) approval. If a performance specification is generated, it will have the same negatives as the physically and functionally interchangeable solution above. A design specification would eliminate those issues but would result in the Government warranting the validity of that specification. There are some procedural pitfalls to reverse engineering which need to be addressed.[2]

5. **Reverse engineering by a third party (RET).** The above noted policy and HCA approval regarding a Government effort to reverse engineer an ICP do not apply to such efforts by a contractor when not done at the direction of the Government. There is a statutorily authorized program (See DoDI 4140.57) by which contractors can purchase or borrow such ICPs for this purpose.

6. **Internal Government Use (IGU) of Limited Rights data.** Case law has established many authorized uses of Limited Rights data which may enable competition without disclosing or releasing LR/RR data to third parties. This use of data may be helpful in connection with reverse engineering efforts by the Government or another contractor. Such uses include:

   - Comparative purposes and evaluating the first article of another contractor;
   - Internal evaluation of third party applications to a Government agency;
   - Validating a competitive copy or reverse engineering effort;[3] and
   - Government oversight of another contractor's performance.

   Always consult with legal counsel when considering use of Limited Rights/Restricted Rights data to facilitate competition.

7. **Miscellaneous (MISC).** The above listing represents those solutions which have been presently identified and which are legally proper. Other solutions may evolve as the Government begins to actively work these data rights issues. Care must be taken to ensure Government compliance with licensing terms. Always consult with legal counsel when interpreting contract provisions concerning data rights, especially in areas outside of clear and explicit license language.

---

[1] See DFARS 217.7503 (PGI) and 227.7103-5(d) (2) (iii).
[2] See AMC, Command Counsel, Information Paper, 13 February 2006, titled: Reverse Engineering. Such issues primarily concern assuring that the reverse engineering effort is isolated from any access to or knowledge of proprietary information.
[3] The Government must assure that its copy of the Limited Rights data (or knowledge obtained by viewing such data) is not used by anyone performing the reverse engineering activity.

Process versus Item or Component.

Items or components are typically developed as a direct result of a funded development effort. The process for manufacturing such items or components (in whole or part) is likely to be developed during that same period of original development. However, sustainment processes (inspection, disassembly, repair, maintenance, assembly…) and possibly some manufacturing processes are often "developed" under a later Government contract for the item or component. This distinction is important as the later developed processes are very often wholly or partially developed by "direct Federal funding." Such Federal funding conveys not less than GPR in such processes.

Appendix C - DFARS Contract Clauses for Data Rights

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

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

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

Use of the above FAR/DFARS clauses in all solicitations and contracts is recommended.

SPECIFIC CLAUSES & THEIR USE (SEE DFARS FOR TITLES):
252.227-7018 - All SBIR contracts. (Do not use -7013 or -7014.)
252.227-7025 - All if access to less than unlimited rights TD/CS is anticipated. Strongly recommended in all contracts.
252.227-7026 - Voluntary clause used only to specifically identify at award TD & CS which may be ordered later.
252.227-7027 - Voluntary clause used to order additional deliverables for TD & CS "generated" during performance of the instant contract. Strongly recommended in all solicitations and contracts.
52.227-1 - All contracts and solicitations with limited exceptions.
52.227-2 - All contracts and solicitations with limited exceptions.
52.227-3 - Mandatory use in some sealed bidding for "commercial" supplies/services & construction with many prohibitions on use.
52.227-10 - All which might result in a classified invention/patent.
52.227-11 - All R&D with small business or nonprofit.
52.227-12 - All R&D except when 52.227-11 used.
252.227-7034 - All if 52.227-11 is used.
252.227-7039 - All if 52.227-11 is used.
252.246-7001 - Recommended whenever 252.227-7013 is used.

Note: DFARS clauses can change periodically so you should always verify the current wording when including in contracts and solicitations.

Appendix D - Data Formats

The PM should define data format preferences or requirements for data to be ordered on contract. The contractor will generate significant data in order to perform the instant contract. That data is available to the Government in contractor format for the administrative costs to copy and review for authorized assertions and markings. Requests for other than contractor format (or unusual data) may increase contract costs.

