U.S. Department of
Homeland Security

United States
Coast Guard

Commandant
United States Coast Guard

US Coast Guard Stop 7714
2703 Martin Luther King JR Ave SE
Washington DC 20593-7714
Staff Symbol: CG-444
Phone: 202 475 5637
Fax: 202 475 5955

COMDTINST 4105.2
10 MARCH 2020

COMMANDANT INSTRUCTION 4105.2

Subj: U.S. COAST GUARD TECHNICAL DATA MANAGEMENT (TDM) POLICY

Ref: (a) The Coast Guard Integrated Logistics Support (ILS) Manual, COMDTINST M4105.14 (series)

(b) The Coast Guard Technical Data Management Handbook (series)

(c) Information and Life Cycle Management Manual, COMDTINST M5212.12 (series)

(d) International Specification for Technical Publications Using a Common Source Database, S1000D (series)

(e) Coast Guard Configuration Management Policy, COMDTINST 4130.6 (series)

(f) Deputy Commandant for Mission Support (DCMS) Engineering Technical Authority (ETA) Policy, COMDTINST 5402.4 (series)

(g) Management of Scientific and Technical Information (STINFO), COMDTINST M5260.6 (series)

(h) Coast Guard Configuration Manager's Handbook (series)

1. PURPOSE.

a. The Coast Guard works with a large volume of technical data that must be managed and controlled.

(1) Reference (a) requires TDM to be conducted in accordance with Technical Data Plan prepared as a part of the asset's Integrated Logistics Support Plan (ILSP). The Technical Data Plan describes how the program will obtain and manage technical data and data rights for the supported asset.

(2) Technical data not related to an asset (e.g., research and development technical data, technical data related to materiel in general use but not tied to a specific asset (such

DISTRIBUTION – SDL No. 170

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X		X		X	X				
B	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X		X	X	
C	X	X		X	X	X	X	X	X		X					X	X	X	X				X	X	X	X
D	X		X	X		X		X	X	X		X	X		X			X	X	X		X				X
E				X	X	X	X	X	X	X	X	X	X	X		X		X	X	X		X		X		
F															X	X	X		X							
G		X																								
H	X	X	X		X	X	X	X	X	X																

NON-STANDARD DISTRIBUTION:

as technical data related to paint, lubricants, etc.)) should be managed in accordance with requirements deemed applicable in this Policy.

b. This TDM Policy also establishes and promulgates The Coast Guard Technical Data Management Handbook (Reference (b)). It provides guidance for developing, implementing, and maintaining TDM plans and programs to support Coast Guard assets. It communicates TDM practices persons responsible for acquiring or developing Coast Guard technical data must evaluate for applicability when acquiring, controlling, distributing, maintaining, and disposing of Coast Guard technical data.

c. While the TDM Policy applies across the Coast Guard, its primary audience is Program Managers (PMs) [1], Technical Warrant Holders (TWHs), Technical Data Managers, other Integrated Logistics Support Management Team (ILSMT) members, Contract Officers, Configuration Managers, Engineers, and others responsible for acquiring or developing Coast Guard materiel as well as product line management teams (Product Line Managers (PLMs), Data Managers, Operator/Maintainers, Service Center/Logistics Center Commanders, etc.) responsible for sustaining technical data.

2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements must comply with the provisions of this Policy. Internet release is authorized.

3. DIRECTIVES AFFECTED. None.

4. DISCUSSION.

a. Technical data is recorded information (regardless of the form or method of recording) of a scientific or technical nature (including computer software documentation but not software itself) necessary to acquire, operate, and sustain an asset or other Coast Guard materiel. The types of technical data required are determined throughout the life cycle. Technical data deliverables may be acquired from contractors as Commercial and Non-Developmental Items (CANDI), developed by contractors, or developed by the Coast Guard. Technical data includes, but is not limited to the items below. Financial, management, tactical operations data (e.g., sensor readings and communications), personnel data, and other business and administrative data are not technical data.

(1) Technical Manuals (TMs)

(2) Engineering Drawings, Bills of Materials, Pre-requirement Drawings, Parts Lists, and Material Call Outs

(3) Engineering Models/Model Data

(4) Specifications that define function, performance, and interfaces

(5) Physical geometry, or other constraints

(6) Process descriptions

(7) Material composition

[1] Enclosure (1) lists and defines acronyms used in this Policy.

