SL150-AA-PRO-010/DMP

REVISION 2

NAVSEA
DATA MANAGEMENT PROGRAM

OPERATIONS AND PROCEDURES MANUAL
FOR CONTRACTOR PREPARED DATA

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

PUBLISHED BY DIRECTION OF COMMANDER, NAVAL SEA SYSTEMS COMMAND

NSN 0910-LP-109-1372 1 JUNE 2009

FOREWORD

1. This manual may be used by all Departments and Agencies of the Department of Defense (DoD).

2. This manual identifies requirements and provides common guidance for the acquisition and management of contractor prepared data within DoD. This manual is applicable to all forms of data whether it is digital, hard copy, or data to which access via contractor provided digital information services is required.

3. This guidance identified in this document provides information necessary to meet public law requirements tied to acquisition data management.

4. Comments, suggestions, or questions on this document should be addressed to: Commander, Naval Sea Systems Command, ATTN: SEA 04L1, 1333 Isaac Hull Avenue, SE, Stop 5160, Washington Navy Yard, D.C. 20376-5160.

CONTENTS

PARAGRAPH PAGE

1. SCOPE 1
   1.1 Scope 1
2. APPLICABLE DOCUMENTS 1
   2.1 General 1
   2.2 Government documents 1
      2.2.1 Specifications, standards, and handbooks 1
      2.2.2 Other Government documents, drawings, and publications 1
   2.3 Non-Government publications 2
3. DEFINITIONS 3
   3.1 Definitions 3
      3.1.1 Acceptance 3
      3.1.2 Access 3
      3.1.3 Accredited Standards Committee X12 (ASC X12) 3
      3.1.4 Acquisition 3
      3.1.5 Acquisition managers 3
      3.1.6 Acquisition Plan (AP) 3
      3.1.7 Acquisition planning 3
      3.1.8 Acquisition program 3
      3.1.9 Acquisition Strategy (AS) 3
      3.1.10 Armed services board of contract appeals (ASBCA) 4
      3.1.11 Acquisition Streamlining and Standardization Information System (ASSIST) 4
      3.1.12 Capability Development Document (CDD) 4
      3.1.13 Capability Production Document (CPD) 4
      3.1.14 Computer Graphics Metafile (CGM) 4
      3.1.15 Concept Decision (CD) 4
      3.1.16 Concept Refinement (CR) 4
      3.1.17 Configuration Management (CM) 4
      3.1.18 Contract 4
      3.1.19 Contract data 5
      3.1.20 Contract data requirements 5
      3.1.21 Contract Data Requirements List (CDRL) 5
      3.1.22 Contract Line Item Number (CLIN) 5
      3.1.23 Contract requirements 5
      3.1.24 Contractor rights in technical data 5
      3.1.25 Controlling DoD office 5
      3.1.26 Cryptographic logic 5
      3.1.27 Current Document Change Authority (CDCA) 5
      3.1.28 Data 5
      3.1.29 Data acquisition document 5
      3.1.30 Data approval 5
      3.1.31 Developed exclusively at private expense 5
      3.1.32 Developed Exclusively with Government funds 5
      3.1.33 Developed with mixed funding 5
      3.1.34 Data call 6

PARAGRAPH PAGE

3.1.35 Data format 6
3.1.36 Data item 6
3.1.37 Data Item Description (DID) 6
3.1.38 Data Management (DM) 6
3.1.39 Data manager 6
3.1.40 Data-of-record 6
3.1.41 Data product 6
3.1.42 Data Requirements Review Board (DRRB) 6
3.1.43 Data rights 6
3.1.44 Data rights validation 6
3.1.45 Data view 6
3.1.46 Defense acquisition system 6
3.1.47 Defense Automatic Addressing System Center (DAASC) 6
3.1.48 Defense Information Technology Standards Registry (DISR) 7
3.1.49 Defense system 7
3.1.50 Defense system data 7
3.1.51 Defense system life cycle 7
3.1.52 Deferred delivery 7
3.1.53 Deferred ordering 7
3.1.54 Delivery 7
3.1.55 Department of Defense FAR Supplement (DFARS) 7
3.1.56 Design Readiness Review (DRR) 7
3.1.57 Digital data approach and implementation plan 7
3.1.58 Digital format 7
3.1.59 Distribution 7
3.1.60 Distribution statement 7
3.1.61 Document 7
3.1.62 Document Type Definition (DTD) 7
3.1.63 DoD clearance office 8
3.1.64 DoD components 8
3.1.65 Electronic Data Interchange (EDI) 8
3.1.67 Extensible Markup Language (XML) 8
3.1.68 Extensible Stylesheet Language (XSL) 8
3.1.69 Federal Acquisition Regulation (FAR) 8
3.1.70 Final review 8
3.1.71 Focal point 8
3.1.72 Full Operational Capability (FOC) 8
3.1.73 Full Rate Production (FRP) 8
3.1.74 Functional Requirements Authentication Board (FRAB) 8
3.1.75 Generated 9
3.1.76 Government Concept of Operations (GCO) 9
3.1.77 Government purpose rights 9
3.1.78 Implementation Conventions (ICs) 9
3.1.79 Independent Verification and Validation (IV&V) 9
3.1.80 Indexing 9
3.1.81 Information Technology (IT) 9

PARAGRAPH PAGE

3.1.82 Infrastructure 9
3.1.83 Initial Operational Capability (IOC) 9
3.1.84 Initial Operational Test and Evaluation (IOT&E) 9
3.1.85 Initial provisioning 9
3.1.86 In-Process Review (IPR)..... 9
3.1.87 In-Service Engineering Agent (ISEA)..... 9
3.1.88 Inspection..... 10
3.1.89 Integrated Digital Environment (IDE)..... 10
3.1.90 Integrated Digital Data Environment (IDDE) 10
3.1.91 Integrated Logistics Support (ILS)..... 10
3.1.92 Integrated Logistics Support Plan (ILSP)..... 10
3.1.93 Integrated Product Team (IPT)..... 10
3.1.94 Intellectual property 10
3.1.95 Inventory Control Point (ICP)..... 10
3.1.96 Joint Engineering Data Management Information and Control System (JEDMICS)..... 10
3.1.97 Legacy data 10
3.1.98 Limited rights 10
3.1.99 Military Engineering Data Asset Locator System (MEDALS)..... 10
3.1.100 Milestones (MS)..... 11
3.1.101 Milestone Decision Authority (MDA) 11
3.1.102 Military Critical Technologies List (MCTL)..... 11
3.1.103 Metadata..... 11
3.1.104 Munitions List (ML)..... 11
3.1.105 National Item Identification Number (NIIN) 11
3.1.106 National Stock Number (NSN)..... 11
3.1.107 Non-Disclosure Agreement (NDA) 11
3.1.108 Non-Government Standard (NGS) 11
3.1.109 One-time DID..... 11
3.1.110 Operations and support..... 11
3.1.111 Ordering data..... 12
3.1.112 Organizational data manager..... 12
3.1.113 Packing, Handling, Storage, and Transportation (PHST)..... 12
3.1.114 Performance 12
3.1.115 Performance specification 12
3.1.116 Performance Work Statement (PWS)..... 12
3.1.117 Personal Identification Number (PIN) 12
3.1.118 Prime contract 12
3.1.119 Prime contractor 12
3.1.120 Procurement Request (PR) 12
3.1.121 Procuring Contracting Officer (PCO) 12
3.1.122 Product data..... 12
3.1.123 Product definition data 12
3.1.124 Production and Deployment (P&D) 13
3.1.126 Program office..... 13
3.1.125 Program Manager (PM)..... 13
3.1.127 Proprietary rights..... 13

PARAGRAPH PAGE

3.1.128 Provisioning 13
3.1.129 Purchase Order (PO) 13
3.1.130 Quality Assurance (QA) 13
3.1.131 Repair 13
3.1.132 Repair parts 13
3.1.133 Repairable item 13
3.1.134 Repurchase data 13
3.1.135 Re-procurement 13
3.1.136 Schemas 13
3.1.137 Secondary distribution 14
3.1.138 Small Business Innovation Research (SBIR) 14
3.1.139 Solicitation 14
3.1.140 Spare parts 14
3.1.142 Special license rights 14
3.1.142 Specification 14
3.1.143 Standard 14
3.1.144 Standard for the Exchange of Product Model Data (STEP) 14
3.1.145 Statement of Objectives (SOO) 14
3.1.146 Statement of Work (SOW) 14
3.1.147 Subcontractor 14
3.1.148 Submittal 14
3.1.149 Subsystem 14
3.1.150 Supply support 14
3.1.151 Sustainment 15
3.1.152 System Demonstration (SD) 15
3.1.153 System Development and Demonstration (SDD) 15
3.1.154 Systems Engineering (SE) 15
3.1.155 System Engineering Management Plan (SEMP) 15
3.1.156 System Integration (SI) 15
3.1.157 Tailoring 15
3.1.158 Technical data 15
3.1.159 Technical Data Package (TDP) 15
3.1.160 Technical Manual (TM) 16
3.1.161 Technical Manual Contract Requirements (TMCR) 16
3.1.162 Technical Order (TO) 16
3.1.163 Technology development 16
3.1.164 Test and Evaluation Master Plan (TEMP) 16
3.1.165 Unlimited rights 16
3.1.166 Validation 16
3.1.167 Verification 16
3.1.168 Virtual acquisition 16
3.1.169 Warranty of data 16
3.1.170 World Wide Web (WWW) Consortium (W3C) 16
3.2 Acronyms 17
4. GENERAL 20
4.1 Applicability 20

PARAGRAPH PAGE

4.1.1 Intended audience ... 20
4.2 Objectives ... 21
4.2.1 Guidance ... 21
5. DATA MANAGEMENT (DM) DUTIES AND RESPONSIBILITIES ... 21
5.1 Data manager ... 21
5.2 Principles ... 21
5.3 Component level ... 21
5.4 Issues ... 22
5.5 Framework ... 22
FIGURE 1 Defense acquisition management system ... 22
5.5.1 DM guidance documents ... 23
FIGURE 2 The structure of data acquisition guidance ... 23
5.5.2 Relation to guidance documents ... 23
FIGURE 3 Implementation of joint data management document ... 24
5.6 Roles ... 24
5.7 Use of specifications and standards in acquisition ... 24
5.7.1 Background ... 24
5.7.2 Policy ... 24
5.7.3 Non-Government Standards (NGSs) Guidance ... 25
5.7.3.1 NGSs ... 25
5.7.3.2 Use of NGSs ... 25
5.8 Training ... 25
6. PLANNING FOR ACQUISITION OF DATA ... 25
6.1 General ... 25
6.1.1 DM ... 25
6.2 Acquisition Strategy (AS) ... 25
6.2.1 Framework of AS ... 26
6.3 Acquisition Planning (AP) ... 26
6.3.1 Objectives of AP ... 26
6.4 Data Acquisition Strategy (DAS) ... 26
6.4.1 Strategy ... 26
6.4.2 DAS process ... 26
6.4.3 In-Process Reviews (IPR) ... 26
6.4.4 DAS considerations ... 27
6.5 Relationship between program and data acquisition strategy ... 27
6.5.1 Acquisition program ... 27
6.5.2 Planning ... 27
6.5.3 Scheduling ... 27
6.5.4 AS elements ... 27
6.5.5 Major milestones ... 27
6.5.5.1 Data acquisition and management life cycle ... 28
FIGURE 4. Acquisition milestones within the acquisition process ... 28
6.5.6 Milestones and overall program schedule ... 28
6.5.6.1 Program schedule ... 28
6.5.6.2 Other activities ... 29
FIGURE 5 Typical contract awards during a defense system life cycle ... 29

PARAGRAPH PAGE

6.5.6.3 Defense and data life cycle relationship 29
6.6 Integrated Logistic Support Plan (ILSP) 29
6.7 Acquisition team 29
6.8 Support contractors 30
7. DATA REQUIREMENTS 30
7.1 Defense system data 30
7.1.1 Program office responsibility 30
7.1.2 Generating requirements 30
7.1.3 Data acceptability 30
FIGURE 6 Relationships between data acquisition document 31
7.2 Major data acquisition documents 31
7.2.1 General 31
7.2.2 Statement of Objectives (SOO) 31
7.2.3 Statement of Work (SOW) 32
7.2.4 Contract Data Requirement Lists (CDRLs), DD Form 1423 32
7.3 Identification of data requirements 32
7.3.1 General 32
7.3.2 Data call 32
7.3.2.1 Time frame for data call 32
7.3.2.2 Program information 33
7.3.2.3 User information 33
7.3.2.4 Functional areas 33
7.3.2.5 Identifying the data manager 33
7.3.2.6 Additional data calls 33
7.3.2.7 Final data call 33
FIGURE 7 Personnel required to generate data requirements 33
7.3.3 Data call responses 34
7.3.4 Integrated Product Teams (IPTs) 34
7.3.4.1 IPT members 34
7.3.4.2 IPT requirements identification 34
7.3.5 Consolidation of data requirements 34
7.3.6 Data Requirements Review Board (DRRB) 34
7.3.6.1 DRRB membership 34
7.3.6.2 DoD components 34
7.3.6.3 DRRB function 34
7.3.6.4 DRRB threshold 35
7.3.7 Data manager roles and responsibilities 35
8. DIGITAL FORMATS 35
8.1 General 35
8.2 Formats 35
8.2.1 Neutral formats 35
8.2.2 Native formats 35
8.2.3 Organizational standard formats 36
8.3 Data and technical data types 36
FIGURE 8 Relationship between the types of data and technical data 36
8.4 Summary of data formats and conventions 37

PARAGRAPH PAGE

8.4.1 Types of data 37
TABLE I Sampling of types of data and related standards 37
9. GOVERNMENT LICENSE RIGHTS IN TECHNICAL DATA & COMPUTER SOFTWARE 38
9.1 General 38
9.2 Data license rights: Automatic and based on funding 38
9.3 Delivery of data and contract procedures 38
9.4 Data license rights categories 38
9.4.1 Unlimited rights in technical data and computer software 38
9.4.2 Government purpose rights in technical data and computer software 38
9.4.3 Limited rights in technical data and computer software 38
9.4.4 Restricted rights in technical data and computer software 38
9.4.5 Special license rights in technical data and computer software 39
9.5 Procedural processes 39
9.5.1 Asserting 39
9.5.2 Marking 39
9.6 Correcting assertions & markings 39
10. DATA MARKING 39
10.1 Distribution statements on technical data 39
10.2 Export control-warning notice 40
10.3 Foreign disclosure 40
10.4 Marking requirements 40
10.5 Responsibility for marking 40
10.6 Destruction and handling 41
10.7 Changes to markings 41
10.7.1 Controling DoD activity 41
11. DATA PRICING 41
11.1 General 41
11.1.1 Price estimates 41
11.1.2 Pricing goals 41
11.1.3 Offerors 41
11.2 Pricing CDRL items 41
11.2.1 Retention of pricing information 42
12. WARRANTY OF DATA 42
12.1 General 42
13. DATA INTEGRATION AND SHARING 42
13.1 General 42
13.2 Availability of existing data 42
13.2.1 Military Engineering Data Asset Locator System (MEDALS) 42
13.2.1.1 MEDALS index entries 42
13.2.2 DoD evolving enterprise effort 43
13.2.2.1 Implementation of Net-Centric Enterprise Services (NCES) 43
13.3 Access to existing data 43
13.3.1 Contractor IT systems 43
13.3.2 Organization's access 43
13.4 Data integration 43
13.4.1 Database accesses 44
13.5 Configuration control of shared data 44
14. LEGACY DATA 44

PARAGRAPH PAGE

14.1 General ... 44
14.2 Planning for legacy data and systems ... 44
14.2.1 Risks for legacy data and systems ... 44
14.2.2 Regulatory requirements for legacy data ... 44
14.3 Cost benefits analysis for data conversion ... 44
15. DATA INFRASTRUCTURE ... 44
15.1 General ... 44
15.1.1 Integrated DM system ... 45
15.2 Government Concept of Operations (GCO) for IDDE ... 45
15.2.1 GCO in DM ... 45
15.2.2 GCO criteria ... 45
16. DATA ACCESS VERSUS DELIVERY ... 45
16.1 General ... 45
16.1.1 Online accessibility ... 46
16.1.2 Data delivery ... 46
16.1.3 Electronic Data Interchange (EDI) ... 46
16.1.4 Data transfer approaches ... 46
16.2 Transition steps to an IDDE ... 46
16.2.1 Security precautions ... 46
16.2.1.1 Formal EDI environments ... 46
16.2.1.2 Informal EDI environments ... 47
16.2.2 Digital signature ... 47
16.2.3 Receipt notice ... 47
16.2.4 Environment ... 47
16.2.5 Acceptance notice ... 47
16.2.6 Data content ... 47
16.2.7 Paperless delivery ... 47
16.2.8 Approach to data delivery ... 47
16.2.9 Use of open system, standard based methods ... 47
16.3 Decision methodology ... 47
16.3.1 Management endorsement ... 47
16.3.2 The contractor ... 48
16.3.3 The EDI team ... 48
16.3.4 The implementation plan ... 48
16.3.5 The groundwork ... 48
16.3.6 The connections ... 48
16.3.6.1 Method of data exchange ... 48
16.3.6.1.1 Formal data exchange ... 49
16.3.6.1.2 Informal data exchange ... 49
16.3.6.2 Contractor EDI files ... 49
16.3.6.3 Program office EDI files ... 49
16.3.7 Production mode ... 49
16.4 Deferred ordering and delivery ... 49
16.4.1 Contract methods ... 49
16.4.2 Delivery of technical data ... 49
17. INSPECTION, ACCEPTANCE, OR REJECTION OF TECHNICAL DATA ... 49

PARAGRAPH PAGE

17.1 General ... 49
17.2 Competitive procurement ... 49
17.3 Acceptance phases ... 49
17.3 Contractor responsibilities ... 50
17.5 Government responsibilities ... 50
17.5.1 Administration of contracts ... 50
17.5.2 Review, approval or rejection ... 50
17.6 Data requiring inspection and acceptance ... 50
17.6.1 Procedures for inspecting and accepting data ... 51
17.6.2 Guidance conference ... 51
17.6.3 Topics for guidance conference ... 51
18. PROTECTION AND RELEASE OF DATA ... 51
18.1 General ... 51
18.2 Authorities and processes ... 51
18.2.1 Arms Export Control Act (AECA), 22 U.S.C., sections 2751 ... 51
18.2.2 10 U.S.C., Section 130 FOIA exemptions ... 51
18.2.3 10 U.S.C. 2320, Rights in technical data ... 52
18.2.4 18 U.S.C. 1905, Disclosure of confidential information ... 52
18.2.5 5U.S.C. 552, Freedom of Information Act (FOIA) ... 52
18.3 Contractor & potential contractor requests for access ... 52
19. MANAGEMENT AND SUSTAINMENT OF DATA ... 52
19.1 General ... 52
19.2 Access to data ... 52
19.3 Maintenance of data and data systems ... 53
19.3.1 Data format ... 53
19.3.2 Data storage media ... 53
19.3.3 Data authoring applications ... 53
19.3.4 Data systems ... 53
19.4 Consideration of available data ... 53

APPENDIX A ... 54
A.1 SCOPE ... 54
A.1.1 Scope ... 54
A.2 LIST OF WEBSITES ... 54
A.2.1 List of websites ... 54

APPENDIX B ... 55
B.1 SCOPE ... 55
B.1.1 Scope ... 55
B.2 PREPARATION GUIDE ... 55
B.2.1 Contract data requirements list ... 55
DD Form 1423-1 Contract Data Requirements List (CDRL) ... 62

1. SCOPE

1.1 Scope. This manual provides a uniform approach within the Department of Defense (DoD) for the acquisition and management of contractor-prepared data. This document provides common policy, procedures, and processes by which data requirements will be made as uniform as possible on differing contracts from the DoD components, thereby reducing the burden upon the contractor in the preparation, delivery, or providing access and use of the data required by the Government. This manual is for guidance only and cannot be cited as a requirement.

2. APPLICABLE DOCUMENTS

2.1 General. The documents listed below are not necessarily all of the documents referenced herein, but are those needed to understand the information provided by this manual.

2.2 Government documents.

2.2.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified herein.

DEPARTMENT OF DEFENSE SPECIFICATIONS

MIL-DTL-31000 - Technical Data Packages

DEPARTMENT OF DEFENSE STANDARDS

MIL-STD-961 - Defense and Program-Unique Specifications Format and Content

MIL-STD-962 - Defense Standards Format and Content

MIL-STD-963 - Data Item Descriptions (DIDs)

DEPARTMENT OF DEFENSE HANDBOOKS

MIL-HDBK-61 - Configuration Management Guidance

MIL-HDBK-245 - Preparation of Statement of Work (SOW)

(Copies of these documents are available online at http://assist.daps.dla.mil/quicksearch/ or from the Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094.)

2.2.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified herein.

UNITED STATES CODE (U.S.C.)

U.S.C. Title 10 - Armed Forces

U.S.C. Title 22 - Foreign Relations and Intercourse

(Copies of these documents are available from the Superintendent of Documents, U.S. Government Printing Office, Washington DC 20401 or online at http://www.gpoaccess.gov/uscode/browse.html.)

DEPARTMENT OF DEFENSE DIRECTIVES

DoDD 5000.01 - The Defense Acquisition System

DoDD 5220.22 - National Industrial Security Program

DoDD 5230.24 - Distribution Statements on Technical Documents

DoDD 5230.25 - Withholding of Unclassified Technical Data

DoDD 5400.07 - DoD Freedom of Information Act (FOIA) Program

DEPARTMENT OF DEFENSE REGULATIONS

DoD 5200.1-R	-	Information Security Program
DoD 5400.7-R	-	DoD Freedom of Information Act Program Defense Federal Acquisition Regulation Supplement (DFARS)

DEPARTMENT OF DEFENSE INSTRUCTIONS

DoDI 5000.02	-	Operation of the Defense Acquisition System

(Copies of these documents are available online at http://www.dtic.mil/whs/directives/.)

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Executive Order 10865	-	Safeguarding Classified Information Within Industry
Executive Order 10909	-	Amendment of Executive Order 10865, Safeguarding Information Within Industry
Executive Order 12829	-	National Industrial Security Program

(Copies of these documents are available from the U.S. National Archives and Records Administration, 7th and Pennsylvania Avenue NW, Old Military and Civil Records Branch (NWCTB), Washington DC 20408 or online at http://www.archives.gov/federal-register/executive-orders/disposition.html.)

2.3 Non-Government publications. The following documents form a part of this document to the extent specified herein.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI/GEIA 859	-	Data Management
ANSI/EIA-649	-	National Consensus Standard for Configuration Management

(Copies of these documents are available from the American National Standards Institute, 25 W. 43rd St, 4th Floor, New York, NY 10036 or online at http://webstore.ansi.org/.)

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME)

ASME Y14.100	-	Engineering Drawing Practices

(Copies of this document are available from ASME International, 22 Law Drive, P.O. Box 2900, Fairfield, NJ 07007-2900 or online at www.asme.org.)