In the area of product data there have been advancements in the generation of model-based 2D and 3D Computer Aided Design (CAD) models. In general, 3D solid models should be delivered in accordance with ISO 10303 Standard for the Exchange of Product model data (STEP), in a native 3D CAD format capable of being exported to ISO 10303 STEP format and in a lightweight viewable format (such as Adobe, Productview and JT) that does not require a CAD application in order to just view and mark-up the model. However, all model formats must comply with ASME Y14.41 PMI content requirements. The validated ISO 10303 STEP format should be strongly considered for use in Engineering and Design product data delivery since it can have a longer shelf life and reduced maintenance costs over native CAD throughout the program, system, or product life cycle, however, a critical issue exists regarding "validation" of the STEP models to ensure consistency with the original native CAD model. No good methods of STEP model validation exist today, so it is up to the PM and the contractor to reach agreement on how this consistency will be determined and verified. If native CAD Engineering and Design data is delivered, be aware that few, if any, CAD packages comply totally with all of ASME Y14.41 currently. Therefore, again the PM must insure an agreement is reached as to what portions of the ASME Y14.41 standard must be met. This should be accomplished by tailoring the ASME Y14.41 standard based on the contractors CAD systems and/or contractor internal modeling standards. It may also be necessary to require the contractor to provide a CAD modeling quality certification as a deliverable. These preferred data delivery formats must be placed in the contract with all attending details on the TDP worksheets contained in MIL-STD-31000. Programs desiring to remain with the traditional 2D format may do so by using ASME Y14.100 and MIL-STD-31000 to guide their formats.

Table 5 provides a sample listing of several types of data normally acquired by the Army and the related standards that should be used to make intelligent format selection decisions. In each case, several formats and content options are available. The referenced standards detail the pros and cons of each option, and the situation in which certain options are preferred. The format and content information from these standards is used to prepare the appropriate contract language and tailor the appropriate DIDs for ordering data on contracts. There are additional types of data and related standards that are not identified in the table, which can be used, where applicable.

Table 5 - Sampling of Types of Data and Related Standards

Type of Data	Related Standard(s)
IETM/ETM	MIL-STD-40051 S1000D
Drawings/Models/Graphics	ISO-10303 (AP 201, 202 & 214) ASME Y14.24 ASME Y14.100 MIL-STD-31000
Logistics	GEIA-STD-0007 ISO-10303 (AP 239) UK DEF STAN-0060
Packaging	MIL-STD-2073-1 ASTM-D3951
Reliability, Availability & Maintainability	MIL-HDBK-338B
Text	ASCII TXT, etc.
Cataloging	DoD 4100.39-M
Configuration Management	MIL-HDBK-61, ANSI/EIA-649

Appendix E - Data Delivery

The DMS should describe the approaches to be used for delivery of the ordered product data, as well as how it will be verified and validated relative to content, quality, and data rights markings.

Typically, there are only two legally acceptable methods of product data delivery, that of delivering to a Government repository or recipient (which is the preferred method), or delivery to a contractor (prime or support) repository to which the PM office has access rights and controls. While a "delivery" under the contract does not create the Government's rights in that data, it does invoke certain contract procedures regarding assertions and markings. These procedures, as explained in Appendix B, are essential to confirming and securing those Government data rights. Informal processes that allow the Government limited access to data without requiring a formal delivery of that data shall not be used for data within the scope of the DMS. DFARS 227.7108 lists just a few of these additional considerations. There is significant benefit to having the data delivered to a Government repository or recipient. Once delivered into Government control, the Government's use of the product data (consistent with its license rights) is endless and is unencumbered. Emergency uses of such data (which are often authorized by the contract licenses or statute) are immediately available to the Government due to its possession of the data. To take full benefit of the Government's "automatic" and "default" rights in data, at least one delivery of the product data shall be scheduled by the end of each contract.

Rationale for delivery to a Non-Government Repository

If delivery to a contractor repository is proposed in the DMS, the rationale for that strategy should be discussed and justified. Such a method of delivery can be problematic since the Government must be prepared to take immediate physical delivery (via contract option or change order) should the contract or contractor hosting the delivered data be terminated, or actions by industry dictate immediate delivery (mergers, buyouts, etc). The Government's inability to timely or fully fund an ongoing contract may also prevent Government access to product data in a contractor's repository or system.

Data Fidelity (Content and Quality)

A key aspect of product data delivery is the suitability of the data. The product data must be suitable for meeting all the supportability and sustainment needs of the program. Technical or product data should always be ordered using the appropriate Data Item Descriptions (DIDs) to adequately define the data content.

Appendix F - Data Storage and Maintenance

PM offices must determine how the program will keep the data maintained, current and accurate, throughout the acquisition program life cycle, so that it will be available for all future needs.

Management and Sustainment of Data

General. Government Data Managers spend a great deal of time ordering, acquiring, and accessing data from contractors. The data should be carefully managed to allow for access, retention, integration, sharing, transferring, and conversion throughout the data and product life cycle. In general, the management and sustainment of data is the responsibility of the IPT or PM for the defense system(s).

Access to data. Data should be stored and identified such that authorized data users can readily search for, locate, and access the data when needed. To assure data is well identified and retrievable, appropriate identification (such as metadata) should be used. The identifying metadata may include date, author, title, general topic key words, document identifier, version identifier, retention date, and data owner information. Identifying metadata is used in data repository index schemes to identify the data type and where the data is located.