(8) Source or supplier data

(9) Safety requirements

(10) Preservation and packaging requirements

(11) Test requirements data and quality provisions

(12) Environmental stress screening requirements

(13) Interchangeability and Form, Fit, and Function (FFF) information

(14) Provisioning Technical Documentation (PTD)

(15) Engineering Data for Provisioning

(16) Installation procedures

(17) Maintenance Procedure Cards (MPCs)

(18) Engineering Change Proposals, Variances, Deviations, and Waivers

(19) Change Notices

(20) Software documentation

(21) Technical and supply bulletins

(22) Repair parts and tools lists

(23) Preventive maintenance instructions

(24) Component lists

(25) Product support data

(26) Hazardous material documentation

(27) Technical Reports

(28) Graphics, photographs, and logos

b. TDM is a discipline intended to:

(1) Provide the standard format, structure, and requirements necessary to produce technical data that accurately defines physical and functional characteristics.

(2) Minimize Total Ownership Cost (TOC). TDM minimizes TOC in two ways.

(a) TDM requires that acquisition and sustainment contracts address the technical data needed to support the asset from development to disposal. Technical data can be expensive to acquire and the ability to sustain the data must be considered when acquiring. Failure to adequately sustain the data can result in obsolescence and a waste of funds.

(b) TDM ensures the necessary data for cost-competitive acquisition of spares, contractor support, and asset upgrades during sustainment is acquired. TDM ensures that they acquire the needed data at the most economical time and make it available when it is needed.

(3) Meet Operational Availability requirements. Technical data is the basis of all operation and maintenance activities. TDM ensures that the right data is provided to the right personnel at the right time to enable asset operation and maintenance.

(a) To remain accurate, technical data must be maintained. Obsolescence can degrade technical data. TDM ensures that technical data is up to date and accurate, and that obsolete technical data is properly disposed of.

(b) Technical data requires protection. Technical data is subject to threats including but not limited to theft, espionage, and sabotage. TDM is needed to keep technical data safe.

(4) Manage Liability. TDM manages risk by ensuring compliance with international and national copyright laws and disclosure limitations, departmental regulations, and agency directives.

5. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide guidance for Coast Guard personnel and is not intended to nor does it impose legally binding requirements on any party outside the Coast Guard.

6. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

a. The development of this Instruction and the general policies contained within it have been thoroughly reviewed by the originating office in conjunction with the Office of Environmental Management, Commandant (CG-47). This Instruction is categorically excluded under current Department of Homeland Security (DHS) categorical exclusion DHS (CATEX) A3 from further environmental analysis in accordance with the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 and the Environmental Planning (EP) Implementing Procedures (IP).

b. This Instruction will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policy in this Instruction must be individually evaluated for compliance with the National Environmental Policy Act (NEPA) and Environmental Effects Abroad of Major Federal Actions, Executive Order 12114, Department of Homeland Security (DHS) NEPA policy, Coast Guard Environmental Planning policy, and compliance with all other applicable environmental mandates.DISTRIBUTION. No paper distribution will be made of this Instruction and its respective guidance. An electronic version will be located on the following Commandant (CG-612) web sites. Internet: https://www.dcms.uscg.mil/directives/ , and CGPortal: https://cg.portal.uscg.mil/library/directives/SitePages/Home.aspx.

8. RECORDS MANAGEMENT CONSIDERATIONS. This Instruction and its respective guidance have been thoroughly reviewed by the Coast Guard, and the undersigned have determined this action requires further scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., National Archives and Records Administration (NARA) requirements, and Reference (c). This policy has significant or substantial change to

existing records management requirements, or inconsistencies with existing determinations relating to documentation requirements.

9. POLICY.

a. General.

(1) This Policy must be applied in concert with Reference (b).

(2) Technical Data Requirements Analysis. Technical data requirements analysis must strive to optimize the versatility, flexibility, quality, accuracy, and ease of use of technical data. Technical data rights are typically most economically procured during acquisition. Technical data must fully support the planned development and support concept to include the entire life cycle of the asset, with consideration for issues including but not limited to Diminishing Manufacturing Sources and Material Shortages, changes in maintenance concept, and the possibility of service life extension program needs. Business case analysis must be performed to ensure that sufficient data rights are obtained to satisfy current and anticipated needs in accordance with Federal procurement law.