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ISO 10303	-	Standard for the Exchange of Product Model Data

(Copies of this document are available from ISO, 1, rue de Varembé, CH-1211 Geneva 20, Switzerland or online at www.iso.org.)

3. DEFINITIONS

3.1 Definitions. The definitions used in this manual are as follows:

3.1.1 Acceptance. The act of an authorized representative of the Government by which the Government, for itself, or as agent of another, assumes ownership of existing identified supplies tendered, or approves specific services rendered, as partial or complete performance of the contract.

3.1.2 Access. Addresses both informal and formal access to contractor furnished data. Informal access is usually the result of of non-binding agreements outside of the contract between the PM and the contractor. Under these informal access arrangements, the contractor voluntarily allows the PM to see and use the data beneficial to, but essential for, contract administration or oversight. Use of informal access to essential data is improper and unenforceable by the Government. Formal access is one method of contract "delivery" of data. As a"delivery," such formal access is contractually enforceable and it initiates critical contract procedures (assertion/marking/justification), which verify/establish the Government's rights to the delivered data. When used in this document, with regards to contractor furnished data, the term "access" must be understood to mean "formal access."

3.1.3 Accredited Standards Committee X12 (ASC X12). The Accredited Standards Committee Standard is a building block concept, which standardizes the essential elements of business transactions. The concept is similar to a "standard bill of material" and the "construction specifications," which give the architect flexibility in what can be designed with standardized materials and procedures. The Electronic Data Interchange (EDI) system designer, like the architect, uses the ASC X12 standards to build business transactions that are often different because of their function and yet utilize the ASC X12 standards. The "bill of material" and the "construction specification" of ASC X12 are the standards found in the published technical documentation. Major parts of the ASC X12 standards are described in technical documentation related to various aspects of electronic data interchange such as data elements; interchange control structure, application control structure, data segments, and security.

3.1.4 Acquisition. The acquiring by contract, with appropriated funds, of supplies or services by and for the use of the Government that are already in existence or should be created, developed, demonstrated, and evaluated. (Federal Acquisition Regulation [FAR] Subpart 2.101). This may include the conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support, modification and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in or in support of military missions.

3.1.5 Acquisition managers. Persons responsible at different levels for some activity related to developing, producing, and/or fielding an Automatic Information System or weapon system; including senior-level managers responsible for ultimate decisions, programs managers, and commodity or functional-area managers.

3.1.6 Acquisition Plan (AP). A formal written document reflecting the specific actions necessary to execute the approach established in the approved acquisition strategy and guiding contractual implementation. Refer to the FAR Subpart 7.1, the Defense Federal Acquisition Regulation (DFARS) Subpart 207.1.

3.1.7 Acquisition planning. The process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency need in a timely manner and at a reasonable cost. It is performed throughout the life cycle and includes developing an overall acquisition strategy for managing the acquisition and a written AP.

3.1.8 Acquisition program. An acquisition program is a directed, funded effort that provides a new, improved, or continuing material, weapon or information system or service capability in response to an approved need.

3.1.9 Acquisition Strategy (AS). A business and technical management approach designed to achieve program objectives within the resources constraints imposed. It is the framework for planning, directing, contracting for, and managing a program. It provides a master schedule for research, development, test, production, fielding, modification, post-production management, and other activities essential for program success. The acquisition strategy is the basis for formulating functional plans and strategies (e.g., Test and Evaluation Master Plan, AP, competition, systems engineering, etc.).

3.1.10 Armed Services Board of Contract Appeals (ASBCA). A board established to act as the authorized representatives of the Secretary of Defense (SECDEF) or department Secretaries, in deciding claims under the disputes clause of Government contracts.

3.1.11 Acquisition Streamlining and Standardization Information System (ASSIST). The ASSIST is a database system for DoD-wide standardization document information. ASSIST is located at the Document Automation and Production Service (DAPS), Philadelphia, PA. ASSIST-Online provides web-based access to digital documents on the ASSIST database. ASSIST is the official source of DoD specification and standards. Also, ASSIST provides online, interactive listing of source documents and Data Item Descriptions (DID) that DoD has approved for repetitive contractual application in DoD acquisitions and those that DoD has cancelled or superseded. ASSIST can be accessed at http://assist.daps.dla.mil (see Appendix A).

3.1.12 Capability Development Document (CDD). A document that captures the information necessary to develop a proposed program(s), normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of military useful, logistically supportable, and technically mature capability. The CDD supports a Milestone B decision review.

3.1.13 Capability Production Document (CPD). The production elements specific to a single increment of an acquisition program are addressed in this document. The CPD should be validated and approved before a Milestone C decision review. The refinement of performance attributes and Key Performance Parameters (KPPs) is the most significant difference between the CDD and CPD.

3.1.14 Computer Graphics Metafile (CGM). CGM has been an International Organization for Standardization (ISO) standard for vector and composite vector/raster picture definition since 1987. CGM has a significant following in technical illustration, interactive electronic documentation, geophysical data visualization, amongst other application areas and is widely used in the fields of automotive engineering, aeronautics, and the defense industry.

3.1.15 Concept Decision (CD). The first decision point of the Defense Acquisition Management Framework. It authorizes entry to the Concept Refinement (CR) phase. The principle document at this decision point is the Initial Capabilities Document (ICD), which also contains an approval plan for conducting an Analysis of Alternatives (AoA). A successful CD does not mean that a new acquisition program has been initiated since the funding is normally limited to the CR phase, which follows.

3.1.16 Concept Refinement (CR). The first phase of the Defense Acquisition Management Framework as defined and established by DODI 5000.02. The purpose of this phase is to refine the initial concept and develop a Technology Development Strategy (TDS). Entrance into this phase depends upon an approved ICD resulting from the analysis of potential concepts across the DoD components, international systems from Allies, and cooperative opportunities; and an approved plan for conducting an AoA for the selected concept, documented in the approved ICD. The milestone decision authority approval to begin CR does not constitute program initiation of a new acquisition program. CR phase ends when the Milestone Decision Authority (MDA) approves the preferred solution resulting from the AoA and approves the associated TDS.

3.1.17 Configuration Management (CM). A management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design and operational information throughout its life.

3.1.18 Contract. A mutually binding legal relationship that obligates the seller to furnish the supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modification.

3.1.19 Contract data. Contract data is data that is identified as a requirement in a solicitation and imposed in a contract, order, or agreement. Contract data is developed, generated, prepared, modified, maintained, stored, accessed, retrieved, distributed, managed, and/or delivered as a result of a contractual tasking requirement or agreement.

3.1.20 Contract data requirements. A requirement identified in a solicitation and imposed in a contract or order, that addresses any aspect of data (i.e., that portion of contractual tasking requirement associated with the development, generation, preparation, modification, maintenance, storage, retrieval, access, and/or delivery of data).

3.1.21 Contract Data Requirements List (CDRL). The standard format for identifying potential data requirements in a solicitation, and deliverable data items in a contract.

3.1.22 Contract Line Item Number (CLIN). A specific separately identifiable requirement for supplies or services in a contract.

3.1.23 Contract requirements. In addition to specific performance requirements, contract requirements include those defined in the Statement of Work; specifications, standards, and related documents; the CDRL; managements systems; and contract terms and conditions.

3.1.24 Contractor rights in technical data. All rights not granted to the Government are retained by the contractor. Until challenged by the Government, the contractor's initial assertions/markings control the allocation of rights to the Government and, thereby, define those retained by the contractor. (See definitions of Limited Rights, Restricted Rights, Small Business Innovation Research Rights, Special License Rights, Government Purpose Rights, and Unlimited Rights.)

3.1.25 Controlling DoD office. The DoD activity that sponsors work that generates data or receives data for DoD and has the responsibility for controlling the distribution of a document containing such data. The controlling DoD office is also responsible for selecting the correct distribution statement and ensuring that it is applied to the data before initial distribution.

3.1.26 Cryptographic logic. The embodiment of one (or more) crypto-algorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic process(es).

3.1.27 Current Document Change Authority (CDCA). The entity that has the decision authority over the contents of the document. The CDCA authority may be transferred. However, there is only one CDCA for a document at a time.

3.1.28 Data. Recorded information regardless of the form or method of recording. The term includes technical data, computer software documentation, financial information, management information, representation of facts, numbers, or datum of any nature that can be communicated, stored, and processed to form information required by a contract to be delivered to, or accessed by, the Government.

3.1.29 Data acquisition document. A collective term for DIDs, specifications, standards, tasking documents such as Statements of Objectives and Statements of Work, and contract clauses used to invoke Defense and other Government agencies' regulatory requirements (e.g., FAR, DFARS, Title 40 Protection of the Environment) for the preparation of data.

3.1.30 Data approval. An authorization from a designated authority certifying information is complete and suitable for its use.

3.1.31 Developed exclusively at private expense. Developed exclusively at private expense means that the development ot the item, component, or process (ICP) to which data pertains was accomplished entirely (100%) with costs charged to indirect cost pools, costs not allocated to a Government contract, or any combination thereof.

3.1.32 Developed Exclusively with Government funds. Developed exclusively at Government expense means development of the ICP to which data pertains was not accomplished exclusively (100%) or partially at private expense.

3.1.33 Developed with mixed funding. Data developed with mixed funding means development was accomplished partially with cost charged to indirect cost pools and/or costs not allocated to a Government contract,

and partially with costs charged directly to a Government contract.

3.1.34 Data call. A request by the Data Manager, system/PM, commander, or other authority to all Government participants to submit their requirements for contractor-prepared data on a given procurement.

3.1.35 Data format. The desired organization, structure, or arrangement of the content of the data product described by the DID or other data tasking document. This term relates to the shape, size, makeup, style, physical organization, or arrangement of the data product described in the DID or other tasking document.

3.1.36 Data item. The contractual term for the data product resulting from discrete requirements (e.g., technical, management, and administrative) specified in a contract or agreement using approved data acquisition documents, and delineated as separate contract line items. A sequential Data Item Number is assigned as an Exhibit Line Item Number (ELIN, DFARS 204.7105) and the exact title of the DID is listed on the CDRL (DD Form 1423).

3.1.37 Data Item Description (DID). A complete document that defines the data required of a contractor. The document specifies the data content, format, media, and intended use as applicable to a single data product.

3.1.38 Data Management (DM). Data management is the process of applying policies, procedures, and tools for the identification and control of data requirements, for assuring the adequacy of data and for facilitating the timely, economical acquisition and availability of data, including digital delivery or access. In simple terms, DM is the process for the acquisition of data (access or delivery) through contractual vehicles, so that data is available for use by authorized users. The type of data to which this applies includes research and development, acquisition, and logistics information. Tools are anything deemed necessary to carry out a function or task (see 4.2.1).

3.1.39 Data manager. A trained individual designated with principal responsibility for promulgating and ensuring compliance with the procedures outlined in this document at the DoD component level. This individual is the focal point within the DoD component for all data management issues. The DoD Clearance Office may delegate DID approval and cancellation authority to DoD component data management focal points.

3.1.40 Data-of-record. The official configuration-controlled representation of an item of data maintained by its current document control authority.

3.1.41 Data product. Information, which is inherently generated as the result of work tasks cited in a Statement of Work (SOW) or in a Source Document invoked in the contract. Such information is treated as a separate entity (for example, drawing, specifications, manual, report, records, or parts list).

3.1.42 Data Requirements Review Board (DRRB). The organization's review body responsible for reviewing the data requirements documentation defined in the solicitation. The DRRB ensures the data requirements are complete and accurate, and are the minimum essential necessary to support the program. Documentation reviewed by the board includes the tasking document, DIDs, and CDRLs. (This process applies to negotiated procurements and sealed bidding.)

3.1.43 Data rights. See definition for Rights in Technical Data (TD).

3.1.44 Data rights validation. The formal process authorized by the contract clauses, DFARS 252.227-7019 (software) and DFARS 252.227-7037 (technical data), by which the Government may challenge the contractor's assertions regarding and /or markings on data. The concept is often extended to include other informal Government inquiries concerning or challenges to assertions and/or markings.

3.1.45 Data view. Presentation and organization of the information for the user. How the user "sees" or uses the data will be unique to individual need. The data could be viewed for a multitude of purposes: recordkeeping, decision-making, information analysis, etc. Data can be viewed either electronically or manually.

3.1.46 Defense acquisition system. Management process by which DoD provides effective, affordable, and timely systems to the users.

3.1.47 Defense Automatic Addressing System Center (DAASC). The Defense Automatic Address System Center provides information on Communication Routing Identifiers (COMMRI), DoD Activity Address Codes (DODAAC), Routing Identifier Codes (RIC), and Military Assistance Program Address Codes (MAPAC).

3.1.48 Defense Information Technology Standards Registry (DISR). The Department of Defense (DoD) Information Technology Standards Registry (DISR) mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information.

3.1.49 Defense system. A weapon system, system component, support equipment, non-weapon systems, items, facilities, and services acquired by DoD.

3.1.50 Defense system data. Data acquired by a defense system program office to support the life cycle acquisition, operation, maintenance, and disposal of a defense system. (See also Product data.)

3.1.51 Defense system life cycle. The entire period from the definition of mission need through acquisition, operation, maintenance, and disposal of a defense system.

3.1.52 Deferred delivery. A contractual right implemented by DFARS 252. 227-7026 or negotiated option language whereby the Government may delay delivery of contractually identified; thereby the cost of delivery, until actual need for the data arises.

3.1.53 Deferred ordering. A contractual right implemented by DFARS 252.227-7027 or negotiated option language whereby the Government may delay ordering the delivery of data "generated" in the performance of the contract; thereby the cost of delivery, until an actual need for the data arises.

3.1.54 Delivery. Delivery of data to the controlling DoD office in any media or official notification of access to the data via contractor digital services in satisfaction of a data requirement listed on the CDRL, contract schedule, or another authorized "data acquisition document."

3.1.55 Department of Defense FAR Supplement (DFARS). DFARS provides DoD implementation and supplementation of the Federal Acquisition Regulation (FAR). The DFARS contains requirement of law, DoD-wide policies, delegation of FAR authorities, deviations from FAR requirements and policies/procedures relating to the procurement of supplies; including data and services.

3.1.56 Design Readiness Review (DRR). A mid-phase assessment of design maturity during the System Development and Demonstration (SDD) phase. According to DODI 5000.02, design maturity may be gauged by the number of subsystems and system design reviews successfully completed; the percentage of drawings completed; planned corrective actions to hardware/software deficiencies; adequate Development Testing (DT); an assessment of Environmental, Safety and Occupational Health (ESOH) risks; a completed Failure Modes and Effects Analysis (FMEA); the identification of key system characteristics and critical manufacturing processes; an estimate of system reliability based on demonstrated reliability rates; and other indicators, as appropriate.

3.1.57 Digital data approach and implementation plan. A description of the contractor's approach, experiences, capabilities, and successes in creating, managing, using, and exchanging digital information, and the contractor's application of digital techniques throughout the contract to satisfy service, infrastructure, media, format and data view requirements associated with the development, generation, preparation, modification, maintenance, storage, retrieval, access, and delivery of data in the contract.

3.1.58 Digital format. Data in a format that is readable by a computer.

3.1.59 Distribution. Data exchange between a data source and data recipient regardless of media used.

3.1.60 Distribution statement. A statement used in marking technical data to denote the extent of its availability for secondary distribution, release, and disclosure without need for additional approvals or authorizations from the controlling DoD office (Refer to DoD Directive 5230.24.).

3.1.61 Document. A self-contained body of information or data that can be packaged for delivery on a single medium.

3.1.62 Document Type Definition (DTD). DTD is a specific schema language that evolved as the document specification language for Standard Generalized Markup Language (SGML) documents, and can be used to specify XML documents.

3.1.63 DoD clearance office. The office, representing the Secretary of Defense, with assigned DoD-wide Office of Management and Budget (OMB) clearance authority, responsibility for preparing and issuing the DID section of the ASSIST, and responsibility for developing and implementing DoD policy for data requirements that is in compliance with Public Law 104-13. The clearance office may delegate DID approval and cancellation authority to designated DoD component data management focal points.

3.1.64 DoD components. Consists of the Services Army, Navy, Air Force, Marine Corps, and Agencies like Defense Logistics Agency and Defense Contract Management Agency.

3.1.65 Electronic Data Interchange (EDI). A technique for electronically transferring and storing formatted information between computers utilizing established and published formats and codes, as authorized by the applicable Federal Information Processing Standards The complete Federal Implementation Guidelines for EDI can be accessed at http://www.defenselink.mil/bta/FedeBiz/FEDGUIDELINE.shtml (see Appendix A).

3.1.66 Engineering Development Model (EDM). A production representative system acquired during the System Development and Demonstration (SDD) Phase. EDMs may be used to demonstrate maturing performance via an Operational Assessment (OA) or Operational Testing (OT) and to finalize proposed production specifications and drawings. Formal Initial Operational Test and Evaluation (IOT&E) required by statute or regulation before a Full Rate Production Decision Review (FRPDR) is normally performed on Low Rate Initial Production (LRIP) articles during the LRIP effort of the Production and Deployment (P&D) phase.

3.1.67 Extensible Markup Language (XML). XML is a human-readable, machine-understandable, general syntax for describing hierarchical data, applicable to a wide range of applications (databases, e-commerce, Java, web development, searching, etc.). Custom tags enable the definition, transmission, validation, and interpretation of data between applications and between organizations.

3.1.68 Extensible Stylesheet Language (XSL). XSL is a language used to specify a set of rules for transforming an XML document from one structure to another. In most cases it is used to indicate how the source content should be styled, laid out, and paginated onto some presentation medium, such as a window in a web browser or a handheld device, or a set of physical pages in a catalog, report, pamphlet, book, or technical manual.

3.1.69 Federal Acquisition Regulation (FAR). The regulation for use by federal executive agencies for acquisition of supplies and services with appropriated funds. The FAR is supplemented by the Military Departments and by DoD. The DoD supplement is called the DFARS.

3.1.70 Final review. The review of completed data, which has been submitted to the specified Government review activity. This review includes a check for completeness of the data, technical adequacy, compliance with contractual requirements, proper identification and marking of rights in technical data, and distribution statements.

3.1.71 Focal point. Person in a particular organization (e.g., headquarters of a major command) who acts as the principal point of contact for coordination and exchange of information related to cost/schedule control system criteria (C/SCSC) implementation or surveillance.

3.1.72 Full Operational Capability (FOC). The full attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specified characteristics, which is manned and operated by a trained, equipped, and supported military unit or force.

3.1.73 Full Rate Production (FRP). Contracting for economic production quantities following stabilization of the system design and validation of the production process.

3.1.74 Functional Requirements Authentication Board (FRAB). A board responsible for validating that functional support templates have been applied to SOWs, that SOWs are integrated and performance-based, and to ensure that the SOW references performance specifications as appropriate. FRABs will be chaired by the requiring acquisition activity, which will be PMs for PM-managed programs and the Army Acquisition Organization (AAO) designee for non-PM-managed programs. The FRAB ensures that data requirements are complete, accurate, value added and are the minimum essential to support the program; and that data requirements reflect task requirements. The board also ensures that approved specifications, standards, and processes have been applied as approved and also ensures that "how-to-manage" requirements are included only when essential.

3.1.75 Generated. Technical data and computer software first created in the performance of a Government contract.

3.1.76 Government Concept of Operations (GCO). A Government document to communicate information to potential contractors about the Government infrastructure and EDI implementation for defense systems.

3.1.77 Government purpose rights. The right to use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction; and release or disclose technical data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data for United States Government purposes.

3.1.78 Implementation Conventions (ICs). Implementation of ASC X12 Electronic Data Interchange Standards requires ICs to fully define the transactions. ICs define the exact transactions required by a trading partner community to conduct business by tailoring the use of the standards' segments, composite data elements, simple data elements and code values. In addition, they document the intended interpretation of a standard. For example, the ANSI ASC X12 Invoice (810) transaction set is used as a Commercial Invoice, a Progress Payment, and a Public Voucher. The segments and data elements used in each of these contexts may be different.

3.1.79 Independent Verification and Validation (IV&V). An independent review of software performed by an organization that is technically, managerially, and financially independent of the development organization.

3.1.80 Indexing. The process of identifying and referencing data to assist in storage and retrieval.

3.1.81 Information Technology (IT). Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources, including National Security Systems (NSSs). It does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

3.1.82 Infrastructure. The foundation of hardware, software, and telecommunications required to create exchange, manage, and use digital data in the evolving Integrated Digital Data Environment (IDDE).

3.1.83 Initial Operational Capability (IOC). The first attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specific characteristics with the appropriate number, type, and mix of trained and equipped personnel to operate, maintain, and support the system. It is normally defined in the CDD and the CPD.

3.1.84 Initial Operational Test and Evaluation (IOT&E). Dedicated Operational Test and Evaluation conducted on production, or production representative's articles, to determine whether systems are operationally effective and suitable.

3.1.85 Initial provisioning. The process of determining the range and quantity of items (i.e., spares and repair parts, special tools, and test and support equipment) required to support and maintain an item for an initial period of service. Its phases include the identification of items of supply, the establishment of data for catalog, Technical Manuals (TM) and allowance list preparation, and the preparation of instructions to assure delivery of necessary support items with related end articles.

3.1.86 In-Process Review (IPR). The review and monitoring of data during preparation. This review reveals inadequacies in the design activities, practices, and procedures, including quality assurance practices for data that will result in deficient (missing dimensions, tolerances, notes, and interface requirements), incomplete (missing reference documents, mandatory processes, etc.) and nonconforming (not in accordance with contractual requirements) data. Discovery of discrepancies during this review will facilitate and expedite final review and acceptance of the data.

3.1.87 In-Service Engineering Agent (ISEA). An ISEA is that activity delegated functions by and in support of the life cycle manager. Responsibilities include overall engineering, testing, maintenance, and logistics requirements incident to specific operational equipment.

3.1.88 Inspection. The examining and testing of supplies or services (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether they conform to contract requirement.

3.1.89 Integrated Digital Environment (IDE). The operating framework for sharing information between physically separated users. The IDE uses value-added networks to provide a unified and consistent interface for users to obtain data and information.

3.1.90 Integrated Digital Data Environment (IDDE). The evolving DoD and industry strategy to generate, exchange, access, manage, and use digital data supporting defense systems more effectively.

3.1.91 Integrated Logistics Support (ILS). All the support considerations necessary to assure the effective and economical support of a system for its life cycle. It is an integral part of all other aspects of system acquisition and operation.

3.1.92 Integrated Logistics Support Plan (ILSP). The ILSP describes the overall ILS program requirements, tasks, and milestones for the current acquisition phase. It also projects ILS program planning for succeeding phases.

3.1.93 Integrated Product Team (IPT). A team composed of representatives from appropriate functional disciplines working together to build successful programs, identify and resolve issues, and make sound and timely recommendations to facilitate decisions making. There are three types of IPTs: Overarching IPTs (OIPTs) that focus on strategic guidance, program assessment, and issue resolution; Working-level IPTs (WIPTs) that identify and resolve program issues, determine program status, and seek opportunities for acquisition reform; and Program level IPTs (PIPTs) that focus on program execution and may include representatives from both Government and after contract award industry.