Data Markings. 10 U.S.C. § 130, DoDD 5230.24 and DoDD 5230.25 require all technical data to be disseminated with the appropriate distribution statement, export control warning notice (where applicable), destruction notice (where applicable), etc, whether produced in hard copy or digital format. PMs should assign distribution statements to all technical data generated in their programs before primary distribution. When data and/or documents are opened, the distribution markings should be clearly discernable. Distribution statements indicate the extent of secondary distribution that is permissible without further authorization or approval of the controlling DoD office. The intent of these markings is to stem the flow of military-related technical data to our adversaries, without inhibiting technological growth or blocking the exchange of technical data that is vital to progress and innovation. When properly applied, appropriate data markings will keep critical technology from our adversaries but permit it to flow to Government Agencies and private organizations that have a legitimate need for it.

Maintenance of data and data systems. Since the Government often needs its data for several decades, it is important the data be kept in a format and data system that is readily usable. Issues to be considered and addressed with long-term data retention are: data formats, storage media, applications, data systems, etc. Decisions in these areas are driven by mission requirements; anticipated product life cycle, acquisition and logistics support strategies, sources of supply, and cost.

1. **Data storage media.** While the technology associated with storage media is more stable than that of data formats, the media should still be considered and re-assessed throughout the life cycle. File servers containing currently active data are continually being refreshed, but external storage media such as diskettes, tape, or compact disc have a shelf life for only a few years and should periodically be migrated to new storage media to assure their accessibility. Procedures to protect data on any storage media from loss or

inadvertent destruction should be established and applied. A common procedure is to back up the original media on another portable or fixed media and store that copy in a location separate from the primary or master copy.

2. Data authoring applications. To ensure data is readable for later use or manipulation, it may be necessary to also store and retain data authoring or viewing application software to view, revise, and print images or refresh the data. Over time, data will periodically need to be migrated to current software applications and hardware formats for continued currency and availability for retrieval.

3. Data systems. In some cases, hardware systems also need to be kept past the normal active life cycle in order to access data. Current examples include microfiche viewers or tape drives that are not technologically current but provide the only method to read or access certain data due to the original storage media.

Data Maintenance Costs.

The Required Resources and Risk Assessment section of the DMS should discuss the plan to fund the maintenance of the product data throughout the life cycle and the efforts to attribute data quality as an attribute of the SE process such that post-production ECPs and related costs are minimized. During program development, it is expected that the product data will be maintained via Research Development Test and Evaluation (RDTE) funded engineering services or similar approaches. Post production and fielding phases also require that the product data be maintained via Sustainment Systems Technical Support (SSTS).

Appendix G - Life cycle Access and Use of Data

The PM must determine how the program will make the data available for use by appropriate organizations and persons during the life cycle. Life cycle data access and use planning includes an analysis of the various IT systems to be used.

General

Some of the data acquired for a new acquisition program will reside in one or more Government data repositories and some will exist with the various industry partners. Users are frequently unaware that needed data exists and subsequently expend valuable time and resources trying to recollect existing data. If users know the data exists, they are often unable to access it due to security, technical, or organizational boundaries. Finally, when users can access needed data, they may find the data unusable due to a lack of understanding of what the data means or the structure of the data. Life cycle access and use of data involves leveraging existing data by:

1. Locating the required data wherever it resides.
2. Obtaining the ability to access or obtain the data where it resides both legally and technologically.
3. Utilizing metadata tags and data mining techniques to understand the data and to combine or integrate different data sets from different repositories into new data sets to fulfill new data needs.
4. Maintaining configuration control of the master copy of all accessed or shared data.

Army approaches to Knowledge Management and enterprise Information Technology

Data management is a foundation element expected to support overall knowledge management and enterprise information technology objectives. As the Department of Defense and Services work toward supporting their respective and collective missions by incorporating enterprise strategies and widespread deployment of tools, it is of vital importance that the relationship between the data management strategies and higher level Army and DoD Knowledge Management and Enterprise IT guidance be taken into account. The data management strategy must adhere to Army KM and IT sustainment objectives in keeping with AR 25-1: Army Knowledge Management and Information Technology Management and the Army Knowledge Management Principles (Established via DA memorandum, 23 July 2008, SUBJECT: Army Knowledge Management Principles).