(3) Technical Data Acquisition Strategy. The approach for developing or acquiring technical data must be analyzed to determine the optimal strategy. The organization responsible for developing and delivering each technical data deliverable must be specified in the Technical Data Plan.

(4) Technical Data Acquisition Schedule. The technical data development/delivery schedule must be coordinated with the overall project schedule to ensure that technical data required for activities such as test and evaluation is available when needed. The technical data delivery schedule must be specified in the Technical Data Plan.

(5) Technical Data Plan. A technical data plan must be developed and managed by the Program Management Office (PMO) or ILSMT during acquisition. During sustainment, the PLM must manage the technical data plan. The technical data plan must specify:

(a) The technical data deliverables, data rights, and the supporting data management needs analyses performed;

(b) The data format standards and data schema that the data must meet (e.g., GEIA Standard-0007, Logistics Product Data, Extensible Markup Language (XML), International specification for technical publications using a common source database S1000D (Reference (d)), etc.);

(c) The process (acquire or develop) and responsibility for providing each technical data deliverable;

(d) The schedule for delivery of technical data deliverables.

(e) How the technical data will be validated, verified, updated, and approved;

(f) How the technical data will be managed, controlled and made available to data users. Issues that must be considered include:

1) Data markings (e.g., security markings, STINFO markings, copyright markings, etc.);

2) Data storage and distribution methodology (e.g., project database, Coast Guard Logistics Information Management System (CG-LIMS), Integrated Data Environment (IDE), etc.);

3) Data disposal considerations; and,

4) How technical data will be delivered to and maintained at its point of use (e.g., Interactive Electronic Technical Manuals (IETMs), hardcopy, databases such CG-LIMS, project or enterprise IDE, etc.).

b. Technical Data Rights.

(1) Technical Data Rights Strategy (TDRS). Technical data rights can be expensive. PMs and their teams must only acquire the rights expected to be needed during the asset's life. A TDRS business case analysis must be performed to optimize the data rights strategy. Considerations must include, but are not limited to:

(a) Identify the data that will be required to design, manufacture, and sustain the system and to support re-competition for production, sustainment, or upgrade if needed

(b) Identify the rights, access, and delivery of technical data needed throughout the asset life cycle

(c) Assess and mitigate the risk that the contractor may assert limitations on the government's use and release of data, including Independent Research and Development (IRAD)-funded data (e.g., consider whether the contract should require the contractor to declare IRAD up front and establish a review process for proprietary data).

(d) The TDRS should reflect the assessment and integration of the data rights requirements across all the functional disciplines required to develop, manufacture, and sustain the system over the life cycle. Restricted use and Intellectual Property (IP) rights should be understood before acquiring.

(2) Data Rights. Data rights describe the legal limits upon how the Coast Guard can use, modify, reproduce, release, perform, display, or disclose technical data. The Coast Guard acquires media containing technical data and a license to use, disclose, and release that data to specified parties. Unless the data owner assigns rights in data to the Coast Guard, the owner retains exclusive control over its use, release, and disclosure while licensees (the Coast Guard) are limited to using that technical data in accordance with the terms and conditions of the license. The Coast Guard must honor any restrictions on its ability to use, release and disclose a corporation's IP (including technical data) and must observe all restrictive markings affixed to that IP. Legal remedies for improper disclosure include monetary damages, injunctions, and criminal sanctions. . See 18 U.S.C. § 1905 (Disclosure of Confidential Information Generally). Technical data rights fall into seven categories:

(a) Unlimited Rights applies to data developed exclusively at Government expense and to certain types of data (e.g., FFF); operation, maintenance, installation, and training). These rights involve the right to use, modify, reproduce, display, release, or disclose technical data in whole or in part, in any manner, and for any purpose whatsoever, and to direct or authorize others to do so;

(b) Government Purpose License Rights include the right to use, duplicate, or disclose technical data for government purposes only, and to have or permit others to do so for government purposes only. Government purposes include competitive procurement, but do not include the right to permit others to use the data for commercial purposes;