3.1.94 Intellectual property. Includes inventions, trademarks, patents, copyrights, and trade secrets.

3.1.95 Inventory Control Point (ICP). The organizational element within a distribution system which is assigned responsibility for system-wide direction and control of material including such management functions as the computation of requirements, the initiation of procurements or disposal actions, the development of worldwide quantitative and monetary inventory data, and the positioning and repositioning of material.

3.1.96 Joint Engineering Data Management Information and Control System (JEDMICS). A DoD initiative for the management and control of engineering drawings and related text in a standard repository. JEDMICS has been designed as an open, client-server architecture conforming to applicable Integrated Data Environment standards which provides the user with the ability to locate approved engineering drawings and associated data that is the required revision in the preferred format.

3.1.97 Legacy data. Defense data that is not in current standard digital format or is residing in older databases maintained with obsolete or inefficient technology. Legacy data can be in hard copy (e.g., paper or microform) or digital format. The ability to use legacy data within an IDDE is severely limited unless the data is converted to standard digital format. Cost-benefit analyses are required to determine which legacy data should be converted.

3.1.98 Limited rights. The rights to use, modify, reproduce, release, perform, display, or disclose technical data in whole or in part, within the Government. The Government may not, without the written permission of the party asserting limited rights, release or disclose the technical data outside the Government, use the technical data for manufacture, or authorize the technical data to be used by another party.

3.1.99 Military Engineering Data Asset Locator System (MEDALS). Managed by the Defense Logistics Information Service, MEDALS is an automatic information system that serves as the central index of engineering data for the DoD. DoD technical data repositories, which store, maintain, and distribute the engineering drawings, supply the MEDALS program with technical drawing index data and associated information. The MEDALS program is linked to the acquisition process of technical data and maintains indexing information throughout the document life cycle. MEDALS can be accessed at https://www.dlis.dla.mil/medals/ (see Appendix A).

3.1.100 Milestones (MS). The point at which a recommendation is made and approval sought regarding starting or continuing an acquisition program, i.e., proceeding to the next phase. Milestones established by DODI 5000.02 are: MS A that approves entry into the Technology Development (TD) phase; MS B that approves entry into the System Development and Demonstration (SDD) phase; and MS C that approves entry into the Production and Deployment (P&D) phase. Also of note are the Concept Decision (CD) that approves entry into Concept Refinement (CR) phase, the Design Readiness Review (DRR) that ends the System Integration (SI) effort, and the Full Rate Production Decision Review (FRPDR) at the end of the Low Rate Initial Production (LRIP) effort of the P&D phase that authorizes FRP and approves deployment of the system to the field or fleet.

3.1.101 Milestone Decision Authority (MDA). The designated individual with overall responsibility for a program. The MDA has the authority to approve entry of an acquisition program into the next phase of the acquisition process and is accountable for cost, schedule, and performance reporting to higher authority, including Congressional reporting.

3.1.102 Military Critical Technologies List (MCTL). A detailed compendium of information on technologies, which the Department of Defense assesses as critical to maintaining superior U.S. military capabilities. The MCTL contains definitions of thresholds that make technology militarily critical. The acquisition of any of these technologies by a potential adversary would lead to the significant enhancement of the military-industrial capabilities of that adversary to the detriment of U.S. security interests. It includes, for example, technologies associated with the proliferation of nuclear, chemical, and biological weapons and missile delivery systems.

3.1.103 Metadata. "Data about data". Properties used to identify or define a data item. Descriptive information can include title, revision level or date, relationship to other data objects, key words, location of data-of-record, and data custodian.

3.1.104 Munitions List (ML). The part of the secondary regulations (the International Traffic in Arms Regulations or ITAR) that defines which defense articles and services are subject to licensing. The list is contained in part 121 of ITAR and is divided into 16 sections, which are further sub-divided into more detailed and specific sub-sections. While all items on the US Munitions List require licenses from the Office of Defense Trade Controls in the State Department, many of them are also listed on a different export control list, the Commodity Control List, which is part of the system for licensing dual-use articles and services. Licensing dual-use articles and services is the responsibility of the Department of Commerce. Items that are on the Munitions List and the Commodity Control List require approved licenses from both the State Department and the Commerce Department before they can be exported.

3.1.105 National Item Identification Number (NIIN). The 9-digit National Item Identification Number consists of a 2-digit National Codification Bureau number designating the central cataloging office of the NATO or other friendly country, which assigned the number and a 7-digit non-significant number.

3.1.106 National Stock Number (NSN). The 13-digit stock number that consists of the 4-digit Federal Supply Classification code and the 9-digit National Item Identification Number. The number should be arranged as follows: 9999-00-999-9999.

3.1.107 Non-Disclosure Ageement (NDA). An NDA is used between two or more parties which authorizes the release and/or use of specified data for spsecified purpose on condition that the receiving party limiting their use and control further dissemination. A standard form NDA for use by the Government with its contractors is at DFARS 252.227-7025 and DFARS 227.7103-7. The term also is used with regards to similar agreements between two contractors usually the prime and a Government support contractor.

3.1.108 Non-Government Standard (NGS). A standardization document developed by a private sector association, organization, or technical society, which plans, develops, establishes, or coordinates standards, specifications, handbooks, or related documents. The term does not include standards of individual companies. All approved NGS, adopted by the DoD, are listed in ASSIST.

3.1.109 One-time DID. A DID approved by a DoD component for one-time use associated with a unique data requirement applicable to a single contract or program.

3.1.110 Operations and support. A phase of the life cycle as defined in DODI 5000.02. The objective of this phase is to execute a support program that meets operational support performance requirements and sustains the

system in the most cost-effective manner over its total life cycle. When the system has reached the end of its useful life, it should be disposed of in an appropriate manner. Operations and Support has two major efforts: Sustainment and Disposal.

3.1.111 Ordering data. A contractually authorized process for requiring the delivery of data (via any approved method to include formal accesss) in accordance with a data requirement document that defines content, format, schedule, and price.

3.1.112 Organizational data manager. An individual in a project or system program office, division, or DoD Field Activity who is assigned responsibility for ensuring compliance, acquisition, and management of technical data.

3.1.113 Packing, Handling, Storage, and Transportation (PHST). The resources, processes, procedures, design consideration, and methods to ensure all system, equipment, and support items are preserved, packaged, handled, and transported properly. This includes environmental consideration, equipment preservation requirements for short and long term storage, and transportability.

3.1.114 Performance. Those operational and support characteristics of the system that allows it to effectively and efficiently perform its assigned mission over time. The support characteristics of the system include both supportability aspects of the design and the support elements necessary for system operation.

3.1.115 Performance specification. A specification that states requirements in terms of required results ('what is' required) with criteria for verifying compliance, but without stating methods ('how to') for achieving the required results.

3.1.116 Performance Work Statement (PWS). A work statement that identifies technical, functional, and performance requirements. PWS specifies what outcomes the Government wants but does not dictate how the work will be performed. This allows the contractor to use innovation in the design, development, and manufacturing of the product.

3.1.117 Personal Identification Number (PIN). A personal identification number is a numeric value (sometimes expressed as text using the standard telephone dial mapping) that is used in certain systems to gain access, and authenticate. PINs are a type of password. Many people say PIN number despite others finding the usage objectionable and redundant because the PIN acronym has the word *number* in it. PINs are (ideally) only known by the person, who's PIN it is, and are sufficiently hard to guess. The PIN should be such that a person or computer cannot guess it in sufficient time by using a guess and check method, where it guesses the PIN, and checks for correctness by testing it on the system that the person is attempting to access.

3.1.118 Prime contract. A contract agreement or purchase order entered in to by a contractor with the Government.

3.1.119 Prime contractor. The entity with which an agent of the United States entered into a prime contract for the purposes of obtaining supplies, material, equipment, or services of any kind.

3.1.120 Procurement Request (PR). A document which describes the required supplies or services so that a PR can be initiated. Some procuring activities actually refer to the documentation by this title; others use different titles such as Procurement Directive. Combined with specification, the SOW, and CDRL, it is called the PR package, a basis for solicitation.

3.1.121 Procuring Contracting Officer (PCO). The individual authorized to enter into contracts for supplies and services on behalf of the Government by sealed bids or negotiations, and who is responsible for overall procurement under the contract.

3.1.122 Product data. Data that describes a defense system/ item used in supporting the system or item through its life cycle.

3.1.123 Product definition data. The totality of data elements and key relationships required to completely define a product. Product Definition Data includes geometry, topology, relationships, tolerances, and features for mechanical and electronic components, software, and documentation necessary to completely define a component part, an assembly of parts or a system for the purpose of design, analysis, manufacture, test, inspection, use, support,

and disposal. The terms "Engineering Data" and "Technical Data", refers to as the Technical Data Packages (TDPs), consists of drawings, specifications, and associated lists that describe how the items are designed and manufactured. Product Definition Data encompasses a broader range of data elements including metadata.

3.1.124 Production and Deployment (P&D). The P&D consist of two efforts, LRIP and Full Rate Production and Deployment (FRP&D), and begins after a successful Milestone C review. The purpose of this P&D is to achieve an operational capability that satisfies mission needs. Operational test and evaluation should determine the effectiveness and suitability of the system. The MDA should make the decision to commit the Department of Defense to production at Milestone C. Milestone C authorizes entry into LRIP (for Major Defense Acquisition Programs [MDAPs] and major systems), into production or procurement (for non-major systems that do not require LRIP), or into limited deployment in support of operational testing for Major Automated Information System (MAIS) programs or software-intensive systems with no production components. There are statutory and regulatory requirements that should be met at Milestone C.

3.1.125 Program Manager (PM). A designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs. The PM should be accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority.

3.1.126 Program office. The office originating contractual data requirements.

3.1.127 Proprietary rights. A broad contractor term used to describe data belonging to the contractor, while this term/marking and similar terms are used by contractors in their commercial dealings, it is NOT an authorized marking on data formally delivered to the Government.

3.1.128 Provisioning. The process of determining and acquiring the range and quantity (depth) of spares and repair parts, and support and test equipment required to operate and maintain an end item of material for an initial period of service. Usually refers to first outfitting of a ship, unit, or system.

3.1.129 Purchase Order (PO). A contractual procurement document used primarily to procure supplies and non-personal services when the aggregate amount involved in any one transaction is relatively small (e.g., not exceeding $100,000).

3.1.130 Quality Assurance (QA). A planned and systematic pattern of all actions necessary to provide confidence that adequate technical requirements are established, that products and services conform to established technical requirements, and that satisfactory performance is achieved.

3.1.131 Repair. The restoration or replacement of parts or components of real property or equipment as necessitated by wear and tear, damage, failure of parts or the like, in order to maintain it in efficient operating condition.

3.1.132 Repair parts. Consumable bits and pieces, that is, individual parts or non-repairable assemblies required for the repair of spare parts or major end items.

3.1.133 Repairable item. An item of a durable nature which has been determined by the application of engineering, economic, and other factors to be the type of item feasible for restoration to a serviceable condition through regular repair procedures.

3.1.134 Repurchase data. Data that is needed to support a re-procurement or recurring acquisition of a continuing functional item currently in the weapon system inventory that does not require research, development, test, and evaluation.

3.1.135 Re-procurement. The recurring acquisition of a continuing functional item currently in the weapon system inventory that does not require research, development, test, and evaluation.

3.1.136 Schemas. A formal language for specifying structure of a document. Document Type Definition (DTD) is the specific schema language that evolved as the document specification language for Standard Generalized Markup Language (SGML) documents, and can be used to specify XML documents. XML Schema Language is another schema language that can be used to specify the syntax or XML documents. XML Schema Language documents are themselves XML documents.

3.1.137 Secondary distribution. Distribution of, or access to, data usually based on a request to a document repository or information center by other than the controlling DoD office.

3.1.138 Small Business Innovation Research (SBIR). SBIR data rights mean a royalty free license for the Government, to include its support service contractors to use, modify, reproduce, release, perform, display, or disclose technical data or computer software "generated and delivered" under a contract for any United States government purpose. See DFARS 252.227-7018.

3.1.139 Solicitation. In Government contracting, the term refers to communication of a procurement request package to potential bidders/proposer.

3.1.140 Spare parts. Repairable components or assemblies used for maintenance replacement purposes in major end items of equipment.

3.1.142 Special license rights. Government data rights which are outside of the DFARS definition categories: Limited Rights; Restricted Rights; Government Purpose Rights; or Unlimited Rights and must, therefore, be specifically negotiated and documented in the contract. DFARS, 10U.S.C. 2320(a)(2)(G)(ii), and Competition in Contracting Act limit what the Government may relinquish in such negotiations.

3.1.142 Specification. A document used in development and procurement, which describes the technical requirements for items, material, and services including the procedures by which it will be determined that the requirements have been met. Specifications may be unique to a specific program (program-peculiar) or they may be common to several applications (general in nature).

3.1.143 Standard. A document that establishes engineering and technical requirements for processes, procedures, practices, and methods that have been decreed by authority or adopted by consensus or typically by consensus.

3.1.144 Standard for the Exchange of Product Model Data (STEP). A comprehensive ISO standard (ISO 10303) that describes how to represent and exchange digital product information.

3.1.145 Statement of Objectives (SOO). A Government prepared document incorporated into the Request for Proposal (RFP) that states the overall solicitation objectives. It can be used in those solicitations where the intent is to provide the maximum flexibility to each offeror to propose an innovative development approach. Offerors use the RFP, product performance requirements, and SOO as a basis for preparing their proposals including a SOW and CDRL. Note: The SOO is not retained as a contract compliance item.

3.1.146 Statement of Work (SOW). The portion of a contract which establishes and defines all non specification requirements for contractor's efforts either directly or with the use of specific cited documents.

3.1.147 Subcontractor. Subcontractors means any supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor.

3.1.148 Submittal. Data or information to be provided by the contractor to the Government for review and approval. There may be several submittals depending on the acquisition and progression of the development of each data item. (See Delivery.)

3.1.149 Subsystem. A functional grouping of components that combine to perform a major function within an element such as electrical power, altitude control, and propulsion.

3.1.150 Supply support. The process conducted to determine, acquire, catalog, receive, store, transfer, issue, and dispose of secondary items necessary for the support of end items and support items. This includes provisioning for initial support as well as replenishment supply support.

3.1.151 Sustainment. The purpose of the Sustainment effort is to execute the support program to meet operational support performance requirements and sustain the system in the most cost effective manner over its life cycle. Sustainment includes supply, maintenance, transportation, sustaining, engineering, data management, configuration management, manpower, personnel, training, habitability, survivability, environment, safety, (including explosives safety) occupational health, protection of critical program information, anti-tamper provisions, IT including National Security Systems, supportability, and interoperability. The provisioning of personnel, logistics, and other support required to maintain and prolong operations or combat until successful accomplishment or revision of the mission or of the national objective.

3.1.152 System Demonstration (SD). A program enters SD after the program has demonstrated the system in prototype articles or Engineering Development Models (EDMs). The effort is intended to demonstrate the ability of the system to operate in a useful way consistent with the approved KPPs. This effort ends when the system is demonstrated in its intended environment using the selected prototype, meets approved requirements, industrial capabilities are reasonably available and the system meets or exceeds exit criteria and Milestone C entrance requirements.

3.1.153 System Development and Demonstration (SDD). The SDD consists of two efforts, System Integration (SI) and SD, and begins after Milestone B. It also contains a DRR at the conclusion of the SI effort.

3.1.154 Systems Engineering (SE). A comprehensive, iterative Technical Management process that includes translating operational requirements into configured systems, integrating the technical inputs of the entire team, managing interfaces, characterizing and managing technical risk, transitioning technology from the technology base into program specific efforts, and verifying that designs meet operational needs. It is a life cycle activity that demands a concurrent approach to both product and process development.

3.1.155 System Engineering Management Plan (SEMP). Includes plans for verification, risk alleviation, analyses, and simulation of the system requirements.

3.1.156 System Integration (SI). A program enters SI when the contractor has a technical solution for the system, but has not yet integrated the subsystems into a complete system. The CDD guides the effort, which typically includes demonstration of prototype articles or EDMs.

3.1.157 Tailoring. The process by which the individual requirements (sections, paragraphs, or sentences) of the selected specification and standard, as well as related documents are evaluated to determine which requirements are most suitable for a specific system and equipment acquisition. The modification of these requirements ensures an optimal balance between operational needs and cost. The tailoring of data product specifications and Data Item Descriptions (DIDs) should be limited to the exclusion of information requirements provisions and eliminate unnecessary information. For DIDs, tailoring is the process by which individual requirements of the selected DID is evaluated to determine which requirements are suitable to a specified acquisition. Tailoring data requirements should consist of reducing the scope of the selected DID by specifying in Block 16 of the CDRL which portion(s) of the DID are not applicable.

3.1.158 Technical data. Recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial or management information. This term is used by many regulatory documents with varying definitions. The above definition applies when discussing rights in data. In other more general uses, the term does include computer software and incidental data.

3.1.159 Technical Data Package (TDP). A technical description of an item adequate for supporting an acquisition strategy, production, and engineering and logistics support. The description defines the required design configuration or performance requirements, and procedures required to ensure adequacy of item performance. It consists of applicable technical data such as models, drawings, associated lists, specifications, standards, performance requirements, quality assurance requirements, software documentation, and packaging details.

3.1.160 Technical Manual (TM). A publication that contains instructions for the installations, operation, maintenance, training, and support of weapons systems, weapon system components, and support equipment. TM information may be presented in any form or characteristic, including but not limited to hard copy, audio and visual displays, magnetic tape, disc, and other electronic devices. A TM normally includes operational and maintenance instructions, part lists or parts breakdown, and related technical information or procedures exclusive of administrative procedures. Technical Orders (TOs) that meet the criteria of this definition may also be classified as TM.

3.1.161 Technical Manual Contract Requirements (TMCR). Provides the required content, format, and style requirements for the preparation and delivery of one or more TMs and/or TM management data items in a definitive contractual document. The TMCR consolidates the requirements from various government specifications and standards and tailors those requirements to produce a manual that satisfies specified user needs.

3.1.162 Technical Order (TO). See Technical Manual (TM).

3.1.163 Technology development It is initiated by a successful Milestone A decision. The purpose of this Technology Development is to reduce technology risk and to determine the appropriate set of technologies to be integrated into a full system. Technology Development is a continuous technology discovery and development process reflecting close collaboration between the Science and Technology (S&T) community, the user, and the system developer. It is an iterative process designed to assess the viability of technologies while simultaneously refining user requirements. This effort is normally funded only for advanced work and does not mean that a new acquisition program has been initiated.

3.1.164 Test and Evaluation Master Plan (TEMP). Documents the overall structure and objectives of the Test and Evaluation (T&E) program.

3.1.165 Unlimited rights. Right to use, modify, reproduce, perform, display, release, or disclose technical data, in whole or in part, in any manner, and for any purpose whatsoever, and to authorize others to do so.

3.1.166 Validation. The process by which the contractor (or other activity as directed by the DoD component procuring activity) tests technical documents for accuracy and adequacy, comprehensibility, and usability.

3.1.167 Verification. The process by which technical data are tested and proved under DoD component control to be technically accurate and complete, comprehensible, and usable for operation and maintenance of equipment or systems procured for operational units.

3.1.168 Virtual acquisition. An acquisition where all or part of the deliverable data of the contract is to be furnished by Government access to a data repository under the control of a Government contractor. Such method of delivery must be accomplished by a contractual right/option for the Government to have a copy of the data placed under direct Government control.

3.1.169 Warranty of data. A voluntary but desirable clause whereby the contractor warrants that all technical data delivered under this contract will at the time of delivery conform to the specification and all other requirements of this contract.

3.1.170 World Wide Web (WWW) Consortium (W3C). The W3C is an international consortium where member organizations, a full-time staff, and the public work together to develop standards for the World Wide Web. W3C's mission is: "*To lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web*". W3C also engages in education and outreach, develops software, and serves as an open forum for discussion about the Web. The Consortium is headed by Tim Berners-Lee, the original creator of the World Wide Web and primary author of the URL (Uniform Resource Locator), HTTP (Hyper-Text Transfer Protocol) and HTML (Hyper-Text Markup Language) specifications, the principal technologies that form the basis of the Web (see Appendix A).

3.2 Acronyms. The acronyms used in this manual are as follows:

AIS	Automated Information System
ANSI	American National Standards Institute
AP	Acquisition Plan
AP xxx	Application Protocol xxx (where xxx –stands for protocol number e.g., AP 203)
AS	Acquisition Strategy
ASBCA	Armed Services Board of Contract Appeals
ASC X12	Accredited Standards Committee (*data exchange standards*)
ASCII	American Standard Code for Information Interchange
ASSIST	Acquisition Streamlining and Standardization Information System
BSM	Business Systems Modernization
CAO	Contract Administration Office
CAD	Computer Aided Design
CAE	Computer Aided Engineering
CAM	Computer Aided Manufacturing
CCAL	Certified Contractor Access List
CCITT	Consultative Committee on International Telegraphy and Telephony
CD	Concept Decision
CDCA	Current Document Change Authority
CDRL	Contract Data Requirements List
CGM	Computer Graphics Metafile
CLIN	Contract Line Item Number
CM	Configuration Management
COTS	Commercial Off-the-Shelf
CR	Concept Refinement
DAPS	Document Automation and Publication Service
DAS	Data Acquisition Strategy
DAU	Defense Acquisition University
DCMA	Defense Contract Management Agency
DFARS	Defense Federal Acquisition Regulations Supplement
DID	Data Item Description
DLA	Defense Logistics Agency

DLIS	Defense Logistic Information Service
DM	Data Management
DoD	Department of Defense
DoDD	Department of Defense Directive
DRR	Design Readiness Review
DRRB	Data Requirements Review Board
DTD	Document Type Definition
EDI	Electronic Data Interchange
EDM	Engineering Development Model
EIA	Electronic Industries Alliance
EPA	Environmental Protection Agency
ERP	Enterprise Resource Planning
ETM	Electronic Technical Manual
FAR	Federal Acquisition Regulations
FOC	Full Operational Capability
FTP	File Transfer Protocol
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FRAB	Functional Requirements Authentication Board
FRP	Full Rate Production
GCO	Government Concept of Operations
GEIA	Government Electronics and Information Technology Association
GIG	Global Information Grid
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transfer Protocol
IC	Implementation Convention
ICP	Item, Component, or Process
IDE	Integrated Digital Environment
IDDE	Integrated Digital Data Environment
IETM	Interactive Electronic Technical Manual
IGES	Initial Graphics Exchange Specification
ILS	Integrated Logistics Support
ILSP	Integrated Logistics Support Plan

IOC	Initial Operational Capability
IPR	In-Process Review
IPT	Integrated Process or Product Team
ISEA	In-Service Engineering Agent
ISO	International Organization for Standardization
ISP	Information Support Plan
IT	Information Technology
IV&V	Independent Verification and Validation
JCO	Joint Certification Office
JTA	Joint Technical Architecture
JEDMICS	Joint Engineering Data Management Information and Control System
KPP	Key Performance Parameters
LCL	Life Cycle Logistics
LMI	Logistics Management Information
MCTL	Military Critical Technologies List
MEDALS	Military Engineering Data Asset Locator System
ML	Munitions List
NCES	Net-Centric Enterprise Services
NGS	Non-Government Standards
NIIN	National Item Identification Number
NSN	National Stock Number
NSRP	National Shipbuilding Research Program
OMB	Office of Management and Budget
PA	Public Affairs
PCO	Procuring Contracting Office(r)
P&D	Production and Deployment
PDD	Product Definition Data
PDF	Portable Document Format
PDM	Product Data Management
PIN	Personal Identification Number
PL	Public Law
PM	Program Manager
PWS	Performance Work Statement

QA	Quality Assurance
RFP	Request for Proposal
RTF	Rich Text Format
SALE	Single Army Logistics Enterprise
SE	Systems Engineering
SEP	Systems Engineering Plan
SGML	Standard Generalized Mark-up Language
SI	System Integration
SIA	Special Interest Area
SOO	Statement of Objectives
SOW	Statement of Work
STEP	Standard for the Exchange of Product Model Data
TDP	Technical Data Package
TM	Technical Manual
TMCR	Technical Manual Contract Requirement
TMINS	Technical Manual Identification Numbering System
TO	Technical Order
VAN	Value Added Network
W3C	World Wide Web (WWW) Consortium
WAWF	Wide Area Workflow
WWW	World Wide Web
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

4. GENERAL

4.1 Applicability. This document applies to the NAVSEA, NAVAIR, MAJCOMs, Field Activities, and all other organizational entities within the Department of Navy, hereafter referred to collectively as "the Navy components."