References Derived from the Army KM Principles:
AR 5-24: Management Improvement and Productivity Enhancement in the Department of the Army
AR 10-87: Army Commands, Army Service Component Commands, and Direct Reporting Units
AR 11-7: Internal Review and Audit Compliance Program
AR 11-33: Army Lessons Learned Program (ALLP)
AR 25-2: Information Assurance

AR 70-1: Army Acquisition Policy
AR 70-38: Research, Development, Test, and Evaluation of Materiel for Extreme Climatic Conditions
AR 71-9: Materiel Requirements
AR 700-8: Logistics Planning Factors and Data Management

Army has several enterprise IT initiatives underway to provide an ability to manage the data associated with acquisition program life cycle. Most of the initiatives have a stated goal of being the common IT tool and repository for certain segments of product data for certain functional user groups or activities. Examples of these enterprise initiatives include (but are not limited to) the Single Army Logistics Enterprise (SALE), the Acquisition Business System (AcqBiz), the AMC enterprise Product Data Management (ePDM) initiative, and the Logistics Data Warehouse initiative.

Access to existing data

Once the Program Manager has determined the data needed by the Government, a decision should be made regarding how best to access or obtain it. If the decision is made to access data resident in other IT systems, then the program office should work with the owners of those systems to establish the electronic connections and accesses needed. If data is to be exchanged between IT systems then use of industry data exchange standards can help minimize the time and cost associated with these interchanges.

Contractor IT systems

In the case of contractor IT systems, provisions that address several aspects related to Government access should be included in the contract. These aspects include:

1. Defining the data to be accessed.
2. Determining the time periods during which data will be accessible.
3. Specifying the required or acceptable data formats.
4. Addressing the type of data access protocols to be used.
5. Determining the protection required for the overall system security, classified data, sensitive but unclassified data (e.g., proprietary data).
6. Identification of access rights, rights to use the data.
7. Specifying any additional data services to be provided (e.g., interfaces for seamless Government access, maintain the systems, and the data to be accessed).
8. See DFARS 227.7108 for additional current policy and guidance.

Similar understandings should be reached with operators of other Government IT systems housing data. A “Memorandum of Understanding,” rather than a contract, is the recommended document to establish the parameters and conditions for data access with other Government IT systems.

Organization's access

Numerous organizations (i.e., designers, manufacturers, maintainers, testers, etc.) need access to or interoperability with data related to many programs. Unless these organizations can access, manipulate, organize, and utilize the data, the necessary functionality and efficiency cannot be achieved. For these organizations, commonality in the form and format of the data exchanged is often a key element to this interoperability. Organizations requiring access to data and rights to use the data from other programs are responsible for making their requirements known. PMs should be sensitive to these requirements and establish the data structures, relationships, and functional capabilities necessary to support these requirements. To the extent practical, these organizations should work with the requisite program offices to establish the necessary data access/exchange conventions. PMs should support these standardization efforts whenever possible. However, non-DoD and non-Government entities may be subject to additional restrictions regarding access due to contractor data rights markings and Distribution Statement (DoDD 5230.24) markings.

Configuration control of shared data

A problem created by widespread access to or sharing of data is the difficulty in identifying and controlling the configuration of the original "master" data. While access to data may be given to several users or organizations, access is usually not provided directly to the master copy of the data. A copy is made available for common access or sharing, and the master copy is tightly controlled in a restricted access repository or vault. Data provided for access or sharing should have metadata tags or other information that identifies the custodian or the master copy. Any changes to the data should be coordinated with the data owner or be identified as changed from the original data.

Appendix H - Required Resources and Risk Assessment

In the program DMS the PM should define the anticipated resources needed to secure and maintain data necessary to support a acquisition program or item throughout its life cycle, and identify risks to the program and to the Service if any of the planned actions or approaches are not carried out or adequately resourced.

Data Acquisition Costs

Generally the cost to the Government of acquiring its "automatic and "default" rights to and delivery of most product data (such as FFF and IOMT) in contractor format will be at or near zero. For data routinely used or generated by the contractor to perform the contract, the cost is "priced-in" at award and only the administrative costs to copy and to review data for authorized assertions and markings are incurred when the Government orders additional deliveries in contractor format. The only significant exceptions are commercial computer software and DMPD pertaining to an ICP where development of the DMPD was exclusively funded by the private sources. While the Government may (and should) order delivery of a "copy" of such DMPD and computer software without significant costs, the "data rights" in such computer software and DMPD must be separately negotiated and at a cost.

The PM must be mindful that contractors will desire to exclude certain ICPs from Government funding which may enable them to claim development of the ICP exclusively at private expense and potentially limit procurement and sustainment alternatives to sole source. One such contractor approach is to exclude certain development from the scope of the contract and then to fund it under IR&D. Any such anticipated or proposed funding of systems, subsystems, or ICPs outside the planned Government contract(s) shall be fully disclosed and justified. Such short-term program cost avoidance choices can result in significant long-term added costs. Government auditors should be tasked to carefully review the contractor's cost accounting standards (CAS) procedures and practices regarding the allocation of costs between IR&D programs and ongoing Government contracts.