(c) Limited Rights are granted via a limited rights agreement, which permits the government to use proprietary technical data in whole or in part. It also means that the government has the expressed permission of the party providing the technical data to release it, or disclose it, outside the government;

(d) Negotiated License Rights pertain whenever the standard license arrangements are modified to the mutual agreement of the data supplier and the government. In this case, the exact terms are spelled out in a specific license agreement unique to each application;

(e) Small Business Innovative Research (SBIR) Data Rights apply to all technical data or computer software generated under an SBIR contract. Non-government users cannot release or disclose outside the government except to government support contractors;

(f) Commercial Technical Data License Rights apply to technical data related to commercial items (developed at private expense). These are managed the same as Limited Rights;

(g) Commercial Computer Software Licenses. Applies to any commercial computer software documentation. These are managed as specified in the commercial license offered to the public.

c. Integrated Data Environment (IDE).

(1) General. Identify whether the program will implement an IDE and/or interface with a vendor or other government agency IDE. An IDE consists of infrastructure, functional applications, and business processes that enable asset digital product data to be produced, acquired, managed, secured, accessed, modified, and sustained by all privileged data users. Critical program data must be explicitly defined and protected accordingly.

(2) Data Storage, Distribution, Disaster Safeguarding and Recovery, Archiving, and Disposal. Technical data must be stored so that it is available when needed; distributed, or otherwise made available to those with access privileges and a need for the data. Technical data must be kept up to date and accurate. Technical data must be properly archived or disposed of when it is no longer actively needed. These activities must be considered and addressed in the Technical Data Plan. Topics to be assessed and documented must include, at minimum:

(a) Identify the process for distributing each technical data deliverable to the data user(s) while meeting security requirements. Program or project specific technical data storage and distribution management approaches must leverage existing DHS, Coast Guard (e.g., CG-LIMS or CGPortal), or other Government agency data management capabilities wherever practicable. Implementing program-level standalone approaches (e.g., program-level IDEs) beyond acquisition are discouraged as a long-term solution because they may duplicate data management infrastructure and hamper data management standardization efforts.

(b) Identify the safeguards to be put in place to prevent data loss, corruption, or unavailability and cite or include plans necessary to ensure the capability to provide continuity of operations and restore the IDE (including restoring hardware, operating and application software, data, networks, etc.) in the event of catastrophic failure.

(c) Identify any and all externally imposed data retention requirements (e.g., from Reference (c)).

(d) Assess the risk that technical data media and/or formats will exceed their shelf life or become obsolete within the life cycle of the asset. Technical data may need to be converted from one format to another.

(e) Identify any unusual technical data/media disposal methods required at the end of life cycle.

d. Technical Data Elements. A technical data element is a technical description of an item adequate for supporting an acquisition strategy, production, engineering, and logistics support. It consists of all applicable technical data such as drawings, associated lists, specifications, standards, performance requirements, QA provisions, and packaging details.

(1) Technical Data Content. Technical data must conform to Department of Defense Standard Practice, Technical Data Packages, MIL-STD-31000 (series).

(2) Engineering Drawings, Bills of Materials, Specifications, Pre-requirement Drawings, Parts Lists, and Material Call Outs must depict the design and manufacture of the asset. These elements must document the level of design maturity achieved. They must be used for development as well quality assurance functions, maintaining configuration, and procuring spare parts and systems. They are the major source of technical information for logistics support throughout the asset's life cycle.

(3) When determining what technical data to obtain with the asset, consider that life cycle sustainment may require changes be made to an asset, system, or part. If this occurs, drawings and associated data that contain all information needed for manufacturing are often needed. These drawings and associated data are usually less costly when obtained during the initial acquisition.

(4) Technical data element selection must take into account the impact of evolving technologies (e.g., Additive Manufacturing (AM)) when determining requirements for technical data elements to be acquired and managed.