4.1.1 Intended audience. The intended audience for this document includes both new and experienced Data Managers, who support defense program offices and command acquisition offices, by preparing contractual requests for data for defense systems; as well as anyone involved in the identification and control of data requirements; the timely and economical acquisition of such data; assuring the adequacy of data; the distribution or communication of the data to the point of use; or analysis of the data use. This document does not apply to the following:

a. Technical data for cryptographic/crypto logic activities.

b. TMs for nuclear weapon systems supported by publications under the Joint Nuclear Weapons Publications System.

c. Information provided solely for source selection purposes.

d. Data generated by any contractors to include support contractors and service contractors are subject to the

same rules and rights in data.

4.2 Objectives. This document identifies requirements and provides common guidance for the acquisition and management of contractor prepared data within the DoD components. This document is applicable to all forms of data whether it is digital data, hard copy, or data to which access via contractor provided digital information services is required. The information in this document is presented in the order in which the events generally occur in the defense system life cycle. In many cases the DM activities are not a single event, but impact every contract award during the life cycle of a defense system. Examples of these contracts are: study contracts, development contracts, demonstration contracts, production contracts, sustainment contracts, and performance-based contracts. These types of contracts and other types occur throughout the defense system life cycle. The planning for acquisition of data (5.1 through 5.) provides an explanation of the relationship between the defense system life cycle and the data acquisition life cycle.

4.2.1 Guidance. The overall objective of this document is to provide guidance for effective acquisition and management of contractor-prepared data. Data Managers and others involved in DM should use this document as an initial reference source for recommended approaches. In situations where more detailed guidance is required, this document should direct the user to sources of additional information and guidance. By following this document's guidance, the Data Manager will:

a. Ensure compliance with DoD regulations, instructions, etc. on the selection, acquisition, and use of data.

b. Determine minimum essential DoD data needs (including tailoring of all data acquisition documents, such as DIDs) and align them as much as possible to the types of data available and acquired when DoD procures goods and services.

c. Ensure acquisition of adequate data and data rights for life cycle support and to allow competitive re-procurement if required.

d. Maximize the cost-effective sharing of data within and among DoD components.

e. Ensure the cost-effectiveness of the defense system data.

f. Coordinate data access and delivery with overall acquisition program schedules.

g. Ensure that the timeliness, accuracy, and data rights marking on the delivered data meet the contract requirements.

h. Ensure proper marking of the data and/or documents further distribution by the Government.

i. Control changes to data requirements, price, and delivery schedules.

j. Ensure data availability, at the point of use, in appropriate media and format throughout a defense system life cycle.

k. Ensure adequate control over the release and distribution of defense system data.

l. Ensure that the required DFARS and FAR Patent and data rights clauses are in the awarded contract and that any required/desired additionally negotiated data rights language is coordinated with legal counsel.

m. Provide for the complete visibility of data requirements in contracts.

n. Promote optimum uniformity in the identification, development, formal access, and control of data requirements in and between DoD component and facilitate the exchange of data between DoD components.

5. DATA MANAGEMENT (DM) DUTIES AND RESPONSIBILITIES

5.1 Data manager. Data Managers will work closely with their customers to ensure effective acquisition and management of contractor-prepared data. Customers include, but are not limited to, PMs, Development and Sustainment Commands, Contracting Officers (COs), Configuration Managers (CMs), and other members of the acquisition team.

5.2 Principles. The Data Manager should ensure that the principles and objectives of the Acquisition Manager are adequately supported with the appropriate data through judicious implementation of this manual.

5.3 Component level. Component level Data Managers will assist the PM in developing internal policies and procedures for implementing and achieving the objectives of this document.

5.4 Issues. DM issues that cannot be resolved at the component level should be elevated to the appropriate element of the OSD for resolution.

5.5 Framework. DoDI 5000.02 establishes a simplified and flexible management framework for translating mission needs and technology opportunities and resources, based on approved mission needs and requirements, into stable, affordable, and well-managed acquisition programs that include weapon systems and Automated Information Systems (AISs). It establishes a rigorous, event oriented management process for acquiring quality products emphasizing effective acquisition planning, improved communications with users, and aggressive risk management by both Government and Industry. Also, a description of the key features and characteristics associated with each phase and milestone of the acquisition process is identified. The Defense Acquisition Management System is on Figure 1.

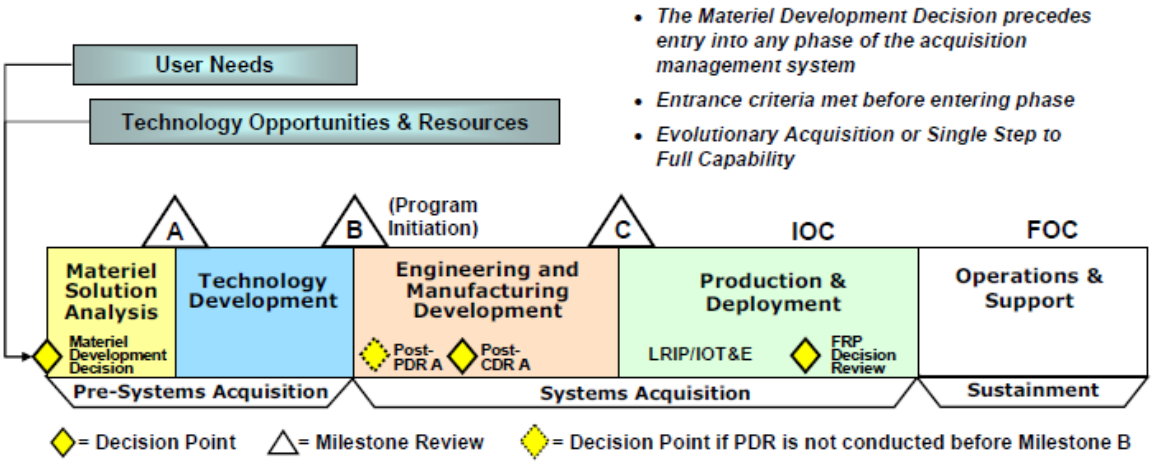

FIGURE 1. Defense Acquisition Management System.

5.5.1 DM guidance documents. While DoDI 5000.02 (Enclosure 12) only mentions DM within the context of sustainment activities, DM is really an integral part of every life cycle phase. The DoD vision for the role of DM within systems acquisition and sustainment is more fully described in the complementary guidance documents: Defense Acquisition Guidebook, Product Support Guide, and Product Support Boundaries.

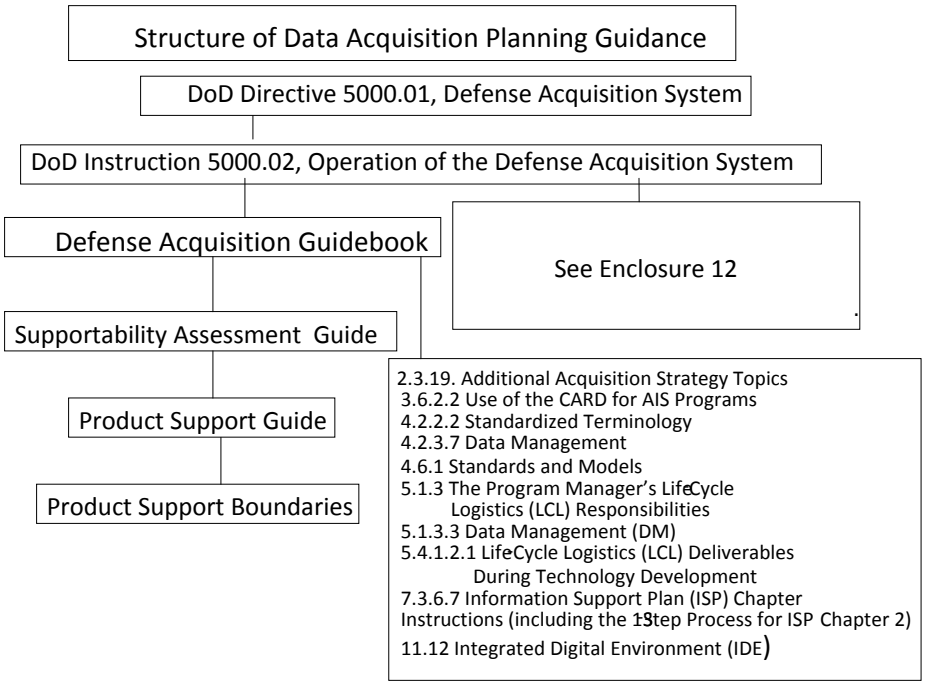

FIGURE 2. The structure of data acquisition guidance.

NOTE: Figure 2 illustrates the structural relationship of these data acquisition guidance documents and cites the primary DM references contained herein.

5.5.2 Relation to guidance documents. Figure 3 depicts how this manual relates to those higher level DoD 5000 series documents and to any lower level service, agency, component, or program specific DM guidance.

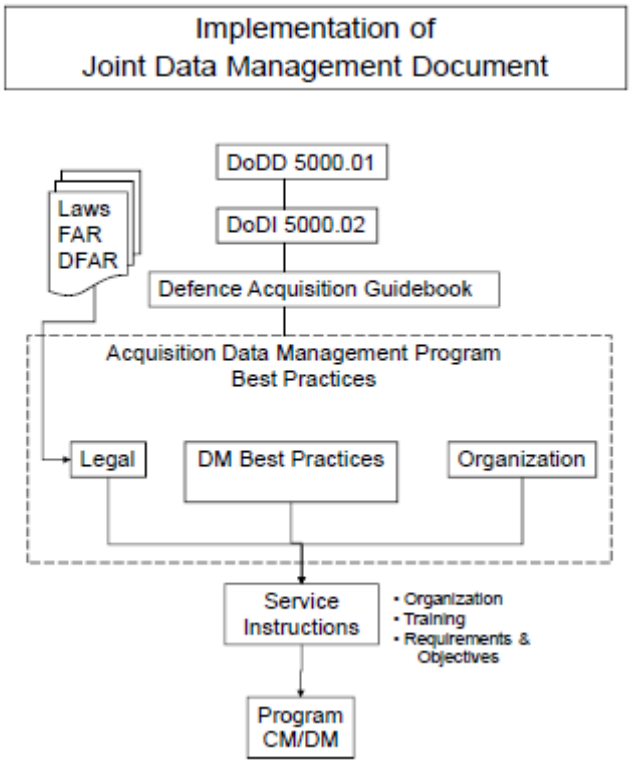

FIGURE 3. Implementation of joint data management document.

NOTE: Figure 3 illustrates how this document relates to those higher level DoD 5000 series documents and to any lower level Service, Agency, Component, or Program Specific DM guidance.

5.6 Roles. Both Government and contractor Data Managers have a role to play in the overall DM planning effort. Since DM is an important part of the Systems Engineering (SE) process, contractors generally describe their DM process in the Systems Engineering Master Plan, and the Government PMs include the Government DM processes and strategies in a program System Engineering Plan (SEP). Programs not using the formal SE process should still plan for and document program data needs and management strategies.

5.7 Use of specifications and standards in acquisition.

5.7.1 Background. Military Specifications and Standards Reform was the driving factor in the Acquisition Reform Initiatives, which identified those military specifications and standards that were cost drivers, incorrect, or the technology had advanced beyond what was contained in the specifications or standards. The use of non-Government specifications and standards is the preferred method in the acquisition process. Many of the military specifications and standards contained "how to" instructions rather than utilizing the "new performance based terms" being introduced under the reform initiatives. However, in some circumstances, Government or military specifications and standards may be more advantageous.

5.7.2 Policy. It is DoD policy to adopt innovative practices, best commercial practices, and to consider the use of performance based strategies for acquiring and sustaining products and services whenever feasible. When using performance-based strategies, contract requirements should be stated in performance terms, limiting the use of military specifications and standards to Government-unique requirements only. This does not preclude data requirements being specified in performance terms.

5.7.3 Non-Government Standards (NGSs) guidance.

5.7.3.1 NGSs. Contractors may propose to use other NGSs that facilitate the production and delivery of items within the parameters of the performance requirements of the acquisition document. Government adopted NGSs can be found in ASSIST.

5.7.3.2 Use of NGSs. The use of non-Government standards usually requires the purchase of the document or access by the Government and contractors. Changes to the non-Government standard may require purchase of the changed document. In order to influence the content of many of the non-Government standards, a DoD representative should be a member or participant of the standards body.

5.8 Training. Each DoD component should establish training programs, as appropriate, for each person assigned responsibilities for the acquisition and management of contractor prepared data, i.e., Data Managers. Training should address the use of the best commercial and/or Government practices to acquire and manage only essential data in support of a defense system throughout the defense system life cycle. To achieve the optimum development of the Data Manager, the recommended training courses are as follows:

AFIT SYS110	Fundamentals of Data Management, PDS Code – 5OQ
AFIT SYS028	Introduction to Configuration Management, Virtual Course (VC), PDS Code: ABO of Service Equivalent
DAU ACQ 101	Fundamentals of System Acquisition Management
DAU ACQ 201	Intermediate System Acquisition
DAU CLE 028	Market Research for Engineering & Technical Personnel
DAU LOG 101	Acquisition Logistic Fundamentals
DAU LOG 201	Intermediate Acquisition Logistics
DAU PBL 236	Performance Based Logistics
DAU PQM 103	Defense Specification Management
DAU PQM 104	Specification Selection and Application
DAU PQM 202	Commercial & Non-Developmental Item Acquisition
DAU PQM 203	Preparation of Commercial Item Descriptions for Engineering & Technical Personnel

NOTE: Key acquisition and PM personnel should receive specialized training in the critical areas of DoD data rights.

6. PLANNING FOR ACQUISITION OF DATA

6.1 General. A critical element of the acquisition process is planning for the acquisition of data to support the life cycle of a defense system. The decision to procure data is the result of a careful examination of the requirements for the data, life cycle cost, and the ability of the Government to maintain and use the data in the future. Since the Government's ability to access and use contractor provided data can range from very limited, due to a lack of data rights, to complete access to or possession of the data, with full rights to use as needed, it is important that alternative approaches for providing the data are evaluated to assure that the necessary Government data rights to support full life cycle needs are met.

6.1.1 DM strategy. Data Managers plan for acquisition and management of defense system data during each phase of the system's life cycle. DM strategy supports the defense system program acquisition, logistic support, and Integrated Product/Process Team (IPT) strategies, and the information processing infrastructure of the program office, support organizations, and field operations (i.e., data users).

6.2 Acquisition Strategy (AS). The AS is a business and technical management approach designed to achieve program objectives within resource constraints. The AS is the framework for planning, directing, and managing a program. The AS provides a master schedule for research development, test, production, fielding, and other activities essential for program success, and for formulating functional plans and strategies; e.g., Test and Evaluation Master Plan, Acquisition Plan (AP), competition, and prototyping.

6.2.1 Framework of AS. The AS serves as the roadmap for program execution from program initiation through postproduction support. Essential elements of AS include, but are not limited to, sources of supply, risk management, cost, contract approach, management approach, environmental considerations, and sources of support. Data acquisition planning, as an integral part of the overall program planning, is essential to sound program management.

6.3 Acquisition Planning (AP). Acquisition planning is the continuing life cycle process of determining, coordinating, and integrating all facets of an acquisition into the overall AS and implementing the AS into a comprehensive AP.

6.3.1 Objectives of AP. The AP is the overall or top-level document that defines the objectives and plan of action for a program. The AP integrates the acquisition documentation required by senior officials into one file. The AP addresses all the technical, business, management, and other significant considerations that should control the acquisition. Elements of a comprehensive AP include a statement of need, compatibility with existing or future system or program, any known cost, schedule, performance constraints, delivery requirements, tradeoffs, risk (management and mitigation), contractor sources; whether competitive or sole source, budget or funding requirements, and other factors relevant to the acquisition. The AP answers the "who, what, when, where, why, and how" of the AS planning process. The AP provides sufficient information so that someone unfamiliar with the program should understand what is being proposed.

6.4 Data Acquisition Strategy (DAS).

6.4.1 Strategy. Planning for the acquisition of data is required by the FAR and the DFARS in order for the DoD to carry out missions and programs. Data is required by the PM and the acquisition team to assure competition among contractor sources; fulfill certain responsibilities for disseminating and publishing the results of acquisition activities; ensure appropriate utilization of the results of research, development, and demonstration activities including the dissemination of technical information to foster subsequent technological development; and meet other programmatic and statutory requirements.

6.4.2 DAS process. DAS is a process by which the resources and efforts of key personnel responsible for the acquisition are integrated. Planning includes the principle elements of decision milestones, contract definition, procurement objectives, schedule formulation, and program execution. The result is the development of an overall strategy for managing the acquisition of data that assures the Government's needs are met in the most effective, economical, and timely manner. The DAS should include identification of the major components or subsystems, component breakout plans, requirements for contractor data (including the re-procurement data), data rights, estimated costs, and the anticipated uses of the data. The DAS will require discussion of:

a. Planned use of warranties for technical data.

b. Requirements for contractor prepared data, including re-procurement data, data rights, estimated costs, and the anticipated uses of the data.

c. The overall program objectives for the acquisition of technical data.

d. Contractor use and certification of the TDP.

e. Planned methodology and schedule for conducting major DM events.

f. Use of DFARS clauses for deferred ordering, deferred delivery, and withholding of payment.

g. Strategies for minimizing the amount of technical data delivered to the Government with other than unlimited rights.

h. Plans for keeping data accurate and current.

6.4.3 In-Process Reviews (IPR). Use IPRs and final reviews of data, when necessary, to establish the Government ability to use the data as intended. A fully developed plan should convey to all readers such information as:

a. What data is needed?

b. When the data is needed.

c. What data is being or will be procured during the current acquisition phase.

d. Who requires and will use the data.

e. What data rights will be obtained?

f. Why that data is being or will be procured (consistent with program goals).

g. What steps the program is taking to enhance future competition.

h. How the data will be accessed, reviewed, inspected, technically approved, accepted, updated, and stored.

i. Who will be involved in the validation process?

6.4.4 DAS considerations. DAS requires updates periodically as programs mature, as key milestones are approached and passed, and as other significant changes occur. However, without adequate planning for the acquisition of sufficient data and the needed rights in that data, the implementation of the AS may be difficult if not impossible.. DAS is necessary, whether or not there is a requirement for full and open competition, in order to obtain the minimal essential data needed for the program. DAS should begin as soon as possible; preferably well in advance of the fiscal year in which contract award is required. Acquisition Data Managers should adapt the previously defined DM principles to defense system programs and user requirements.

6.5 Relationship between program and data acquisition strategy.

6.5.1 Acquisition program. An acquisition program may have a plan and strategy for full and open competition of an item. However, without adequate plans for the acquisition of a TDP, other technical data and management data, the implementation of the AS becomes difficult, if not impossible to achieve. DAS, as an integral part of the overall program planning, is essential to sound program management.

6.5.2 Planning. It is important that the acquisition of data be planned as thoroughly and in as much detail as possible, and performed regardless of the acquisition phase in which a program resides. This planning should assist in establishment of baselines and attainment of exit criteria at phase completion, and assist in the management of risk not only in the next phase, but for the remainder of the program.

6.5.3 Scheduling. Early DAS should center on scheduling the time and the resources needed to develop, review, access, and accept the TDP during the engineering and manufacturing (full-scale) development, production, and deployment phases. Early planning for data acquisition includes:

a. The data acquisition strategy identifies the data to be acquired and accessed, and why the data is to be acquired and accessed. In the case of the defense system, an AS calling for some organic logistics support of the system should require a data acquisition strategy that provides the needed logistic support data.

b. The data acquisition milestones (see figure 4)

c. The key players in data acquisition.

d. The resources required to implement the data acquisition and management of contractor prepared data.

6.5.4 AS elements. The elements of the overall AS include:

a. Competitive development.

b. Competitive production.

c. Multiple sourcing.

d. Life cycle support.

e. Qualifying additional sources or ICPs by internal only Government review of Limited Rights or Restricted Rights data.

6.5.5 Major milestones. The program Data Manager identifies and addresses each milestone of the data acquisition process. To a great extent, the overall AS will dictate what these milestones are and when they would occur. In data acquisition the major milestones include:

a. SOW or SOO preparation (see 7.2).

b. Data call (see 7.3.2).

c. Data Requirements Review Board (DRRB) or equivalent approval (see 7.3.6).

d. Contract award.

e. Data conference and IPRs.

f. Contractor certification.

g. Inspection, acceptance, or rejection of technical data (see Section 17).

6.5.5.1 Data acquisition and management life cycle. Figure 4 depicts the major data acquisition milestones within the context of the typical data acquisition process.