Data Maintenance Costs

The DMS should also discuss the plan to fund the maintenance of the product data throughout the life cycle and the efforts to monitor and control data quality as an attribute of the Systems Engineering (SE) process such that post-production ECPs and related costs are minimized.

The accuracy and currency of the product data, in general, is critical to the product's future use and availability. The PM should plan for the maintenance of the product's product data after its delivery. During program development, it is expected that the product data will be maintained via Research Development Test and Evaluation (RDTE) funded engineering services or similar approaches. Post production and fielding phases also require that the product data be maintained via SSTS funds.

Data Risk Assessment

This section of the DMS should also identify the risks, and consequences of the risks where there is a gap between the data rights needed for competitive development, production and/or support efforts and the presently available (or anticipated future) data rights. The following common risks, if applicable to a given program, should be addressed.

- *Acquisition of product data for Competitive Prototyping Contract*: The DoDI 5000.02 requires competitive prototyping as part of the Acquisition Strategy and Technology Development Strategy. The decision to have multiple contractors competing within the Materiel Solution Analysis and the Technology Development Phases requires a strategic approach to determining which product requirements and design concept related data should be acquired. The decision to acquire or not acquire the data carries potential risk with either decision.
- *Affordability Risk*: Often times product data risks are defined in terms of initial cost or affordability. If product data costs, rights, accuracy and delivery are carefully planned and investigated by the PM, risks associated with acquiring product data and securing the Government's data rights are likely to be minimal or non-existent with the exception of commercial computer software and DMPD. The statute and DFARS provides ample leverage such that cost and affordability issues can be mitigated for all FFF and IOMT data (excluding DMPD for ICPs developed exclusively with private funding).
- *Product Data Access Risk*: Vendors who threaten no-bid or arbitrarily become hostile when the Government pursues product data threatens the Government's responsibility to adequately support the product. To mitigate this risk, the PM should be prepared to communicate this as an issue to the PEO, Overarching Integrated Program Team (OIPT), or Defense Acquisition Board (DAB) venues. Remember that the Government requires a copy of all product data (even without competitive rights) in order that the statutorily and contractually authorized emergency repairs and overhauls by third parties and the Government can be accomplished.
- *Product Data Maintenance Cost Risk*: The maintenance primarily of Engineering and Design product data is a consequence of product changes. The mitigation of this risk is to implement strong SE process that enforces the processes to ensure the accuracy and fidelity of the product data required to define and support the system/product. Management of data costs are NOT driven by the quantity of data received but by the quality of data that the Government needs to manage for Government purposes.
- *Product Data Storage Cost Risk*: Another legacy risk area that has historically been assigned to product data delivery is the "bricks and mortar" costs of housing and maintaining the data in a government repository. Advancements in IT infrastructure and capabilities are driving down the cost such as with commercial product data management (PDM) systems.
- *Product Data Format Risk*: Product data that is stored in repositories must be retrievable, 15, 20 or more years in the future. If the PM desires delivery of the product data in a native CAD or other unique formats, then the long term efforts to migrate the data to newer versions of the formats should be addressed here.

Consequences of Not Acquiring Product Data

This section of the DMS will describe the impacts to the viable production and sustainment alternatives (and life cycle cost impacts associated with noncompetitive alternatives) which result from the failure or decision to not acquire the program's product data and to secure the Government's rights in that product data. Areas of risk to be assessed include limited production sources, increased re-procurement costs, limited logistics support options, increased logistics support costs, inability to adequately address parts obsolescence issues and environmental/ESOH regulatory requirements, and the inability to organically or competitively handle acquisition program's RESET or RECAP initiatives.

Appendix I - DMS Worksheet Tool

A spreadsheet file has been created that will assist in the information gathering necessary to support the creation of a program data management strategy.