(5) Technical data must be managed and placed under configuration control in association with its configuration item in accordance with Reference (e).

e. Technical Manuals (TMs). TMs are publications that contain instructions for installation, operation, maintenance, training, and support of an asset, its components and its support equipment. They may be presented in any form, including but not limited to hard copy, audio and visual displays, optical discs, and other electronic devices. Technical Orders (TOs) that meet the criteria of this definition may also be classified as TMs. Technical Manual Content Requirements (TMCRs) identify the specifications, standards, and content requirements for TMs. All new TMs developed expressly for the Coast Guard (including those developed by contractors) should be acquired and authored in digital form in XML in accordance with the World Wide Web Consortium (W3C) recommendation, “Extensible Markup Language (XML) 1.0 (Third Edition)”. Compliance with Reference (d) is strongly recommended.

(1) TM/Electronic Technical Manual (ETM)/IETM delivery to the Government must consist of the following:

(a) XML/Standard Generalized Markup Language (SGML) source file(s)

(b) Graphic source files

(c) Associated Document Type Definition (DTD) (whether new or existing)

(d) Entity files

(e) DTD Data Dictionary

(f) Tagging Conventions Document

(g) Any associated style sheets and filters

(2) A TMCR or equivalent document must be developed for acquisitions that include TMs. Literacy level, safety/hazard call-outs, delineated lifting levels, and maintenance envelopes, etc. must meet Human-System Interface (HSI) standards as defined by Commandant (CG-1) in accordance with Reference (f).

f. Technical Data Formats. Technical data deliverable formats must support the operational and maintenance requirements of the asset, and technical data deliveries must be compatible with existing Coast Guard information processing systems and repositories (e.g., CG-LIMS). Technical data format selection must take into account file formats required as a result of evolving technologies (e.g., AM) when determining format requirements.

g. Technical Data Protection and Markings. Technical data must be properly marked and protected from unauthorized disclosure.

(1) All deliverables (both hard copy and digital) must include distribution statements and procedures to protect critical technology information and assure that limited distribution data is properly handled at all times.

(2) Classified and Sensitive But Unclassified Information (SBU) Technical Data. Technical data programs must ensure that all unclassified, classified, and SBU technical data is managed (received, marked, safeguarded, accessed, disseminated,

reproduced, destroyed, etc.) in strict compliance with the Classified Information Management Program, COMDTINST M5510.23 (series).

(3) Personally Identifiable Information (PII)/Sensitive PII. PII and sensitive PII are not themselves technical data, but certain programs may encounter PII or sensitive PII within test or operational data (e.g., data handled by a Coast Guard nautical licensing system). PII and sensitive PII must be managed in accordance with the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (series).

(4) Scientific and Technical Information (STINFO). The Program Office must ensure that all technical data is reviewed for STINFO applicability and managed (received, marked, safeguarded, accessed, disseminated, reproduced, destroyed, etc.) in accordance with Reference (g).

(5) Destruction Notice. All classified or limited-access technical data be marked with a destruction notice. Consult Reference (g) for further information about destruction notices.

h. Quality Assurance and Data Integrity.

(1) Technical Data Validation, Verification, and Maintenance. Technical data must be verified (evaluated for accuracy, comprehensiveness, adequacy, and usability) and validated (evaluated for compliance with requirements and standards). Whenever feasible, physical demonstration of a maintenance and operating actions using the technical publications (MPCs and Coast Guard drawings when available), required tools, and other necessary support equipment must be used to validate and verify technical data.

(a) Technical data validation and verification considerations that must be considered and documented in the Technical Data Plan include:

1) Identify who will perform technical data acceptance inspection

2) Technical Data must be verified through a Physical Configuration Audit as part of the Configuration Management (CM) process. Identify support (e.g., field engineering, CM, etc.) required for validation and verification.

3) Technical data used for sustainment, modernization, etc., should be retrieved from and stored in an authoritative source.

4) Identify what support will be required to update the technical data.

(b) Technical data must remain accurate, complete, and consistent throughout the asset life cycle. The Technical Data Plan must describe how the technical data will be maintained.

(2) PMs must ensure that all Coast Guard technical data is reviewed for data rights assertions, validated, and verified before it is formally accepted. Technical data rights assertions regarding data deliveries must be reviewed by Government personnel for contractual compliance upon receipt, before technical data validation and verification reviews begin, to ensure that data rights assertions conform to

contract requirements, are valid, and to prevent possible data right violations by distribution to non-Government personnel.

i. Reviews and Audits.