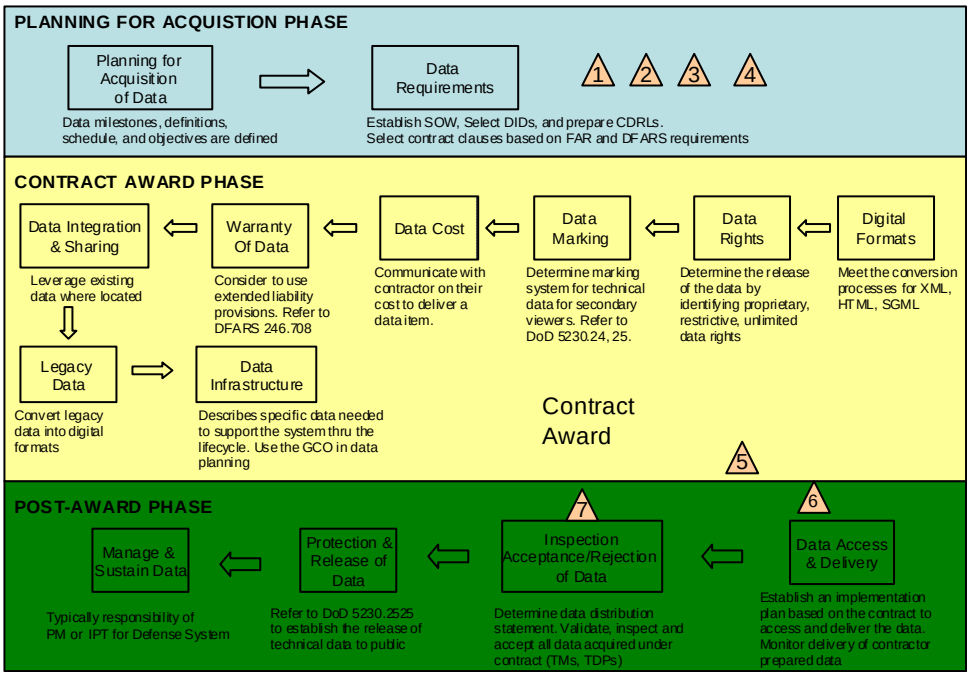

FIGURE 4. Acquisition milestones within the acquisition process

Legend for Figure 4:

Colors.

Blue – indicates actions typically done in the planning phase.
Yellow – indicates actions typically done prior to contract award.
Green – indicates actions typically done after contract award.
Orange – indicates major milestones in data acquisition.

Number Label for Data Acquisition Milestones.

1 – SOW or SOO
2 – Data Call
3 – DRRB or equivalent approval
4 – Contractor Certification
5 – Contract Award
6 – Data Conferences/IPRs
7 – Inspection, Acceptance, and Storage

6.5.6 Milestones and overall program schedule.

6.5.6.1 Program schedule. Clearly, each of these milestones should be established within the overall program schedule. The timing of data acquisition milestones and the time allowed for completion of each milestone should be compatible with the requirement for the data and synchronized with overall schedule. Just as importantly, schedules should be coordinated with activities responsible for performing reviews, audits, inspection, and verification of the data, technical data, and the TDP. For example, if an ISEA, other field activity, or contractor is to be tasked with IV&V of the TDP package, the capability to meet the scheduled award of production contracts should be confirmed and a definite plan for conducting the IV&V developed

6.5.6.2 Other activities. Additionally, other activities may be involved in the data acquisition process. Some may need to participate in data calls; others may be responsible for access, receipt, and storage of the data. The Data Managers should identify these activities, clearly describe the roles of each, identify a responsible point of contact within each organization, and establish schedules for each segment of the data acquisition strategy.

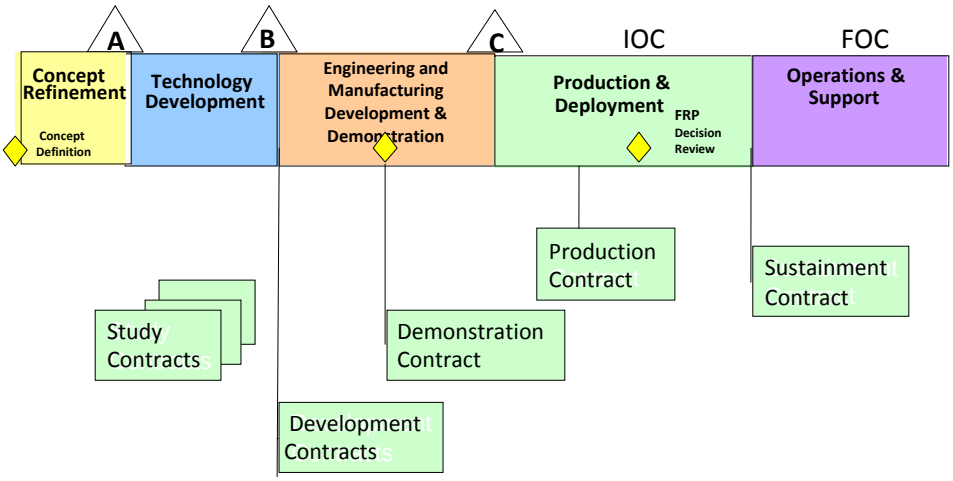

FIGURE 5. Typical Contract Awards during a Defense System Life Cycle.

6.5.6.3 Defense and data life cycle relationship. The relationship between the defense system life cycle and the data acquisition life cycle is illustrated in the combination of Figure 4 and Figure 5. Figure 4 shows the process for the acquisition of data that typically occurs for each contract. Figure 5 shows the process repeats for each contract that may occur throughout the defense system life cycle. The exact types of contracts and the number of contracts should vary for each defense system. The contract type typically is tailored to a particular phase and milestone in the defense system life cycle.

6.6 Integrated Logistic Support Plan (ILSP). The planning for technical data is also addressed in the ILSP. The ILSP requires documentation of hardware and software technical DM acquisition and management strategy, including delivery of digital data, review activity, post-production support, engineering data requirements, inventory control point data requirements, data rights, data warranty, and drawings.

6.7 Acquisition team. The acquisition team (or equivalent) consists of all participants in a Government acquisition including representatives of the technical, logistics, procurement communities, the customers they serve, other possible functional areas, and the contractor who provides the product or services. The acquisition PM is the principal resource manager responsible for execution and achievement of acquisition goals and assignment of the Data Manager for the program. Requirements for contractor prepared data, including re-procurement data, are identified in a solicitation and imposed in a contract or order. The requirements address every aspect of the individual data product; i.e., that portion of the contract tasking requirements associated with the development, generation, preparation, modification, maintenance, storage, retrieval, access, management, use, distribution, and/or delivery of data. Data Managers, as members of the acquisition team, perform the duty of abstracting the data required for the life cycle of the program (see Figure 7).

6.8 Support contractors. Unless additional statutory authority is granted, the Government may allow support contractors access to or use of another contractor's data only when the Government has Unlimited Rights or Government Purpose Rights in that data. Minor exceptions can be found in the DFARS clauses. When the contractor has asserted greater limitations upon the Government's use (such as Limited Rights and Restricted Rights) those limitations may be waived by the contractor (explicity and in writing) or challenged by the Government.

7. DATA REQUIREMENTS

7.1 Defense system data. Defense system data is acquired when needed to support the life cycle acquisition, operation, maintenance, support, or disposal of the system.

7.1.1 Program office responsibility. Program offices should coordinate with affected data users through the Data Manager when selecting data for ordering and when evaluating the technical, cost, and programmatic factors associated with data requirements. Acquisition PMs should state the requirements in clear and concise terms to support the acquisition approach for the program, minimizing format and contract restrictions while maximizing cost benefits and intended use analysis. Requirements need to be communicated consistently in the contract and at all tiers of the acquisition.

7.1.2 Generating requirements. The contract work tasks, specifications, and standards generate the requirements for data. MIL-STD-961 contains preparation instructions for specifications and MIL-STD-962 contains preparation instructions for standards. Figure 6 depicts the relationship between data acquisition documents. During the DID selection process it may be necessary to generate a new DID in support of the program requirements. MIL-STD-963 contains preparation instructions for the development of DIDs. The PM should ensure that data acquisition documents are tailored, delivery requirements are specified, and any special instructions and ordering requirements are documented in the DD Form 1423, CDRLs.

7.1.3 Data acceptability. Data being ordered should be delivered, inspected, and accepted per the FAR, DFARS, and the applicable contract requirements. The inspection and acceptance requirements cited in the contract apply regardless of method of delivery.

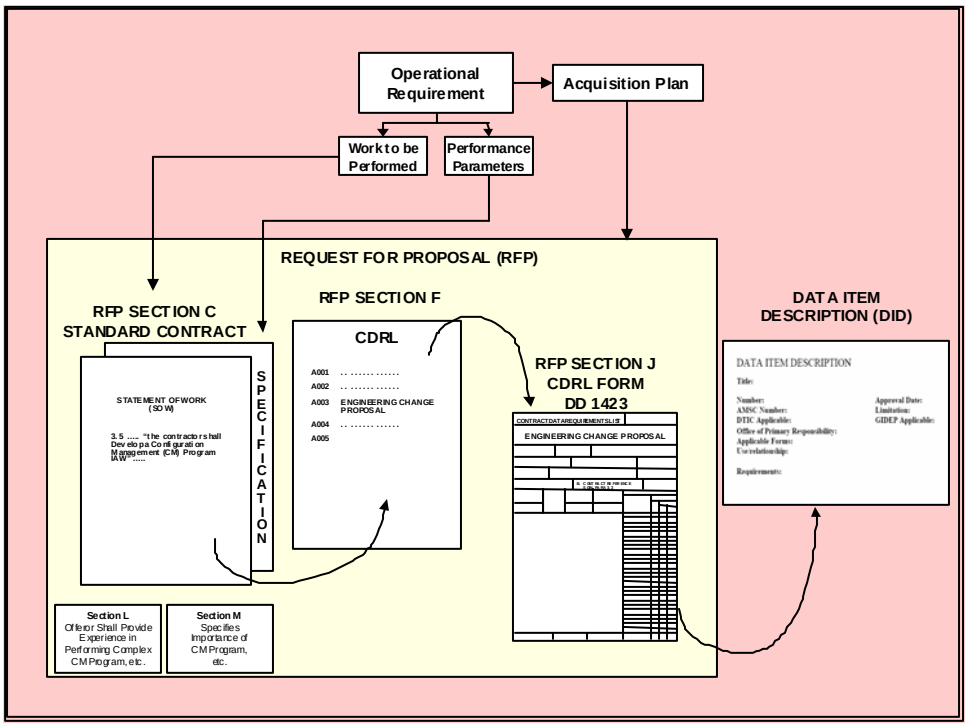

FIGURE 6. Relationships between data acquisition documents.

7.2 Major data acquisition documents.

7.2.1 General. Many acquisition documents are created during the course of preparing for a contract solicitation. One of the very first documents created that should prove useful in determining data requirements is the AS, and together with the AP, it provides insight into the specifics of the data that will be needed to support the defense system or product throughout the life cycle. The major contracting documents used for data acquisition are the SOO, SOW, CDRLs, Contract Provisions, and Contract Clauses. All documents should not be used on every contract requirement package, but may vary depending on the specific requirements of the solicitation. The PM, IPT, and legal office, in conjunction with the contracting officer, may identify, determine, and review the contract provisions and clauses for use in the acquisition.

7.2.2 Statement of Objectives (SOO). The SOO is a Government prepared document incorporated into the RFP. The SOO states the overall solicitation objectives in top-level broad and basic terms. It can be used in those solicitations where the intent is to provide the maximum flexibility to each offeror to propose an innovative development approach. Offerors use the RFP, program performance requirements, and SOO as a basis for preparing their proposals. The key to writing a SOO is to keep the requirements clear, concise, and to provide potential offerors with enough information and detail to structure a sound program, designed to be executable and to satisfy Government objectives. It should be noted that the SOO is not retained as a contract compliance document, and that it shifts the responsibility for preparing the SOW from the Government to the contractor. (See Section 5 of MIL-HDBK-245 for additional information.)

7.2.3 Statement of Work (SOW). The SOW should specify in clear and concise terms the work to be done in developing or producing the product or services to be performed, and/or delivered by the contractor. A SOW prepared in explicit terms will enable offerors to clearly understand Government needs. In addition, a well written SOW enhances the opportunity of all potential offerors to compete equally for Government contracts, and serves as the standard for determining if the contractor meets the stated performance requirements. MIL-HDBK-245 contains clear and concise guidelines for preparing SOWs, appropriate for each phase of the acquisition life cycle. (Section 4 of that reference contains detailed instructions on the specific requirements for each type of SOW tailored to specific needs.) The SOW defines, either directly or by reference to other documents, all work performance requirements. A well-written performance based SOW should:

a. Structure all aspects of the acquisition around the purpose of the work to be performed.

b. Not dictate "how" the work is to be accomplished.

c. Ensure contractors are given freedom to determine how to meet Government performance objectives.

d. Provide for positive incentives when the results meet or exceed the objectives.

e. Maximize contractor control of work processes.

f. Allow for innovation in approaching work requirements.

g. Emphasize performance that can be contractually defined to measure contractor results in terms of technical and quality achievements, schedule progress, or cost performance.

h. Be definitive enough to protect Government interests.

i. Serve as a basis for contractor response, evaluation of proposals, and source selection.

j. Ensure statements of requirements are written in a style that eliminates the possibility of more than one interpretation; legal participants should be utilized to avoid misinterpretations.

k. Provide a realistic balance among elements in keeping with the program acquisition phase.

l. Make maximum use of current federal, military, and nationally recognized industry specifications and standards.

m. Use tailoring and streamlining effectively to adapt existing specifications and standards to actual program requirements.

n. Minimize the Government's control, which may preclude contractor's creativity.

7.2.4 Contract Data Requirement Lists (CDRLs), DD Form 1423. The purpose of the CDRL is to provide a standardized method of clearly and unambiguously delineating the Government minimum essential data needs. The CDRL groups all of the data requirements in a single place rather than have requirements scattered throughout the solicitation or contract. CDRLs are linked directly to SOW requirement paragraphs and are managed by the Data Manager. Data requirements can also be identified in the contract via Special Contract Clauses, such as DFARS clauses, which can define special data provisions; i.e., Rights in Data, Warranty, etc. The CDRL is the standard format used to order data and also identifies the required method of delivery (e.g., electronic or hardcopy) and the location (e.g., data repository, office or computer address). The DD Form 1423 or electronic equivalent may be used. DFARS Subpart 215.470 requires the use of the CDRL in solicitations when the contract will require delivery of data. See Appendix B for the preparation guidance for the CDRL.

7.3 Identification of data requirements. The data requirements identified in the contract should be consistent with and support the program AS, life cycle maintenance, and support concepts and be acquired in a timely manner to support user needs. Data requirements are usually derived from the SOW tasks.

7.3.1 General. Data requirements should fall within the range of data and data formats contractors typically generate in performing development, production, or service contracts.

7.3.2 Data call.

7.3.2.1 Time frame for data call. Data Managers issue data calls prior to release of the RFP or sealed bid. Data Managers should conduct the data call early enough to translate data requirements identified in the data call into contractual requirements.

7.3.2.2 Program information. The data call should provide or refer to all program information pertinent to each functional area receiving data or data user decision on the proposed acquisition regarding program data requirements.

7.3.2.3 User information. The data call should obtain the data user information or requirements needed to create the GCO for an IDDE or similar environment.

7.3.2.4 Functional areas. The data call should include all functional areas that support the defense system or representation on an IPT. The data call should also include the operational end user of the data, the system or project management team, and contracting office. Figure 7 depicts the generation of data requirements.

7.3.2.5 Identifying the data manager. The Data Manager or equivalent working under the direction of the PM should be involved in setting up the initial IPT meeting. The Data Manager contacts all the functional area representatives for a meeting to discuss program requirements, documents preliminary SOO and SOW input and revisions, and defines applicable data acquisition documents and DIDs.

NOTE: The PM, along with the user, when possible, can provide the program requirements and obtain any preliminary inputs before developing a SOW requirements document, etc. and allow the functional areas to determine whether or not they have any requirements in support of the acquisition. The functional areas should develop any appropriate documentation identifying their requirements. This documentation should be incorporated into the SOW or requirements document.

7.3.2.6 Additional data calls. Subsequent data calls can be planned to eliminate any errors in the SOW or requirements document, review any previously prepared CDRLs, eliminate duplication of CDRLs, develop source selection criteria for the different functional areas, and to allow input to Section L and M of the solicitation.

7.3.2.7 Final data call. A final data call is conducted to accomplish a review of the complete SOW or requirements document, CDRLs, and Sections L and M of the solicitation. This should allow the Data Manager to sign off all the CDRLs.

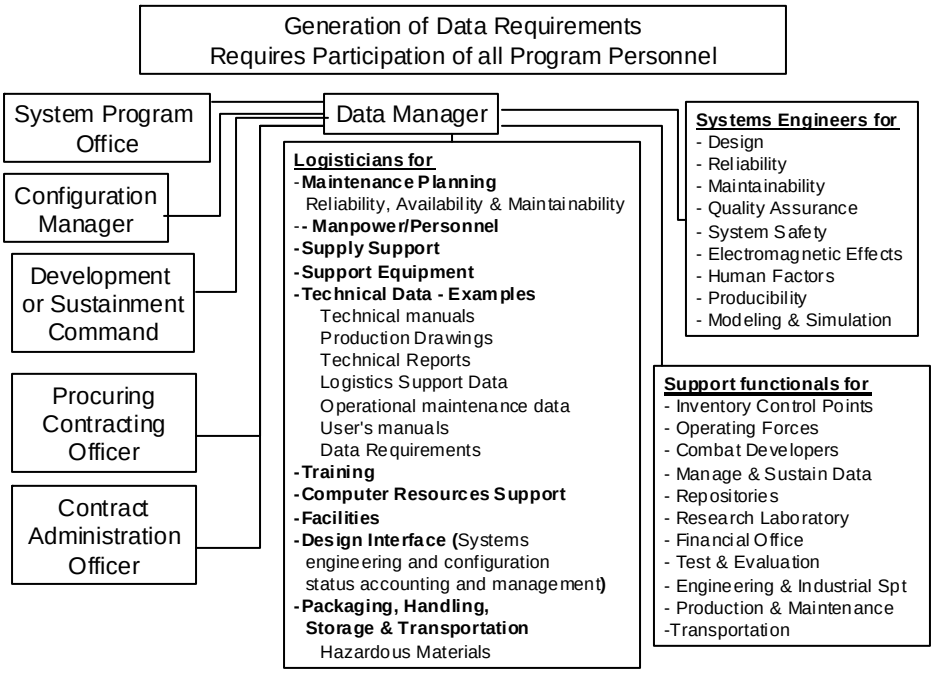

FIGURE 7. Personnel required to generate data requirements.

NOTE: Figure 7 depicts the relationships between the Data Manager and the rest of the acquisition team.

7.3.3 Data call responses

a. Each data call participant should identify specific, minimum essential data requirements based on the life cycle needs of the defense system, tailored to prevent unnecessary data preparation. Data call participants should refer to the SOW or other requirements documents to determine whether a valid contract requirement supports the proposed data requirement.

b. Data call participants should tailor source documents cited for tasking purposes to delete unnecessary data preparation tasks. When such documents do not provide clear data requirements, the data call participants should write the tasking requirements into the SOO, SOW, or PWS in concise and unambiguous terms.

c. All data requirements included in a solicitation or contract should be selected from the listing of Office of Management and Budget (OMB) cleared documents. Refer to ASSIST for lists of cleared data acquisition documents (i.e., military specifications, military standards, and DIDs). Data acquired by any data clause of the FAR, DFARS, or EPA Title 40 is, however, exempt from this requirement. If already cleared DIDs are deemed inadequate, then one-time DIDs may be prepared in accordance with MIL-STD-963. Preparation of a one-time DID is to be accomplished by the requiring office with the assistance of the Data Manager. The DoD component focal point is responsible for assigning an identification number to the one-time DID and for ensuring that this DID is used on only one specific contract. The office of primary responsibility may also be contacted to request revision of the DID.

7.3.4 Integrated Product Teams (IPTs).

7.3.4.1 IPT members. Organizations can use IPTs to generate data requirements. IPTs are cross-functional teams that are formed for the specific purpose of delivering a product or service to a customer. IPT members should have complementary skills and be committed to a common purpose.

7.3.4.2 IPT requirements identification. The acquisition manager or PM can assemble one or more IPTs to support a given acquisition program. The IPT will specifically define data requirements. The IPT should consist of all those who access, use, manage, specify, or are otherwise affected by the functional data throughout the product life cycle. The IPT works to ensure that the data requirements are the minimum essential necessary to support the program.

7.3.5 Consolidation of data requirements. To avoid duplication of effort and reduce costs, the Government data requirements should, whenever possible, be satisfied by data previously submitted to the Government in response to the most basic data requirements placed upon the contractor. Similarly, in developing the current requirements package, Data Managers should, where appropriate and practical, take into consideration the impact of any known or anticipated future data requirements for the entire program life cycle.

a. The Data manager should consolidate all data requirements into one coherent package, eliminate duplication of requirements, and resolve any inconsistencies of requirements with the AS or other data requirements.

b. Data managers should ensure that the data requirements are documented via approved and properly tailored "data acquisition documents."

7.3.6 Data Requirements Review Board (DRRB). A DoD component should establish a DRRB, FRAB, or equivalent to authenticate contract and data requirements, including the corresponding SOW tasking requirements, for any acquisition having an estimated total contract cost of $10,000,000 or more. The DoD components may establish lower dollar thresholds based on the circumstances of the acquisition. The DRRB or equivalent may be conducted separately or incorporated within the IPT process. The functionality and review levels described below should be followed regardless of the forum selected.

7.3.6.1 DRRB membership. The DRRB membership represents a cross section of defense system subject matter experts that have direct authority to approve or disapprove the data requirements and associated tasks for the respective functions.

7.3.6.2 DoD components. The DoD components usually vest the DRRB Chair with total decision authority for all DRRB actions. However, a DoD component may allow higher organizational levels to review DRRB decisions, if requested by dissenting members.

7.3.6.3 DRRB function. The function of the DRRB is to review all data requirements to ensure that data requirements are appropriate to the program, reduced to the minimum essential set, and properly specified in the

contract.

7.3.6.4 DRRB threshold. For acquisitions having an estimated total contract cost in excess of $10,000,000, DoD components should perform data reviews. For acquisitions without a DRRB, the organizational Data Manager should perform the functions of the DRRB.

7.3.7 Data manager roles and responsibilities.

a. Ensures that all valid requirements for technical data are identified by functional area, coordinated among functional areas, and consolidated to eliminate redundancy.

b. Determines when the data will be needed during the acquisition life cycle.

c. Verifies that work tasks, which will generate the required technical data, are set forth in appropriate specifications, the SOW, or contract clauses.

d. Informs and advises the contracting officer and the PM of the importance of ensuring that the prime contractor is required to flow down data requirements to subcontractors and vendors. If flow down is a contract requirement, the Data Manager will monitor the data deliverables or formal access.

e. Ensures that all technical data requirements are expressed in terms of currently approved data acquisition documents.

f. Verifies that technical data requirements are expressed in terms of currently approved "data acquisition documents."

g. Ensures that tailoring is accomplished for data items on the appropriate document. Tailoring is specified in Block 16 of the DD Form 1423 or the document summary list. Keep in mind that tailoring can only be accomplished downward. The DID requirements can be tailored "down" or "out" in Block 16 of the CDRL. DID requirements cannot be tailored "to enhance" or "up" in Block 16 of the CDRL.

h. Monitors progress of data requirements. Data Managers should monitor delivery of contractor prepared data by establishing procedures for the receipt, inspection, acceptance, and access of the contract data prior to and after contract award. When appropriate, the Data Managers should validate that the contractor has properly enabled the Government inspection and acceptance of deliverable data through "On Line Access" or other electronic methods. Validation can consist of an electronic message from a responsible official of the contractor that notifies the appropriate Government organization that specific contract data is available for inspection and acceptance. Data Manager should then confirm delivery of validated data by the scheduled delivery data by:

1). Establishing and maintaining a schedule of all contractor deliverables and tracking the status.