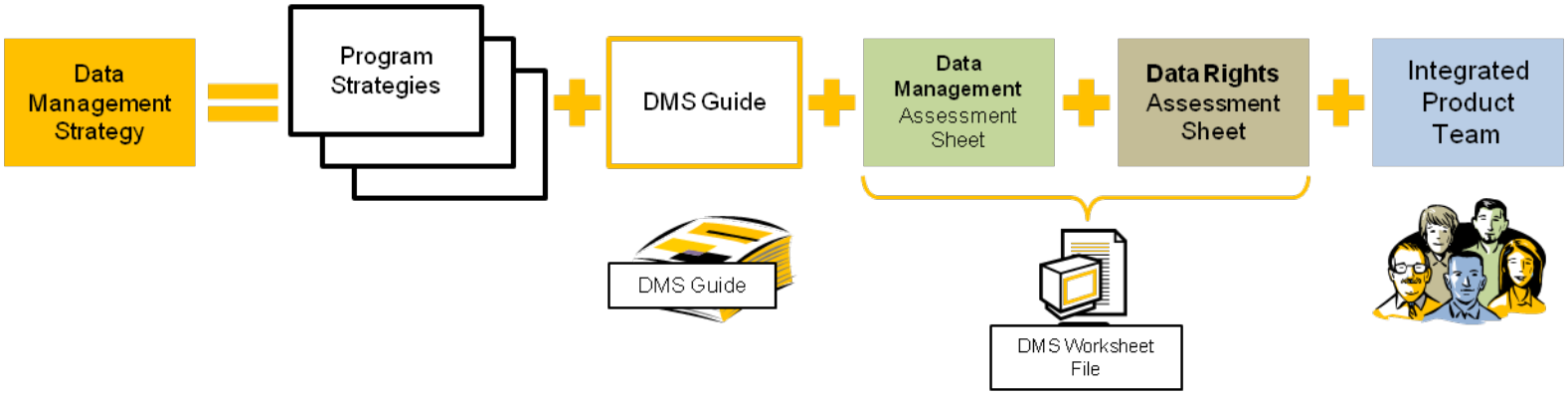
The file consists of tabbed sheets for instructions, Data Rights Assessment, Data Management Assessment and additional information that may be helpful to prepare the data management strategy. A number of diagrams on the following pages are shown as an introduction to the worksheet tool.

Figure 8 depicts the different program strategy documents, reference documents (like the DMS Guide), and support tools (such as the DMS Worksheet and DMS IPT) that serve as components of DMS development.

Figure 9 is a summary description of the Data Rights Assessment Sheet (a.k.a. Data Rights Sheet) contained in the DMS worksheet file.

Figure 10 is a summary description of the Data Management Assessment (a.k.a. Data Management Sheet) contained in the DMS worksheet file.

Components of DMS Development



Data Management Assessment	Tool to *Identify* weapon system *Data Requirements* and assess the Acquisition, Management, and Use of Product Data throughout the lifecycle.
Data Rights Assessment	Tool to identify and assess Government procurement rights. Focuses on the COMPONENTs of the Weapon System.

Figure 8 - Components of DMS Development

Data Rights Sheet

This spreadsheet goes through the components/sub-systems of the weapon system and asks about responsibility, data rights needed, and data rights issues.

The primary goals of this spreadsheet are:

1. Identify whether the Government or a contractor is responsible for that component/sub-system.
2. Identify potential or actual data rights issues
3. Outline plans to address rights issues
4. Assess risks associated with data rights