2). Apprising management of the status of active data items, schedules, and reporting any data scheduling problems.

3). Coordinating the delivery of contractor deliverables.

4). Monitoring data deliverables to ensure compliance with the CDRL.

8. DIGITAL FORMATS

8.1 General. When acquiring data on contracts, the general rule is to acquire data in a digital format suitable for the data's intended use. The Data Managers or other appropriate authorities should ensure that digital data formats and versions are consistent with the organization's existing operational and archiving requirements and environments. Other formats may be added, as required, to address additional strategies or needs.

8.2 Formats. Choices of desired digital data formats include neutral formats, formats native to a particular application, or organization (DoD or company) standard digital formats.

8.2.1 Neutral formats. Neutral formats include industry standards, such as the American Standard Code for Information Interchange (ASCII) for text or STEP model data, which are usable by a variety of different applications.

8.2.2 Native formats. Native formats are those automatically generated by a particular application, such as a word processing or Computer Aided Design (CAD) program, are usually proprietary to the company making the application and readable only by that application or a few others. Use of a company proprietary format is usually recommended only when it is part of your organization's existing standard set of formats, or when it is required to

obtain essential information and further use within DoD is unnecessary. Some native formats, such as Rich Text Format (RTF), or Portable Document Format (PDF), while proprietary, are viewable or processable by enough other programs or by free software, that their use by the Government does not incur additional costs, but may limit the uses of the data. For example, PDF format is readily viewable by free viewers but cannot be further manipulated or changed without Adobe Company proprietary software.

8.2.3 Organizational standard formats.

a. Organizational standard formats can be neutral or native, but are formats selected by a particular data ordering organization for their internal use. In this case, the organization has applications that can make full use of these formats, so no additional cost is incurred in using these formats.

b. Native data formats, such as native CAD, are dependent on the software that created the data and thus subject to a risk of not being usable after many years of archival if the original creation software or version of that software is no longer available. If the intent of the data is for long-term use and archiving, then preference should be given to neutral formats based on industry standards in order to maximize long-term data utility.

8.3 Data and technical data types.

a. Data may be classified into various types based on their specific use in support of an acquisition program or the operation and support of an item. Examples are: management data, financial data, administrative data, cost and pricing data, technical data, computer software, and other data.

b. Technical data may be further classified into other types of data based on its specific use in support in the operation and support of an item. Examples are: maintenance data, including reliability, availability, and maintainability data; provisioning data; cataloging data; standardization data; logistics technical data, including re-procurement technical data; engineering drawings; TMs; packaging data; hazardous materials data; Logistics Management Information (LMI), also known as Logistics Support Analysis (LSA) or Logistics Support Analysis Records (LSAR); and manpower, personnel, and training data. There are many ways contractors communicate operation and maintenance requirements and data to the users. TMs are one way this is done. Figure 8 illustrates the relationship between the various types of data and technical data.

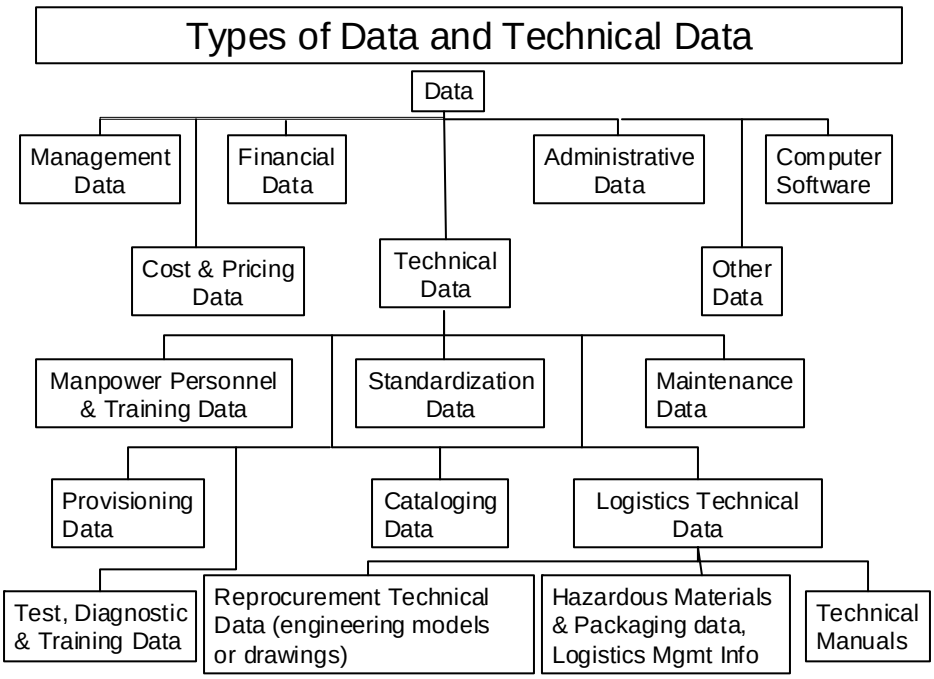

FIGURE 8. Relationship between the types of data and technical data.

NOTE: Figure 8 illustrates the relationship between various types of data and technical data. This is not an all inclusive list of data but identifies some "top" level types of data.

8.4 Summary of data formats and conventions.

8.4.1 Types of data. Table I provides a sample listing of many types of data and the related standards that should be used to make intelligent format selection decisions. In each case, several formats and content options are available and 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 Table I, which can be used, were applicable.

TABLE I. Sampling of types of data and related standards.

Type of Data	Related Standard(s)
IETM/ETM	MIL-PRF-28001 MIL-STD-40051 S1000D
IETM/ETM Graphics	MIL-PRF-28003 MIL-PRF-28002
Other Drawings/Graphics	MIL-PRF-28000 ISO 10303 AP 201, 202 ASME Y14.26 ASME Y14.100 MIL-DTL-31000
Logistics	MIL-PRF-49506 ISO 10303, AP 239 UK DEF STAN-0060 GEIA-STD-0007
Packaging	MIL-STD-2073-1
Reliability, Availability & Maintainability	MIL-HDBK-338
Text	ASCII TXT, etc.
Cataloging	DoD 4100.39-M
Configuration Management/ Data Management	MIL-HDBK-61, ANSI/EIA 649 ANSI/GEIA 859

NOTES:

1. DI-SESS-81000 identifies the applicable DID numbers for use with engineering and technical data, and product data. The DID number for Product Drawings/Models and Associated Lists contains the format and content preparation instructions resulting from the work task described in MIL-DTL-31000. Tailoring of this DID require the use of TDP Option Selection Work Sheets from MIL-DTL-31000, together with content information found in ASME Y14.100.
2. For technical manuals, the DoD is striving for neutral format data by requiring use of XML based on W3C recommended guidelines. This non-proprietary XML is prepared in accordance with buying agency supplied DTD or Schemas. The XML is then displayed by XSL 1.0 or 2.0 stylesheets for presentation in either page based (e.g., PDF) or framed based for Interactive Electronic Technical Manuals (IETM). The stylesheets for IETM should reflect the Joint Service guide for common look and feel.

9. GOVERNMENT LICENSE RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE

9.1 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 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 merely takes a license in the Data. This remains true even when the Government exclusively funds development costs.

9.2 Data license rights: automatic and based on funding. Certain license rights in Data arise automatically upon contract award 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 license rights (e.g., "Unlimited Rights" and Government Purpose Rights") are created by direct Federal funding for the development of related items, components, or processes (ICPs).

9.3 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.

9.4 Data license rights categories. There are five 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. All such special negotiations should be reviewed by Government legal counsel. In all categories below, a copyright marking by the contractor is allowed and such marking is not inconsistent with the stated license rights.

9.4.1 Unlimited rights in technical data and computer software. There is 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. This category applies to commercial AND noncommercial Data. The Government may share this Data with anyone for any reason.

9.4.2 Government purpose rights in technical data and computer software. If neither party proves exclusive (100%) funding by that party, then the development of an ICP is generally presumed to have been with mixed funding. The Government receives a "Government Purpose rights" 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 NDA. This category applies only to noncommercial data. There is only one contractually authorized marking for such data.

9.4.3 Limited rights in technical data. When the contractor has exclusively (100%) funded the development of an 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.

9.4.4 Restricted rights in computer software. When the contractor has exclusively (100%) funded the development of computer software, the Government receives "Restricted Rights" in that computer software for which the Government has not received automatic "Unlimited Rights." Automatic rights 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

9.4.5 Special License rights 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 increase it rights by negotiation (without coercion) to "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.

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

9.5.1 Asserting. A proper assertion is one made before award (and incorporated into the contract) or made prior to delivery (and justified as a "new" or "inadvertent omission" not affecting source selection). 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."

9.5.2 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 specific form but may not contain limiting words);

- Government Purpose Rights;

- Restricted Rights (computer software);

-Limited Rights (technical data);

-Specially Negotiated Rights.

The restrictive/limiting markings (Government Purpose Rights, Restricted Rights, Limited Rights, and special License Rights) must be limited to the Data on each page (by circling or other method of identifying appropriate pieces of Data on that page) which is subject to that asserted limitation/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/restriction.

9.6 Correcting Assertions and Markings Regarding Data Rights. "Unauthorized" assertions/markings are those which are not covered by a current assertion or which are not in the contractually specified format. The Contracting Officer may order these unauthorized markings to be removed/corrected within 60 days of notification. "Unjustified" assertions/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.

10. DATA MARKING

10.1 Distribution statements on technical data. In accordance with10 U.S.C. § 130, a DoD distribution marking system for technical data (to included computer software) has been established by DoDD 5230.24 and DoDD 5230.25. Depending on the technical content of the data, one of seven distribution statements defined in

DoDD 5230.24 is to be applied to indicate the extent of secondary distribution that is permissible without further authorization or approval of the controlling DoD office. The intent of this system 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, this system 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.

10.2 Export control-warning notice. The marking system requires the use of a warning notice on all documents that contain export controlled technical data. That notice is used in conjunction with any of the six limited distribution statements ("B," "C," "D," "E," "F," or "X"; refer to DoDD 5230.24). Distribution Statement A, which authorizes public release, cannot be used in conjunction with the export control notice. The exact wording of the notice should be in accordance with DoDD 5230.24. Procedures for dissemination of this technical data outside of the U.S. Government are contained in DoDD 5230.25. Due to several overlapping and outdated regulations, it is recommended using either a "B" or "E" Distribution Statement for contractor data/documents in which the Government has less than "unlimited" rights.

10.3 Foreign disclosure. Marking requirements with respect to foreign disclosure is directed by the following documents:

a. Executive Order 10865

b. Executive Order 10909 (amendment of Executive Order 10865)

c. Executive Order 12829

d. DoDD 5220.22

e. DoD 5220.22-M

Technical data will be reviewed to comply with these requirements.

10.4 Marking requirements.

a. Mark 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. Distribution statement markings are mandatory for all newly generated technical data. DoD managers of technical programs 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. This requirement does not apply to contractors' technical proposals or similar documents submitted in anticipation of contract award.

b. In the case of unmarked technical data the controlling DoD office will determine releasability in accordance with DoDD 5230.24, DoDD 5230.25, and DoD 5400.7-R. Technical data not marked with a distribution statement, export control warning notice (where applicable), destruction notice (where applicable), etc. should be reviewed and managed by the controlling DoD activity.

c. Each revision should be considered new technical data to be reviewed and marked appropriately. Whether or not previous versions of that data have been publicly released should not be the determining factor in the dissemination determination.

d. Although six of the seven distribution statements indicate that public disclosure may be inappropriate, Data Managers and other DoD personnel should be aware that distribution statements are not in themselves authority to withhold unclassified technical data from public disclosure. Such determination should be made in accordance with DoDD 5400.7.

10.5 Responsibility for marking.

a. It is the responsibility of the controlling DoD activity to select the correct distribution statement and to ensure that corresponding letter code, "A," "B," "C," "D," "E," "F," or "X", is annotated in Block 9 of the DD Form 1423. Additionally, Block 16 of the DD Form 1423 should contain the exact verbiage of the applicable distribution statement identified for the data product.

b. The controlling DoD activity will coordinate the distribution statement requirements with respect to the statutory and regulatory requirements governing the export or other dissemination of technical data.

c. In the case of joint sponsorship of technical data, the controlling DoD activity is determined by advance agreement and may be a party, a group, or a committee representing the interested activity or component.

d. When the Government desires to have the contractor initially mark deliverable data with the appropriate Government designated Distribution Statement and limited/restrictive contractor markings on the data are possible, the contract instructions must be phrased in the alternative: For all data marked with less than "unlimited rights" by the contractor a Distribution Statement of "B or E" shall be used and the reason of "proprietary information" listed as a minimum. For "unlimited rights," a Distribution Statement (insert controlling activity determination to include basis wording – "C or D' is often used.

10.6 Destruction and handling. All unclassified technical data marked with distribution statements "B," "C," "D," "E," "F," or "X" may be handled and destroyed as "For Official Use Only" (FOUO) documents, in accordance with DoD 5400.7-R. Classified, limited technical data should be handled and destroyed in accordance with the procedures of DoD 5200.1-R and DoD 5220.22-M.

10.7 Changes to markings.

10.7.1 Controlling DoD activity. The controlling DoD activity will notify the proper technical data dissemination facilities, e.g., repositories, when the controlling DoD activity is re-designated, the office address is changed, or the markings or statements are changed. An official change to the to the Distribution Statement is "not" required for the DoD controlling activity to authorize other specific releases, i.e. when a Distribution Statement B or E is present solely due to "proprietary information." The DoD controlling activity may routinely authorize release of "Government purpose rights" data to other Government contractors for Government purposes on the condition that a DFARS NDA is executed in advance. This qualification may even be added to the Distribution Statement wording.

11. DATA PRICING

11.1 General. The estimated price of each requirement for technical data to be included in the contract solicitation should be either developed by the requiring DoD component or obtained from potential contractors.

11.1.1 Price estimates. Price estimates should be used in making initial decisions and judgments as to whether or not the requirement for technical data should be included in the contract. The level of effort put into developing price estimates should be related to or dependent upon the importance of the data products to making management decisions. Obtaining technical data at a fair and reasonable price is the goal of all involved in the contracting process. In achieving that goal, good management practices ensure that the prospective contractors and the Government have a mutual understanding of the technical data requirements, especially complex digital data products, and services, to be contractually provided.

11.1.2 Pricing goals. To achieve pricing goals, contracting officers, PMs, technical data managers, or functional area managers are encouraged to enact or use separate contract line items in the contract for Technical Data Packages, Technical Manuals, and other data requirements. When the acquisition of greater rights in technical data is a factor, the contract should contain a separate line item for these rights.

11.1.3 Offerors. Offerors are asked to provide a price estimate for each technical data requirement. If the price estimate appears unreasonable, the offeror may not understand the technical data requirements. Should there be any questions or concerns as to whether the contractor has an understanding of the technical data requirements during the source selection process, contact the contracting officer for guidance before making a decision to delete or retain the data requirement.

11.2 Pricing CDRL items.

a. The requiring activity uses DD Form 1423 in solicitations when the contract will require delivery technical data by any means; hardcopy, electronic copy, or formal access. Every offeror is tasked to provide a price estimate for each technical data requirement. The requiring activity should determine if a solicitation should identify a separate line item for technical data, which allows data to be priced separately from the administrative, development, design, or production tasks.

b. When pricing CDRL data items, the contractor pricing methods should include all costs for method of delivery indicated, in order to support the Government reviews and audits of technical data products and the management of separate or integrated database systems.

c. The requiring activity uses the price estimate to determine whether or not it can afford the data. If the requiring activity determines the price is too high, it can modify the requirement or delete it completely.

d. It is critical to understand that data used or generated in performing the contract will be paid for regardless of any scheduled delivery. Adding a requirement for delivery of such data in the contractor's format merely adds reproduction and administrative review costs.

11.2.1 Retention of pricing information. Retention of Cost Analysis Reports and CDRL price estimate information should be maintained by the project office for the following reasons:

a. Developing technical data costs on follow-on acquisition.

b. Developing estimated technical data costs for new acquisitions.

c. Determining cost versus need of technical data.

d. Identifying cost drivers.

12. WARRANTY OF DATA

12.1 General. Warranties on technical data should be obtained when practicable and cost effective. The factors in FAR 46.703 for traditional warranties should be considered in deciding whether to obtain warranties of technical data via DFARS 252.246-7001. The following should be considered in deciding whether to use extended liability provisions (clauses alternates):

a. The likelihood that correction or replacement of the non-conforming data, or a price adjustment, will not give adequate protection to the Government.

b. The effectiveness of the additional remedy as a deterrent against furnishing non-conforming data.

13. DATA INTEGRATION AND SHARING

13.1 General. While the majority of this document is focused on the activities involved in ordering, accessing, and receiving newly developed data, it should be remembered that much of the data of interest to the Government already exists. Some of it will reside in one or more Government data repositories and even more exists 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. The concept of "Data Integration", therefore, involves leveraging existing data by:

a. Locating the required data wherever it resides.

b. Obtaining, both legally and technologically, the ability to access or obtain the data where it resides.

c. 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.

d. Maintaining configuration control of the master copy of all accessed or shared data.

13.2 Availability of existing data. Determining the availability and location of existing data is not an easy task. Most Government and industry data repositories are separate and stand alone IT systems with no readily accessible index of the contents. Users currently need an account on many systems in order to access data.

13.2.1 Military Engineering Data Asset Locator System (MEDALS). MEDALS serve as the DoD single central locator system for engineering drawings. DoD technical data repositories, which receive, store, maintain, and distribute engineering drawings, supply MEDALS program with technical drawing indexing data and associated information. The MEDALS program in turn supplies this information to its customers along with drawing location(s). The MEDALS program indexes information from the primary component repositories (e.g., Joint Engineering Data Management Information and Control System [JEDMICS]) and various Product Data Management (PDM) systems).

13.2.1.1 MEDALS index entries. DoD components will establish and maintain index entries in the MEDALS program of all technical data maintained in component repositories. DoD components will coordinate the data elements for those indices with other components to maximize the interchange of data assets. Each component will maintain control procedures for the component's engineering data indexed in the MEDALS database using a

combination of document numbers, part numbers, NSN/NIIN, and titles.

13.2.2 DoD evolving enterprise effort. DoD has several enterprise IT initiatives underway to provide an ability to manage the data associated with acquisition program life cycle. Several of the initiatives have a stated goal of containing the index information for all data associated with items managed. Examples of these enterprise initiatives include (but are not limited to) the Single Army Logistics Enterprise (SALE), the DLA Enterprise Business System (EBS) project, Navy Enterprise Resource Planning (ERP) efforts, and various Air Force Information Technology (IT) or Data Warehouse efforts. None of these efforts provide a "universal" data index, but each should provide significantly improved capabilities for data searching.

13.2.2.1 Implementation of Net-Centric Enterprise Services (NCES). DoD is also in the process of implementing the NCES concept. NCES will provide a combination of a secure Government operated network and extensive use of metadata tags. This combination will provide a comprehensive list of available data, wherever it resides. The NCES concept is currently being implemented as part of DoD's Global Information Grid (GIG) project. DoD GIG policy requires all data that will be or has the potential to be accessible or exchanged, to be tagged (using metadata tags) in accordance with the JTA standard for tagged data items (e.g., XML. Metadata tags should be registered in accordance with the DoD XML Registry and Clearinghouse policy and implementation plan.

13.3 Access to existing data. Once the Data Manager has identified and located the data they are interested in, the decision should be made regarding how best to access or obtain it. Section 19 herein describes issues to be considered when deciding whether to access existing data "in place" or to require delivery of data to the Government. 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.

13.3.1 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:

a. Defining the data to be accessed.

b. Determining the time periods during which data will be accessible.

c. Specifying the required or acceptable data formats.

d. Addressing the type of data access protocols to be used.

e. Determining the protection required for the overall system security, classified data, sensitive but unclassified data (e.g., proprietary data).

f. Identification of access rights, rights to use the data.

g. Specifying any additional data services to be provided (e.g., interfaces for seamless Government access, maintain the systems, and the data to be accessed).

h. 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.

13.3.2 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.

13.4 Data integration. Data integration is the ability to share data between different organizations and users. This feature is instrumental to any attempts to collaborate actions between business partners. Collaboration services allow users to work together and jointly use selected capabilities and shared data on a network or over the Internet. Examples of collaborative services include: chat, online meetings, and work group software. Metadata tags enhance data sharing and collaboration by allowing users and applications to comprehend the data, both structurally

and semantically, and readily determine how the data may be used for their specific needs.

13.4.1 Database accesses. Data integration is more than just being able to locate and access required data on other IT systems. Data integration also involves the ability to access databases directly and retrieve sets of data based on user(s) needs. These data sets can then be re-formatted or combined with other data sets (possibly from other IT systems) to create new representations of the data. For example, several leading edge companies have instituted "digital dashboards" as a mechanism to access data from several company databases, combine or simplify it, and create summary level company performance data for use by management. In other cases, product design data is utilized directly by manufacturers to create manufacturing instructions for computer aided machine tools and inspection equipment.

13.5 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.

14. LEGACY DATA

14.1 General. Legacy data is data that is inherited from programs, systems, software, platforms, techniques, and other sources that are earlier than those currently in use. Often legacy data takes the form of records in an existing database either on a system that is no longer in use or that is scheduled for obsolescence or replacement, or data that may no longer be useable or accessible. Legacy data may include not only data that has been generated by, developed for, or owned by the Government, but also similar data from non-Government entities, such as commercial proprietary data. For PMs and Data Managers, the existence of legacy data creates a challenge when planning for new systems, applications, tools, and databases in several areas, including: access, re-use, retention, cleansing, integration, sharing, transferring, conversion, or migration and processing of the legacy data. Legacy data is typically defined and delivered in its native format.

14.2 Planning for legacy data and systems. Any data or data system created has the potential for becoming or creating legacy data at some point in time. To the extent that one can anticipate this occurrence, planning may be beneficial by attempting to lessen the impact on future operations (whether tactical, administrative, or otherwise). The planning should include mission requirements, product life cycle, planned obsolescence, advance notice of obsolescence, economic downturn, and other contributors; such as loss of suppliers, etc.

14.2.1 Risks for legacy data and systems. The recent increase in outsourcing the development of software and data systems, including the use of foreign sources, increases the potential for operational or tactical vulnerability as well as general considerations concerning the retention and access of the legacy data. This is true whether the customer or end user is military or non-Governmental. Program risk management needs to address access, delivery, and rights to use software and data developed in a foreign country, based on planned use of the data.

14.2.2 Regulatory requirements for legacy data. The controlling DoD activity needs to consider whether there are regulatory requirements associated with legacy data or any Government or non-Government standards that cover legacy data, based on the planned use of the data.

14.3 Cost benefits analysis for data conversion. When a cost benefit analysis suggests that it is cost effective to convert data maintained as legacy information to another format, such as a standard digital format, program offices may need to modify existing contracts to achieve such data conversion.

15. DATA INFRASTRUCTURE

15.1 General. Data infrastructure describes the specific data resources needed to effectively support the defense system throughout its life cycle. Program, product, and item managers need a robust infrastructure to develop a seamless flow of defense systems data from development to disposal. A robust infrastructure requires melding development, acquisition, and sustainment data systems into a true total life cycle data environment. A robust infrastructure also facilitates the capability to reduce the logistics footprint and plan effectively for sustainment, while also ensuring that acquisition planners have accurate information about total life cycle costs. The

data infrastructure supporting the defense system life cycle should be able to interface or integrate specific requirements of the defense program with the Government supporting enterprise architecture and existing IT systems. All systems (contractor and Government) need to be accessible so that authorized users can get the information needed throughout the defense system life cycle.

15.1.1 Integrated DM system. An integrated DM system should support the following:

a. Technology insertion for affordability improvements during re-procurement and post-production support.

b. Configuration Management processes.

c. Serve as a ready reference for the systems engineering effort.

d. Data correlation and traceability (among performance requirements, designs, decisions, rationale, and other related program planning and reporting elements).

e. Total life cycle systems management efforts and provide the data required for performance based logistics implementation.

f. Long-term access of data to facilitate the following:

1) Competitive sourcing decisions.

2) Maintenance and sustainment analysis.

3) Conversion of product configuration technical data to performance specifications when required for enabling technology insertion to enhance product affordability and prevent product obsolescence.

4) Contract service risk assessment over the life of the system.

5). Qualifying additional sources or ICPs by internal only Government review of contractor restricted data such as Limited Rights or Restricted Rights data.

15.2 Government Concept of Operations (GCO) for IDDE. The Government IPT develops the GCO for IDDE with input from other supporting Government activities involved in the life cycle support of the defense system. The GCO should be consistent with and support the overarching AS. The GCO provides a foundation for defining the data requirements in the IT environment for the data user (e.g., contractors, the program office, maintenance, supporting organizations, and field operations).

15.2.1 GCO in DM strategy. Data Managers use the GCO in DM strategy for acquisition programs. Contracting officers should include the GCO in requests for proposal to provide information about the Government infrastructure, interface standards, data standards, and DM strategy for defense systems to potential offerors. Contractors may use this information to determine how they will best support Government requirements with their existing infrastructure or identify any changes they need to make.

15.2.2 GCO criteria. The GCO will address as a minimum the following criteria:

a. Hardware and software systems the Government has, or is developing, to manage and use data through interaction with service or agency enterprise efforts (i.e., AF Enterprise Systems, SALE, ERP efforts, or EBS/PDM).

b. Data users (including the number of concurrent users), types of data stored, data accessed, frequency of use, and timeliness of data access or delivery to each user.

c. Data use and the review, inspection, approval, and acceptance processes to support life cycle functions. Data acceptance requirements, including data format and content, and the Government processes for accepting data.

d. User locations and primary functions in support of the defense system.

e. Data interface standards and data standards.

f. Access authorization and restrictions.

g. Data approval methodology (e.g., electronic signatures and passwords).

h. Data distribution markings and physical distribution requirements.

16. DATA ACCESS VERSUS DELIVERY

16.1 General. Access may be formal access, contract scheduled delivery subject to the contract clauses, or informal access, via teaming agreements or other non-contractual arrangements. Informal access is a management

tool and may not be relied upon for obtaining program necessary data. All required data must be scheduled for delivery via an approved method such as hardcopy, electronic copy, or formal access. Formal access via a data repository controlled by a contractor raises numerous additional contractual and legal issues. See DFARS 252.227-7108. The terms of the contract must address these additional issues and assure that the contract procedures for assertions/markings/justifications regarding data rights claims by the contractor are applied to all deliverables regardless of the method chosen.

16.1.1 Online accessibility. Online access can take many forms. Typical examples include a contractor allowing a Government customer to access their internal application to view selected data (e.g., cost and schedule data). There is also the example of contractor access of Government systems. Where a secure Internet or intranet site has been established, this will allow a customer to access data that can be viewed online with a browser. This provides the customer with immediate access to the data. Typically, this is a view and print only mode; the data cannot be manipulated, downloaded, or saved into another application. Depending on contract requirements, there may be contractor unique applications to access the data; Internet based browser approaches provide a more universal and open system user interface.

16.1.2 Data delivery. This is data required for delivery to the Government as specified on a DD Form 1423 or specified with a clause contained in a contract. The Government receives or accesses data, inspects, validates, and accepts the data ordered under the contract. When data is accepted by the Government, the contractor makes delivery according to the instructions in the CDRL. The contract and/or the CDRL may instruct the contractor to deliver data directly to the contractor data repository in lieu of direct delivery to the Government. This data is inspected, validated, and accepted by the Government using the same process as any other data delivery. When specified in the contract, the contractor will organize, manage, and maintain the data and establish a process for Government access and use. This type of delivery should include provisions for transitioning the data directly to the Government, using electronic methods, such as, e-mail or File Transfer Protocol (FTP), special delivery, or conventional mail service when and if the need arises. The data may be delivered on a contractor or Government provided digital environment.

16.1.3 Electronic Data Interchange (EDI). EDI plays a role when the data will be extracted or downloaded for the purpose of transferring the data into one or more application systems. For users needing to use or manipulate the data, EDI supplies the means to collect and merge data for use in other applications regardless of the source. The EDI application, in neutral standard format, approach allows data to be extracted and read into a variety of application systems for further analysis and reporting.

16.1.4 Data transfer approaches. Online and EDI approaches could also be combined in a secure Internet/intranet site to allow the customer to view the data. In the event the customer wants to extract the data for further analysis, a download option should also be included on the website. A download function would use the EDI format to provide the data to the customer in a standard format. This approach also embraces the future of standards on the Internet including XML. A proposal under consideration with the W3C provides the guidelines to combine XML with EDI to provide a standard framework to describe data in a standard format; look for these Internet and EDI environments to continue to merge over time.

16.2 Transition steps to an IDDE. The goal of IDDE is to streamline processes, make information and data easier to use and access, eliminate paper, and make better use of data for timely management control and decision making. Some things to consider in the transition process to an IDDE include the following:

16.2.1 Security precautions. The security precautions taken to protect data exchanged or accessed in an electronic environment should be at least as strong as those employed for the exchange of paper, but should not be so stringent that the trading partners realize unnecessary cost or burden.

16.2.1.1 Formal EDI environments. In a formal EDI environment, the normal operating procedure level of data protection is usually sufficient. The EDI software and Value Added Network (VAN) connections usually require some type of password to control access to the data and transmission process. The VAN can track the movement of a message because of operation in a controlled environment. Studies have shown that business sensitive data is much more secure going through a formal EDI message exchange than when paper is exchanged. In the event a more secure environment is desired, the ASC X12 EDI Standards define outer envelopes that can be used to provide encryption.

16.2.1.2 Informal EDI environments. In an informal EDI environment, computer system firewalls, access control, and Commercial Off-the-Shelf (COTS) encryption and digital signatures can be used. Computer system firewalls and access controls can be employed to protect the system, application, and data from unauthorized signatures. Generally, the encryption and digital signature software or utilities should be the same at both ends, providing a more open approach.

16.2.2 Digital signature. Digital signature is typically tied to encryption methods when moving an electronic message over the Internet. The outer envelopes in a formal EDI environment can also include a PIN, a form of digital signature. Digital signatures provide authentication that an electronic message has been sent by an authorized person. This can provide a measure of control to replace hardcopy signatures typically used today to certify delivery of program management data. The goal is to replace the current paper processes with electronic equivalents.

16.2.3 Receipt notice. In a formal EDI environment, the 824 Application Advice Transaction Set is used to verify receipt of an EDI transaction. Federal guidelines on ASC X12 transactions are found at http://www.defenselink.mil/bta/FedeBiz/private/edit/document/guidelines/part10/Part_10_004030.pdf (see Appendix A). When a VAN is not available, then receipt may be verified through other means (e.g., e-mail notification).

16.2.4 Environment. In an informal environment, it may be necessary to establish some type of electronic based procedure to verify that an electronic data delivery has occurred. Keeping a backup copy of the receipt notice should also be considered. This information can be important in the event of a contract dispute.

16.2.5 Acceptance notice. Acceptance of the data is a separate process from receipt of the data. It may be necessary to establish an electronic acceptance notice advising the contractor that the program office has accepted the data or there are deficiencies in the submission(s) and the data needs to be resent. This can be as simple as an e-mail notice. If there are problems with the data, the notice includes an error report attachment that identifies specific data problems.

16.2.6 Data content. The content of data is outside the scope of the EDI standards. The EDI standards are only concerned with providing standard format to exchange the data. If there are certain data content rules that should be followed, then those requirements should be provided to all trading partners. Data content requirements can range from using specific reporting structure element codes to verifying data calculations. Various commercial off the shelf software analysis tools can also be used to verify the data content before submission using electronic delivery.

16.2.7 Paperless delivery. The preferred method is electronic. One objective of an IDDE is to reduce the delivery of data using a paper media. In the event both paper and electronic copies of data are being submitted, there needs to be an established plan to stop the contractual delivery using paper process.

16.2.8 Approach to data delivery. Use of an acceptable approach to data delivery is important to assure compatibility and availability of the data and ability to import and export this data regardless of the application. The approach to data deliveries should avoid using different delivery methods for various types of data and use compatible methods (e.g., e-mail, FTP exchange, web access, or formal EDI data exchange). The use of various (non-compatible) electronic delivery methods and the paper delivery method depending on the type of data makes it difficult and resource intensive for users to access the right data efficiently and effectively.

16.2.9 Use of open system, standard based methods. The use of open standards provides the ability to take continuous advantage of changes in the underlying technology. Open system, standard changes, and growth of rapid advances in technology allow all types of applications, components, and computing environment to work together. The use of closed environments (i.e., proprietary systems and solutions) limits contractor and government options and guides the user into a specified approach.

16.3 Decision methodology. Steps to be taken when deciding best method of delivery (e.g., hardcopy, electronic copy, or formal access at a contractor's data repository.

16.3.1 Management endorsement. This is a fundamental step required to ensure success. A top level commitment should be made to use standards based electronic systems instead of paper, proprietary formats, and contract unique requirements. PMs and other personnel need to maintain an understanding of Government policy, future direction, the bigger picture surrounding a digital program environment, and how an IDDE provides tangible

benefits. The results of cost and benefit analysis can also help to illustrate that an EDI can improve efficiency and reduce costs.

16.3.2 The contractor. The contractor is the next important step and should be a willing trading partner. The PM addresses any related contractual issues or consideration that the contractor proposes and counters with negotiation strong points. The PM presents a general idea or concept of the IDDE to sustain an integrated digital program office environment. The PM should furnish a functional and technical point of contact to answer any questions the contractor may have.

16.3.3 The EDI team. The members of the team are the key people that work with the PM to create the EDI implementation plan and make sure all the resources are available. Along with the PM, the team will set the goals, establish time frames, and document any operational criteria. The EDI team should include representatives from the program office (e.g., PM, Data Manager, engineer, etc.), from the contractor, from an audit organization (e.g., Defense Contract Management Agency [DCMA]), and a functional area having knowledge in the use of the application system that receives the data for the PM or military service. The functional area representative will address communication, programming, or other related issues.

16.3.4 The implementation plan. The implementation plan will determine what needs to be done, who is doing it, when it is going to be done, and what kind of resources are required. The plan should also include the type of measurement criteria to be utilized, such as milestones to demonstrate that progress is being made. This plan should also be provided to the contractor for comment, revision, and agreement to proceed as recommended.

16.3.5 The groundwork. The groundwork will include consideration for the following items before any data is exchanged:

a. Provide copy(s) of applicable Implementation Conventions (ICs) to everyone involved. The IC verifies the version and release of the standard and provides information about the structure and parameters of the data exchange.

b. Identify all data content requirements. Provide the contractor sufficient information so that the contractor is aware of any specific data content requirements. Content requirements are generally dictated by the receiving application or by specific program office data requirements that are outside the scope of the ICs.

c. Identify the application that will be used and any interface requirements. The data coming out of the application system should be mapped into an EDI ready format. Conversely, an EDI ready file should be mapped into a format that an application can read to import the data.

d. Resolve contractual, administrative, and security issues. For example: CDRLs may need to be modified; the contractor may wish to negotiate the cost of changing the deliverable methods. The PM should address these issues with the contractor through the contracting office.

e. Train personnel. Consider providing executive overview briefings or technical training for the end users so all parties understand how to use the IDDE.

f. Set up a getting started meeting. This is where you will work out the details in the implementation plan with the people involved in the EDI process.

g. Establish operating criteria. All parameters for exchanging the data should be set and agreed upon before the testing process begins. The criteria should establish the method of data exchange, whether formal or informal, and include a detailed definition of conditions for receipt and acceptance. This criteria should also include target time frames (e.g., minutes or hours) to move the data from one point to another, security, procedures for problem resolution, points of contact, and if applicable, a distribution list to identify all parties that need to receive the data. Backup and audit requirements should be included in the criteria.

h. Verify that the data to be furnished by the Government is authorized for such a release (security classification, distribution statement and data rights markings) and is required for contract performance.

16.3.6 The connections. This step includes determining the method of data transfer and setting up all the required connections among the various hardware systems and application software that physically move the data from one place to another.

16.3.6.1 Method of data exchange. The program office and contractor should first determine if a formal or informal method of data exchange will be used. The activities involved to establish the necessary connections will

vary depending on the method of transport.

16.3.6.1.1 Formal data exchange. In a formal EDI environment, a program office may elect to enlist the services of an established federal EDI server compatible with the program management transaction sets, such as the Defense Automatic Addressing System Center (DAASC) system, for help in setting up network connections and determining the method of data delivery to the program office and other interested parties. Net-centric Data Strategy and Guidance is another example of a formal EDI environment.

16.3.6.1.2 Informal data exchange. An informal EDI environment is typically much easier to implement as established Internet based connections provide the means to transport the data; however, data access controls, encryption, and digital signatures may need to be added to the connection process at both ends.

16.3.6.2 Contractor EDI files. The contractor should establish a process for extracting the data from the native application system(s) into an EDI ready file. EDI ready files should comply with the EDI standards syntax and with the applicable federal implementation conversion and follow any contract specific data content requirements and verification procedures.

16.3.6.3 Program office EDI files. The program office should have the capability to import an EDI ready file into an application system and perform the defined data content verification procedures to ensure contractor compliance and data acceptability.

16.3.7 Production mode. The successful planning and implementation efforts result in an EDI that can be a catalyst for changes and improve business processes and procedures. The EDI concept and implementation drives stringent data requirements analysis, proves data needs, and defines the processes important to manage a contract in the most cost effective and efficient manner.

16.4 Deferred ordering and delivery. Deferred ordering and delivery techniques should be used with complex or long-term defense system acquisitions, when exact data requirements are difficult to determine. This technique is also applicable for cases when delivery of specific data is difficult to prescribe. Deferred ordering is a technique for delaying the ordering of data generated in the performance of the contract until the Government determines what data is actually needed and when it is needed. This technique ensures the availability of the raw data while avoiding the cost of buying the data, if the need never arises. Deferred delivery of data is a technique for delaying delivery of the data and associated costs until the Government determines there is an actual need for delivery.

16.4.1 Contract methods. Each contract will specify the proper method for ordering/obtaining additional data. Absent a specifically state method, the Change Clause is usually available for additional data related to contract performance. The period of time during which such orders may be placed will also be stated in the contract. For deferred delivery, the period is two (2) years after acceptance of all items. For deferred ordering, the period is three (3) years after acceptance of items. For the Change Clause it is prior to contract close out.

16.4.2 Delivery of technical data. The delivery of additional data requirements will be in accordance with an existing and referenced DID (or other approved data requirement documentation) or pursuant to a new DID added at the time of ordering.

17. INSPECTION, ACCEPTANCE, OR REJECTION OF TECHNICAL DATA

17.1 General. The Government should have procedures in place for receiving delivery (chose method of delivery) , technical validation to include contractor markings, inspection, and acceptance/rejection of data delivered under DoD contract. Government inspection, acceptance, or rejection is required for TMs, TDPs, and other data that will be used by DoD personnel for the installation, operation, or maintenance of defense system items.

17.2 Competitive procurement. To directly support competitive actions, generally the Government requires Unlimited Rights or Government Purpose Rights in data. The Government may indirectly support the qualification of sources and ICPs by a limited internal only use of Restricted Rights and Limited Rights data. Establishing and confirming the Government's rights in data requires a critical review of deliverable data to assure that any restrictive contractor marking is consistent with the contractor's assertion, subject to challenge, and that it is limited to only that data on a page which is, in fact, subject to the asserted restriction. (See Section 9)

17.3 Acceptance phases. The phases of the acceptance process are contractor orientation, (i.e., guidance

conference), IPRs, audits, final reviews, technical approval, inspection, acceptance, or rejection. The systematic process of inspecting and accepting TMs, TDPs, and other data should begin as soon after contract award as practical. This process includes identification and enforcement of the CDRL requirements, contract FAR and DFARS clauses, inspection, acceptance, and rejection of the TMs, TDP, and other data by an authorized Government representative. This process should include the initiation of contractual enforcement actions for non-performance or lack of progress when appropriate.

17.4 Contractor responsibilities. The contractor is responsible for establishing and maintaining effective procedures for implementing and maintaining quality control consistent with the data requirements and the provisions of the contract. The contractor should provide and maintain a quality system that will ensure that all data submitted for acceptance is technically accurate and conforms to contract requirements. In addition to data generated or processed by the prime contractor, the contractor should levy on subcontractors or vendors appropriate quality requirements to assure the provisions of the contract are met. The contractor quality program requirements should also ensure compliance with procedures governing preparation, marking, and control of technical data to comply with the contract requirements.

17.5 Government responsibilities. Government personnel accept technical data only after ensuring that the data complies with the applicable contract clauses and the contract data exhibit comprised of completed DD Form 1423. DoD components have the responsibility of ensuring a prompt review and acceptance or rejection of submitted or accessed data, and that all deliverable data items or accessed data items meet contract requirements. When DoD components require inspection and acceptance of delivered or accessed data, it is necessary to prescribe a DD Form 250 or equivalent to accompany each contractor data submission. Guidelines for inspection and acceptance of deliverable or accessible data items can be found in the DFARS 227.7103, and other documents identified in the contract. The DoD has implemented the Wide Area Workflow (WAWF), where the contractor can submit any claims for payment electronically. (See Section 1008, National Defense Authorization Act of Fiscal Year 2001.)

17.5.1 Administration of contracts. The Government is responsible for administrating all defense system acquisition contracts. This function is typically accomplished in the DoD by DCMA. Contract administration includes the authority to perform all of the normal functions related to the acquisition of data that maybe assigned and performed by DCMA, as part of the CAO responsibility. Memorandum of Agreement may be written between the Government organization and DCMA outlining the responsibilities DCMA will administer for the contract. Part of the CAO function, as listed in FAR Subpart 42, should include:

a. Ensuring the contractor complies with contractual Quality Assurance (QA) and warranty requirements.

b. Maintaining surveillance of contractor engineering effort and management system, including data control systems.

c. Evaluating engineering efforts and management systems for adequacy.

d. Evaluating and monitoring contractor procedures for complying with contract requirements regarding restrictive markings on data.

e. Ensuring submissions of required reports.

f. Notifying the Procuring Contracting Officer(r) (PCO) of any discrepancies or inadequacies noted in the contractor's performance of the contract, including requirements for technical data.

17.5.2 Review, approval or rejection. Government personnel responsible for the inspection, acceptance, or rejection of technical data on all acquisition contracts should be aware of the following: acceptability of technical data delivered or accessed under a contract should be determined by application of SOW paragraphs, appropriate contract clauses, and the contract exhibit for technical data prescribed using DD Form 1423. A prompt review and approval or rejection of submitted data is provided to the contractor.

17.6 Data requiring inspection and acceptance. Inspection and acceptance criteria for contract data items are identified in Block 7 of the DD Form 1423. Government inspection and acceptance is required for TMs, TDPs, and other data that will be used by the DoD component for re-procurement, installation, operations, or maintenance of defense system items. The TMs, TDPs, and any data used by DoD component for re-procurement, installation, operation, or maintenance of defense system items should be part of the IPRs and audits to verify the contractor is meeting contract requirements and the data is meeting the acceptance criteria.

17.6.1 Procedures for inspecting and accepting data. The Data Manager should track the principle phases of this process, which includes contractor orientation (i.e., guidance conference), IPRs, audits, final reviews, technical approval, inspection, acceptance, or rejection. These phases should include initiation of contractual enforcement actions for non-performance or lack of progress. Procedures need to be in place to verify that the data is marked properly.

17.6.2 Guidance conference. The Data Manager and the controlling DoD activity, along with the contractor, should coordinate the guidance conference. Generally, the guidance conference is held within 60-90 days after contract award. The guidance conference is a joint Government-contractor review of contractual data requirements to ensure that the contractor understands the contractual obligations, to review the contractor's approach to satisfy those obligations, and the requirements to submit accurate, clear, complete, current, and adequate data for the intended purpose. The guidance conference may be held in conjunction with other contractor guidance and introduction conferences (e.g., post award conference, kick-off meeting, engineering data guidance conference, etc.).

17.6.3 Topics for guidance conference. This conference, as a minimum, should identify such topics:

a. The CDRL requirements, applicable DIDs, specifications, standards, and the applicable tailoring.

b. The conference should review and clarify contract requirements and different sections of the contract to provide both the Government and the contractor a better understanding of the data requirements, schedules (e.g., IPRs and audits), deliveries (e.g., preliminary and final), drafting practices, formats (e.g., Government or contractor based on the CDRLs), numbering system for drawings, part number process, and management of engineering documentation.

c. The contractor data rights marking procedures and policies.

d. The contractor's process for developing, releasing, and controlling data in digital form, including data updates, transfers, and the identification of data exchange protocols used by the contractor.

e. The contractor's QA procedures and the quality of the subcontractors and vendors, who will be delivering data.

f. The role of the subcontractors and vendors, who will be delivering the data.

18. PROTECTION AND RELEASE OF DATA

18.1 General. Data is withheld from public release, and its further distribution controlled, under a number of different authorities and processes. This withholding and controlling of Data may be mandatory under the law (e.g., the Arms Export Control Act) or discretionary. Only statutory mandates (and special contract language) control a contractor's use and release of contractor owned/generated Data. Technical data (to include software) within the Government's possession is required to be properly marked to indicate any such limitations or controls. As explained under the Freedom of Information Act authority, Data (in the form of an already existing agency record) may be withheld only pursuant to a statutory authority authorizing such. Classified data is subject to DoD 5200.1-R. The following applies to unclassified data.

18.2 Authorities and processes. The following is a summary of the mandatory and discretionary authorities and their implementing regulatory processes:

18.2.1 Arms Export Control Act (AECA) , 22 U.S.C. sections 2751, et. Seq. (Mandatory). Prohibits the export/release of certain restricted data. See E.O. 12470 and implementing regulations at 15 CFR Part 125 and (ITARS) 22 CFR part 120. This is a very complex area with overlapping authorities, assigned responsibilities, and regulatory coverage. If a specific point of contact has not been assigned to assist in such matters, contact your security office. For markings and dissemination, see DODD 5230.24 and DODD 5230.25.