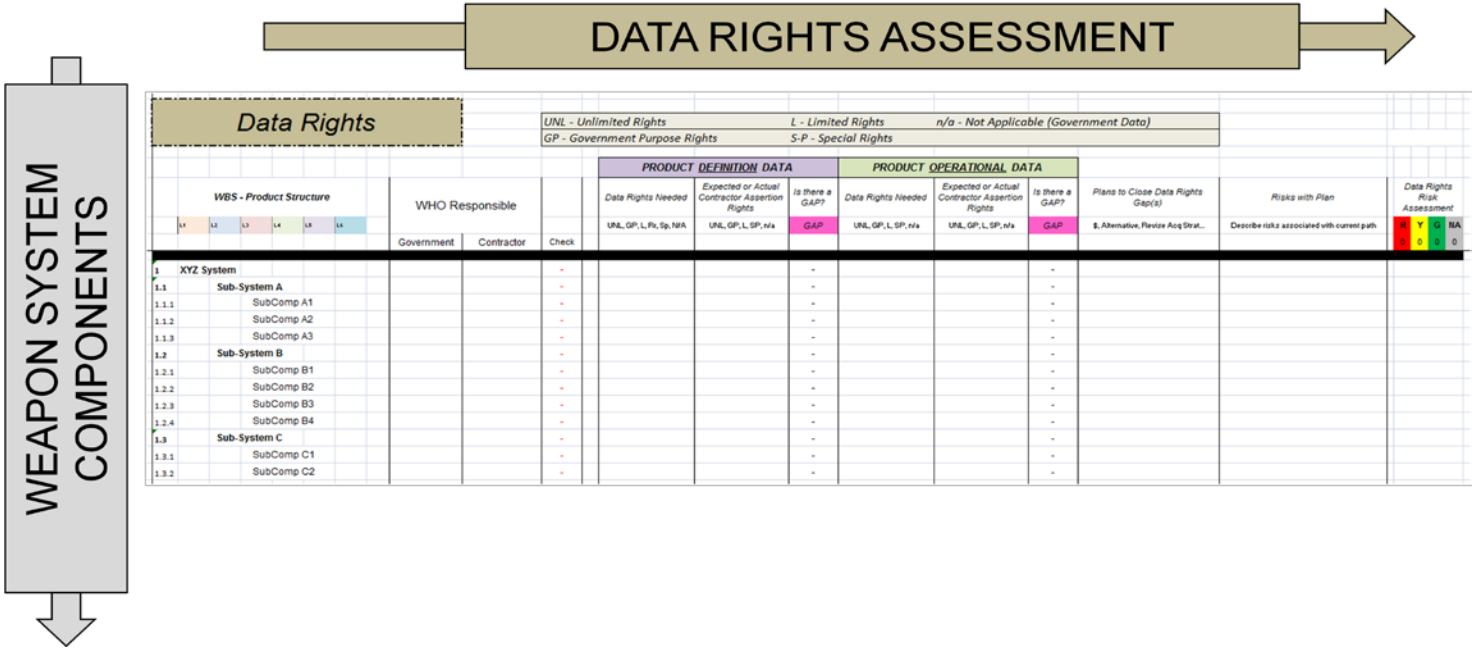


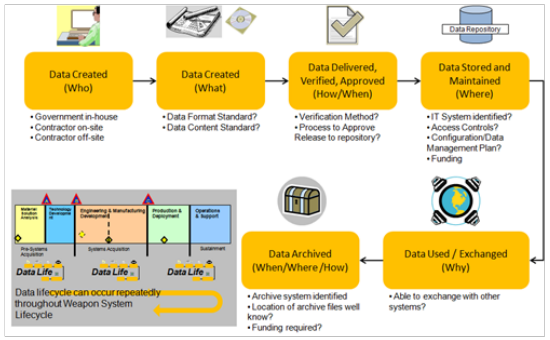
Figure 9 - Data Rights Tool Introduction

Data Management Sheet

This spreadsheet goes through each set of data (Product Definition, Product Operational, and Associated) and steps through each phase of the data lifecycle (shown at right).

Three primary goals of this spreadsheet are:

1. Identify what data is needed to support the weapon system and who needs it.
2. Determine how the data will be formatted, delivered, stored, and used throughout the lifecycle.
3. Assess risks associated with the product data.



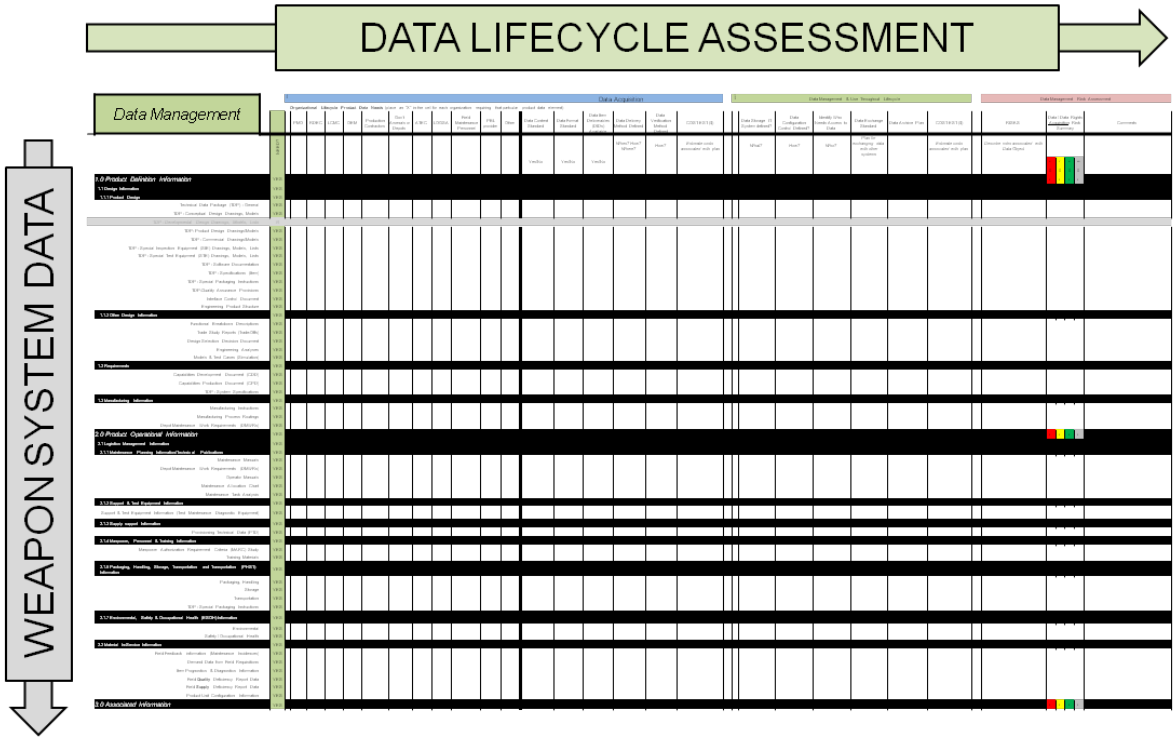


Figure 10 - Data Life cycle Management Tool Introduction

Appendix J - Acronyms

The following acronyms are used within this document.