18.2.2 10 U.S.C. Section 130 (formerly 140) (Discretionary). Authorizes the withholding (as a statutory FOIA exemption) of "any technical data [includes software] with military or space application…if such data may not be exported lawfully outside the United States without an approval, authorization, or license under the Export Administration Act of 1979 (50 U.S.C. App. 2401-2420) or the [AECA]." (Essentially a subset of the data covered by the AECA which is actively managed by DoD.) If a specific point of contact has not been assigned to assist in such matters, contact your security office. For markings and dissemination, see DODD 5230.24 and DODD 5230.25.

18.2.3 10 U.S.C. 2320, Rights in Technical Data (Mandatory). Certain contractor data, generally referred to as proprietary, may not be voluntarily released by the Government to third parties. A subset of that data referred to as Government Purpose Rights (or certain limited exceptions) may be released to third parties but not to the public. See DFARS Part 27 for implementation and markings. While the statute excludes computer software, the DFARS implementation gives it the same treatment by regulation. The contractor initially marks such data at delivery subject to review and verification by the PMO and Contracting Officer. Such data usually requires a Government determined Distribution Statement.

18.2.4 18 U.S.C. 1905, Disclosure of confidential information generally (Mandatory). When the Government possesses the trade secrets or other confidential information of another, Government personnel are prohibited from releasing that information except as authorized by another law. Improper releases of such data are a crime. The contractor applies its own markings for such trade secrets but not when that Data is delivered under a DFARS contract subject to the specified DFARS markings.

18.2.5 5 U.S.C. 552, Freedom Of Information Act (FOIA) (Discretionary). This statute requires the release of all existing agency "records" unless one or more of the stated exemptions applies. While the law and implementing procedures at DoDD 5400.7 apply only to formally designated FOIA requests from the public, it is generally accepted practice to apply these FOIA standards for release to all public requests for records. All FOIA requests must be coordinated with an assigned FOIA official and are subject to short suspense. The authority to partially or totally deny a FOIA request is restricted to certain agency officials. A contractor marking or a Government marking is not by itself a sufficient basis to withhold from release. When the contractor or the Government initially place a restrictive marking on data, they do so based upon a "good-faith" belief or assumption that one of the statutory bases for withholding can be met by the specific facts. When an actual FOIA request is received, those facts supporting the statutory basis for withholding must be verified and documented.

18.3 Contractor and potential contractor requests for access. Direct releases of technical data (Government information) are often made under the terms of a contract, by Public Affairs offices, or by other processes. Any such release must be consistent with the security markings, export control issues, Government Distribution Statement, and any contractor restrictive markings. Secondary releases (such as from data repositories and libraries) to third parties must assure that these same concerns/restrictions are applied. Two regulatory processes are available to Government contractors and potential contractors for access to Government data: DoD Form 2345 pursuant to DoDD 5230.25 and DD Form 1540 pursuant to Agency regulations (DLAR 4185.10, AR 70-21, AFR 80-39, MCO 5512.9, and NAVMATINST 3900.15). Unfortunately, these processes have not been updated and may allow releases inconsistent with the Government's obligations under a DFARS contract to protect contractor data. Any system or individual providing access to or release of restrictively marked contractor data must assure that the following conditions are met notwithstanding compliance with the existing regulatory processes: contractor data marked with a legend noting "Limited Rights," "Restricted Rights," or "Special License Rights" may NOT be released to third parties; and contractor data marked with a "Government Purpose Rights" legend may be released only after the requester has signed a DFARS authorized use and non-disclosure agreement (NDA) and a valid Government purpose for access/release is established.

19. MANAGEMENT AND SUSTAINMENT OF DATA

19.1 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).

19.2 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. (See Section 13 for further elaboration on the need for metadata and data indexes to enable access and integration.)

19.3 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.

19.3.1 Data format. When ordering data, the format of the data should be chosen to support current needs and long-term usability. The choice of neutral formats such as Standard for the Exchange of Product Model Data (STEP) for Computer Aided Design (CAD 3-dimensional files) or PDF for text or 2-dimensional drawings will ensure a longer useful life than a vendor proprietary format. Even vendor neutral formats may change over time. Existing data should be periodically reviewed and assessed to determine the need for the data to be converted to a more current format.

19.3.2 Data storage media. When 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.

19.3.3 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.

19.3.4 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.

19.4 Consideration of available data. Data requirements for a new procurement action should always be compared to available data at both Government and contractor data repositories to determine if the data already exists. If data does exist and the Government has rights that match those of the new requirement, then additional data should not be procured. If the required data exists but the Government does not have the necessary rights to use the data, negotiations should be attempted with the contractor or organization owning the data rights to determine the cost of acquiring sufficient rights to the data only for the specific intended purpose. The rights requested and the specific intended purpose should be reflected in the RFP as a contract clause. In many cases, this approach will provide a less expensive option than paying for redevelopment of the same data. Availability of a current, accurate data index is a key capability to be able to survey the existing data in a timely and cost efficient manner. The Data Manager should consider these possibilities when planning for new data acquisitions. These possibilities are normally identified in the AP and AS (See Section 13).

APPENDIX A

APPLICABLE WEBSITES

A.1 SCOPE

A.1.1 Scope. This appendix provides websites relevant to this manual.

A.2 LIST OF WEBSITES

A.2.1 List of websites. The following applicable websites are provided for further guidance.

(a) Acquisition Streamlining and Standardization Information System (ASSIST) website:
http://assist.daps.dla.mil or http://assist.daps.dla.mil/quicksearch/.

(b) Defense Automatic Addressing System Center (DAASC) website:
https://www.daas.dla.mil/daashome/daasc_home.asp

(c) Federal Guidelines on ASC X12 website:
http://www.defenselink.mil/bta/FedeBiz/private/edit/document/guidelines/part10/Part_10_004030.pdf

(d) Federal Implementation Guidelines for Electronic Data Interchange (EDI) website:
http://www.defenselink.mil/bta/FedeBiz/FEDGUIDELINE.shtml

(e) Military Engineering Data Asset Locator System (MEDALS) website:
https://www.dlis.dla.mil/medals/

(f) Net Centric Data Strategy website:
https://acc.dau.mil/simplify/ev.php?ID=43115_201&ID2=DO_TOPIC

(g) Wide Area Work Flow (WAWF) websites:
https://wawf.eb.mil/
http://www.bta.mil/index.html

PREPARATION GUIDE FOR CONTRACT DATA REQUIREMENTS LIST (DD FORM 1423)

B.1 SCOPE

B.1.1 Scope. This appendix provides information for preparing the Contract Data Requirements List.

B.2 PREPARATION GUIDE

B.2.1 Contract data requirements list. The following is a guide to filling out DD Form 1423.

CDRL Block	Description/Instructions
Definition	The standard form for identifying potential data requirements in a solicitation and deliverable data requirements in a contract. Subpart 215.470 of the DFARS requires the use of the CDRL (DD Form 1423) in solicitations when the contract will require delivery of data.
Purpose	The purpose of the CDRL is to provide a standardized method of clearly and unambiguously delineating the Government's minimum essential data needs. The CDRL groups all of the data requirements in a single place rather than have them scattered throughout the solicitation or contract and thus use of a CDRL reduces the burden on both the Government and the contractor.
Content	
A. Contract Line Item No. (CLIN)	Enter the CLIN associated with the CDRL. (Note: The Contract Schedule lists Data CLINs, which are related to other CLINs for hardware, software, or services. Each Data CLIN cites a contract exhibit consisting of a CDRL)
B. Exhibit	Enter the contract exhibit letter assigned to the CDRL. DFARS Subpart 204.7101 requires the DD Form 1423 to be a contract exhibit versus an attachment.
C. Category	This block provides a convenient means of identifying and grouping individual data items which relate to a separate contract exhibit. Enter one of the following, which applies to all the data items on the CDRL for a given contract exhibit: ☐ **TDP** for Technical Data Package Elements - MIL-DTL-31000 defines the types of data that comprise a TDP, makes reference to the applicable Government and Industry standards, and provides application worksheets: Specifications, Engineering Drawings and Associated Lists, Process Descriptions, Acceptance Test Procedures Other data that describes the performance characteristics, physical geometry, material composition, manufacture, and assembly. ☐ **TM** for Technical Manuals. Types of DoD manuals included under the TM category are defined as: Installation, Operation, Maintenance, Training, and Support. ☐ **Other** Types of data in the "Other" category may be further sub categorized into functional area assignments such as ADMN, SESS, MGMT etc. per the Standardization Directory (SD-1).
SD. System/Item	Enter the system, item, project designator, or name of services being acquired that the data will support.

E. Contract/PR No.	Enter the contract or Purchase Request (PR) number when known; if unknown, enter the RFP number or other appropriate designator.
F. Contractor	When known, enter the contractor's name, and Commercial and Government Entity (CAGE) code.
G. Prepared by	Enter the name and signature of the CDRL preparer, or the name of the activity responsible for preparation of the CDRL.
H. Date	Enter the date the CDRL was prepared.
I. Approved by	Enter the name (and signature) of the individual approving the CDRL.
J. Date	Enter the date the CDRL was approved. Note: The specific method of CDRL package approval is the responsibility of each DoD component. For paper CDRLs, it is sound management practice to paginate, sign, and date each approved page of the CDRL package to ensure that unauthorized pages have not been added or previously approved pages changed.
Blocks 1-16 are repeated for each individual data item listed on the CDRL	
1. Data Item Number	Enter the Exhibit Line Item Number (ELIN) per the DFARS Subpart 204.7105(c)**.** When the CDRL contains fewer than 1,000 data line items, numeric numbering of the last three positions of the exhibit line item number is allowed.
2. Title of Data Item	Enter the title of one data acquisition document. The title will be identical to the title of the DID when cited in Block 4. Note: When using Technical Manual Contract Requirements (TMCRs), or the CDRL to acquire TMs, enter the specific type of TM.
3. Subtitle	If the title in Block 2 requires further identification, enter a subtitle referencing the item to which the specific data item applies. e.g., Title: Conference Agenda; Subtitle: Program Reviews
4. Authority	(Data Acquisition Document Number) -- Enter the DID number of the approved DID that provides the format and content requirements for the data item listed in Block 2. Tailoring of the DID is identified in Block 16. Notes: (1) Except for a one-time DID, the DIDs cited in Block 4 are cleared for listing in the ASSIST by the DoD Clearance Office. (2) When using the CDRL to acquire TMs, enter the specific number of the applicable military specification or standard that provides the data preparation verification and validation instructions. (3) When using a TMCR, enter "See TMCR_" and attach the TMCR to the CDRL. (The TMCR lists the applicable military specifications or standards for TM preparation, verification, and validation.)
5. Contract Reference	Enter the specific paragraph number(s) of the SOW, or other applicable contractually referenced document that cites the tasking for generating the data requirement.
6. Requiring Office	Enter the technical office responsible for ensuring the adequacy of the data.
7. DD 250 REQ	Enter one of the following DD Form 250 codes to designate the requirement for inspection and acceptance of the data item:

	CODE	INSPECTION	ACCEPTANCE
	SS	At source	At source
	DD	None at source; final inspection at destination	At destination
	SD	At source	At destination
	DS	None at source; final inspection at destination	At source, based on written approval from the Contracting Officer
	LT	Letter of Transmittal only	As specified in Block 16
	NO	None required; DD Form 250 or letter of transmittal not required	None required; DD Form 250 or letter of transmittal not required
	XX	Requirements specified elsewhere in the contract	Requirements specified elsewhere in the contract

8. Approval Code	Enter "N/A" (not applicable) if the Government does not require approval of the data item. Enter "A" if written approval is required before distribution of the final data item. Indicate (in Block 16) the extent of approval required, e.g., technical content and/or format. If it is other than the Requiring Office listed in Block 6, enter the responsible reviewing activity in Block 16. When a draft is to be submitted for Government review prior to the final document, show (in Block 16) the allotment of time for Government review, and for contractor re-submittal after reviewing activity approval or disapproval. (Note: These times become contractual commitments. Both the Government and the contractor are obligated to provide notice of a revised length of time required, if they cannot meet the allotted times.)
9. Distribution Statement Required	Enter the code letter ("A," "B," "C," "D," "E," "F," or "X") to indicate the distribution statement that the contractor is to mark on the technical data item, in accordance with DoD Directive 5230.24. Note: If the acquisition activity does not know the appropriate statement to apply, or if it may vary among specific submissions of the data item, enter "See Block 16." Indicate in Block 16 that the Government requires a distribution statement and will provide it before delivery of the data.
10. Frequency	Specify frequency of submittals using one of the following typical codes. (If a code is used that is not on this list define it in Block 16 or on a CDRL Supplemental Section.)

	CODE	DEFINITION	CODE	DEFINITION	CODE	DEFINITION
	ANNLY	Annually	DAILY	Daily	QRTLY	Quarterly
	ASGEN	As generated*	DFDEL	Deferred delivery	R/ASR	Revision as required*
	ASREQ	As required*	MTHLY	Monthly	SEMIA	Every 6 months
	BI-MO	Every 2 months	ONE/P	One preliminary	WEKLY	Weekly
	BI-WE	Every 2 weeks	ONE/R	One time with revisions	XTIME	Number of times **

	*Explain these codes further in Block 16 as necessary. **A number is inserted in place of the "X."
11. As of Date	Enter the date for stopping data collection. For a single submittal of data, the date will be entered as follows: year/month/day (e.g., 1991Oct02). For recurring type data, a numeral will indicate the number of days prior to the end of the report period, established in Block 10, that data collection will be cut off (e.g., "15" would place the "as of" date for the data at 15 days before the end of the month, quarter, or year, depending on the frequency established in Block 10,etc.) In instances where an "as of" entry is appropriate, but cannot be numerically expressed because it is contingent upon a specific event, enter the notation "See BLK 16" and provide explanatory information in Block 16. If an "as of" date is not applicable enter "N/A" in this block. Note: Do not cite classified dates in the CDRL.
12. Date of First Submission	Enter the initial submission date one of the following ways: - Year/month/day (e.g., "1998Mar10"). Do not insert classified dates. - Specific event or milestone that constrains submittal (e.g., "30 DP-PDR"). - If the contract start date is not known, indicate the number of calendar days after contract (DAC) start that the data is due (e.g., "90 DAC"). Ensure that deliverables with a fixed date are compatible with program milestones; adjust the deliverable date if milestones change.

	Typical abbreviations in Block 12 are:

CODE	DEFINITION	CODE	DEFINITION
ASGEN	As generated*	DFDEL	Deferred delivery*
ASREQ	As required*	EOC	End of contract
XXDAC	Days after contract start**	EOM	End of month
CODE	**DEFINITION**	**CODE**	**DEFINITION**
EOQ	End of quarter	XDARP	Days after reporting period**
XDACM	Days after contract modification**	XDATC	Days after test completion**
XDADO	Days after delivery order**	XDPTT	Days before test**
XDARC	Days after receipt of comments**		

	*Provide specific instructions for these requirements in Block 16. **Insert a number in place of the "X."
13. Date of Subsequent Submission	If submittal of the data item is required more than once, enter the date(s) of subsequent submission(s). Do not insert classified dates. If a specific event or milestone constrains submittal, explain constraint in Block 16.
14. Distribution	Enter the addresses and the corresponding number of draft copies and final copies (regular and/or reproducible) to be provided to each. The first addressee is Normally the requiring office code shown in Block 6. The acceptance activity for the data item, if it is different from the requiring office and it will accept the data item by DD Form 250 at the destination. Do not insert classified locations. Block 14 will provide for the following particulars: (a) Block 14a. Addressee. The DoD component designator and office symbols and/or codes, or unit identification codes (UICs) may be used. Explain these symbols and codes in a supplemental section of the CDRL package, or in Block 16. Note: When a DD Form 250 is required by Block 7, the first addressee is the acceptance office for the data item. (b) Block 14b. Copies. Insert the specific number and type of copies (Draft, Final/Regular or Reproducible) to be delivered to each addressee. For online Access see Block 15. (c) When the data item requires written approval (indicated by an "A" in Block 8), enter draft quantities in Block 14b and an explanation in Block 16 (e.g., "Submit draft for approval 90 DAC award. Government will approve/disapprove within 30 days after receipt. Submit final copies 30 days after receipt of Government approval of the draft.") (d) Unless otherwise indicated on the DD Form 1423, all addressees listed in Block 14 will receive both draft and final documents. (e) Include (in Block 16 with a reference to Block 14) digital media details and constraints (when appropriate), such as source document requirements of tape density per inch, Tape size, Record and header formats, File headers, Files constructs, and Target system environment (such as DEC VAX -6000 series environment).

	(f) Include (in Block 16 with a reference to Block 14) non-digital media details and constraints, such as source document requirements (e.g., MIL-D-5840 or MIL-M-38761/1) type and class of microfilm, paper, vellum, etc., as necessary to fully describe media constraints. (g) If the contractor is not to actually deliver data to the Government or associated contractors, or if the Government requires deferred delivery, so indicate by entering "DFDEL" in this block. Provide disposition instructions in Block 16. ☐ The user, acquisition agent, and applicable Data Managers will coordinate procedures for distribution to classified locations.
15. Total	☐ Enter the total number of draft and final (regular and reproducible) copies required by Block 14. For digital media, enter the total number of copies required by Block 14. ☐ For online access, enter a reference to Block 16, and in Block 16 provide the access capabilities that are required for the data item.
16. Remarks	☐ Use this block to provide additional or clarifying information for Blocks 1 through 15. Examples include clarification relative to distribution statements, DID tailoring requirements, use of contractor format, and distribution of the data. When the data item requires online access or digital delivery, include relevant requirements in Block 16 (e.g., references to the appropriate standardization documents). ☐ Where data is to be provided by e-mail, or e-mail notification of data access availability is to be provided, include the e-mail addresses in Block 16 or in an attachment referenced in Block 16.
The bidder or offeror completes Blocks 17 and 18 to provide data pricing information for each data item, as specified in DFARS 215.873, Estimated data prices.	
17. Price Group	Enter the appropriate price group (as shown on the reverse side of the DD Form 1423). ☐ **Group I.** Data that is not otherwise essential to the contractor's performance of the primary contracted effort (production, development, testing, and administration) but which is required by the CDRL (DD Form 1423). ☐ **Group II.** Data that is essential to the performance of the primary contracted effort but the contractor is required to perform additional work to conform to Government requirements with regard to depth of content, format, frequency of submittal, preparation, control, or quality of the data item. ☐ **Group III.** Data that the contractor will develop for his internal use in performance of the primary contracted effort and does not require any substantial change to conform to Government requirements with regard to depth of content, format, frequency, of submittal, preparation, control or quality of the data item. ☐ **Group IV.** Data that is developed by the contractor as part of his normal operating procedures and his effort in supplying these data to the Government is minimal.

18. Estimated Total Price	Enter the total estimated price equal to that portion of the total price that the contractor estimates to be attributable to the design, development, production, or reproduction for the Government of items of data. ☐ **Group I.** Costs to be included are those applicable to preparing and assembling the data item in conformance with Government requirements, and the administration and other expenses related to reproducing and delivering such data items to the Government. ☐ **Group II.** Costs to be included are those incurred over and above what the essential data would cost without conforming to Government requirements, and the administration and other expenses related to reproducing and delivering such data items to the Government. ☐ **Group III.** Costs to be included are the administration and other expenses related to reproducing and delivering such data items to the Government. ☐ **Group IV.** Should normally be shown on the DD Form 1423 at no cost. **Where all, or a portion of the data price involves charges for online access, enter a reference to the location in the Proposal/Contract where the pricing for the access services are included.** Notes: (1) The entry "N/C" for "no charge" is acceptable. (2) DFARS Subpart 204.7105(a) (6) provides specific guidance for entering the negotiated price for separately priced or "Not Separately Priced (NSP)" data on the DD Form 1423 or in the contract. (3) Also provided is guidance on when to detach, or leave attached, DD Form 1423 Blocks 17 and 18.

CONTRACT DATA REQUIREMENTS LIST *(1 Data Item)*	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services and Communications Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY: TDP _____ TM _____ OTHER _____
D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE	17. PRICE GROUP
4. AUTHORITY *(Data Acquisition Document No.)*	5. CONTRACT REFERENCE	6. REQUIRING OFFICE	18. ESTIMATED TOTAL PRICE

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
8. APP CODE		11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION

16. REMARKS

14. DISTRIBUTION			
a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
15. TOTAL →	0	0	0

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE

DD FORM 1423-1, FEB 2001 PREVIOUS EDITION MAY BE USED. Page _____ of _____ Pages

Reset

CONTRACT DATA REQUIREMENTS LIST
(1 Data Item)

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY: TDP _____ TM _____ OTHER _____
D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR

16. REMARKS *(Continued)*

DD FORM 1423-1, FEB 2001 Reset Page_____ of_____Pages

Ref: NAVSEAINST 4160.3A NAVSEA S0005-AA-GYD-030/TMMP

NAVSEA/SPAWAR TECHNICAL MANUAL DEFICIENCY/EVALUATION REPORT (TMDER)

INSTRUCTIONS: Continue on 8 ½" x 11" page if additional space is needed.
1. Use this report to indicate deficiencies, problems and recommendations relating to publications.
2. For CLASSIFIED TMDERs see OPNAVINST 5510H for mailing requirements.
3. For TMDERs that affect more than one publication, submit a separate TMDER for each.
4. Submit TMDERs at web site https://nsdsa2.phdnswc.navy.mil or mail to: **COMMANDER, CODE 310 TMDER BLDG 1389, NAVSURFWARCENDIV NSDSA, 4363 MISSILE WAY, PORT HUENEME CA 93043-4307**

1. PUBLICATION NUMBER	2. VOL/PART	3. REV/DATE OR CHG/DATE	4. SYSTEM/EQUIPMENT ID

5. TITLE OF PUBLICATION	6. REPORT CONTROL NUMBER (6 digit UIC-YY-any four: xxxxxx-03-xxxx)

7. RECOMMEND CHANGES TO PUBLICATION

7a. Page #	7b. Para #	7c. RECOMMENDED CHANGES AND REASONS

8. ORIGINATOR'S NAME AND WORK CENTER	9. DATE	10. ORIGINATOR'S E-MAIL ADDRESS	11. TMMA of Manual (NSDSA will complete)

12. SHIP OR ACTIVITY Name and Address (Include UIC/CAGE/HULL)	13. Phone Numbers:
	Commercial (___) ___-_____ DSN ___-_____ FAX (___) ___-_____

FOLD HERE AND TAPE SECURELY
PLEASE DO NOT STAPLE

INCLUDE COMPLETE ADDRESS

USE PROPER POSTAGE

FOR OFFICE USE ONLY

COMMANDER
CODE 310 BLDG 1389
NAVSURFWARCENDIV NSDSA
4363 MISSILE WAY
PORT HUENEME, CA 93043-4307

FOLD HERE AND TAPE SECURELY
PLEASE DO NOT STAPLE