ACAT	- Acquisition Category
AcqBiz	- Acquisition Business System
ACC	- Army Contracting Command
AR	- Army Regulation
ARN	- Additional rights negotiations
AS	- Acquisition Strategy
ASME	- American Society of Mechanical Engineers
ATEC	- Army Test & Evaluation Command
CAD	- Computer Aided Design
CAS	- Cost Accounting Standards
CBM	- Condition Based Maintenance
CDD	- Capabilities Development Document
CDR	- Critical Design Review
CDRL	- Contract Data Requirements List
CPD	- Capabilities Production Document
CS	- Computer Software
CSD	- Computer Software Documentation
CSP	- Competitive Sourcing Proposal
DA	- Department of the Army
DAB	- Defense Acquisition Board
DAG	- Defense Acquisition Guide

DID	- Data Item Description
DFARS	- Defense Federal Acquisition Regulation Supplement
DLA	- Defense Logistics Agency
DMPD	- Detailed Manufacturing or Process Data
DMS	- Data Management Strategy
DMWR	- Depot Maintenance Work Requirements
DoD	- Department of Defense
DoDD	- DoD Directive
DoDI	- DoD Instruction
DBSMC	- Defense Business System Management Council
DT&E	- Developmental Test and Evaluation
ECP	- Engineering Change Proposal
EMD	- Engineering & Manufacturing Development
ePDM	- enterprise Product Data Management
ERR	- Engineering Release Record
ESOH	- Environmental Safety and Occupational Health
ETM	- Electronic Technical Manual
FAR	- Federal Acquisition Regulations
FFF	- Form, Fit, and Function
FOC	- Full Operational Capability
FRP	- Full Rate Production
GFE	- Government Furnished Equipment
GFI	- Government Furnished Information
GIDEP	- Government Industry Data Exchange Program
GPR	- Government Purpose Rights

GSC	- Government Support Contractors
HCA	- Head of the Contracting Activity
HSI	- Human Systems Integration
IAW	- In accordance with
ICP	- Items, Components, or Processes
IDE	- Integrated Data Environment
IETM	- Interactive Electronic Technical Manual
IOC	- Initial Operational Capability
IOMT	- Installation, Operation, Maintenance, and Training
IPT	- Integrated Product/Process Team
IR&D	- Independent Research and Development
IT	- Information Technology
IUID	- Item Unique Identification
J&A	- Justification and Approval
LCMC	- Life Cycle Management Command
LCSP	- Life Cycle Sustainment Plan
LIW	- Logistics Information Warehouse
LMI	- Logistics Management Information
LMP	- Logistics Modernization Program
LOGSA	- U.S. AMC Logistics Support Activity
LR	- Limited Rights
LRIP	- Low Rate Initial Production
MDR	- Milestone Decision Review
MIL-HDBK	- Military Handbook
MIL-STD	- Military Standard

MS	- Milestone
NDA	- Non-Disclosure Agreement
NMWR	- National Maintenance Work Requirements
OEM	- Original Equipment Manufacturer
OIPT	- Overarching Integrated Program Team
OMB	- Office of Management and Budget
OSD	- Office of the Secretary of Defense
OT&E	- Operational Test & Evaluation
PBL	- Performance Based Logistics
PCB	- Product Configuration Baseline
PDM	- Product Data Management
PDR	- Preliminary Design Review
PEO	- Program Executive Officer
PEWG	- Product Data and Engineering Work Group
PFI	- Physically and Functionally Interchangeable
PHST	- Packaging, Handling, Storage, and Transportation
PM	- Program/Project Manager
POC	- Point of Contact
QA	- Quality Assurance
RDEC	- Research, Development & Engineering Center
RDTE	- Research Development Test and Evaluation
RR	- Restricted Rights
SALE	- Single Army Logistics Enterprise
SBIR	- Small Business Innovative Research
SE	- Systems Engineering

SEP	- System Engineering Plan
SLR	- Special License Rights
SS	- Supportability Strategy
SSTS	- Sustainment Systems Technical Support
S&T	- Science and Technology
STEP	- Standard for the Exchange of Product model data
TD	- Technical Data
TDP	- Technical Data Package
TDS	- Technology Development Strategy
UR	- Unlimited Rights
U.S.C.	- United States Code
WBS	- Work Breakdown Structure