(1) Requirements Review. Acquisition teams must formally review their technical data requirements (e.g., via a Data Requirements Review Board (DRRB)) prior to release of solicitations. Requirements for this documentation and review include but are not limited to:

(a) All requirements for the format, content, preparation, media, data rights provisions, and delivery of the data must be specified;

(b) The requirements must be limited to the data determined essential to asset support by a technical business analysis in a format supportable throughout the asset life cycle;

(c) Intended data users must agree with the acquisition needs and requirements;

(d) The requirements must conform to the applicable clauses of the FAR, Defense Federal Acquisition Regulation Supplement (DFARS), and Homeland Security Acquisition Regulation (HSAR);

(e) The requirements must be properly documented (e.g., on work statements and Contract Data Requirements List (CDRL) forms);

(f) Data warranty and quality assurance provisions must be specified to ensure that the data meets its intended use;

(g) Data deliverable approval authorities must be defined; and,

(h) Delivery dates must be consistent with the program schedule.

(2) In-Process Reviews (IPRs). IPRs are Government reviews of deliverable content conducted at defined points of the data development process to ensure satisfactory progress and that the technical data meets requirements.

(a) IPRs must be scheduled when enough data has been generated to allow meaningful inspection for contractor compliance with content, process, and schedule requirements and time to correct and re-inspect the data.

(b) All deliverable data associated with a given contract must be 100% complete and inspected before Government acceptance. Data must not be accepted with known errors or deficiencies.

(c) IPR findings and appropriate corrective measures must be documented in minutes.

(3) Functional Configuration Audit (FCA). The FCA uses the technical data, performance specifications, and related information to verify and certify that the actual performance of the asset meets the stated requirements. FCAs must be conducted in accordance with the References (e) and (h).

(4) Physical Configuration Audit (PCA). The PCA is a formal technical review of the asset as manufactured, tested, and delivered to its associated drawings/models and

released engineering data. The PCA establishes the configuration item(s) product baseline. PCAs must be conducted in accordance with References (e) and (h).

(5) Final Review. The Final Review must be conducted on the contractor's final deliverable under the contract. All data for an asset (such as a specific system) must be 100 percent complete and inspected before acceptance. Data must not be accepted with known errors or deficiencies.

(6) Logistics Assessments.

(a) Independent Logistics Assessment (ILA). An ILAs is a structured assessment and certification of the adequacy of logistics planning, management, resources, and execution to proceed with acquisition. ILAs reduce risk, ensure affordability, and provide adequate information for informed decision-making. Reference (a) sets forth policy, timing, and specific areas for review for ILAs.

(b) Logistics Readiness Review (LRR). An LRR is a structured assessment and certification of the implementation of logistics planning and management, availability of resources, and overall ability to support the asset as planned. LRRs ensure readiness. Reference (a) sets forth policy, timing, and specific areas for review for LRRs.

(c) Logistics Compliance Inspection (LCI). The LCI program documents compliance with ILS policies during sustainment. They ensure proper selection and use of technical standards, tools, and processes that deliver the safety, reliability, and performance required by the assets (cutters, aircraft, boats, facilities, and equipment) throughout their life cycle. The Logistics Compliance Inspection Program, COMDTINST 4730.1 (series), sets forth policy, timing, and specific areas for review of LCIs.

j. Conversion of Legacy Data. Legacy data is existing TMs, drawings, and associated lists that may be on paper, vellum, acetate, aperture cards or microfilm. Conversion is the process of capturing this data in digital form. The following requirements apply when considering converting legacy data.

(1) Legacy data must be reviewed to identify its importance to system life cycle support and conversion decisions based upon importance.

(2) Conversion cost, data storage requirements, data versatility, and data maintenance costs depend in part upon the target data format. When selecting legacy data conversion formats, data managers must perform a Business Case Analysis to strike the best balance between conversion cost, maintainability, anticipated data use, and data storage capabilities.

k. Model Based Design (MBD) and Model Based Enterprise (MBE).

(1) Engineering models/model data are two-dimensional (2D) or three-dimensional (3D) geometric representations of a design. Models may include different ranges and depths of data. They may:

(a) Describe the engineering concepts on which an approach is based (Conceptual Design Data)

(b) Provide a visual understanding of the item (Limited Design Disclosure Models), or,

(c) Fully define the product (Product Model Data).

(2) Formats for 2D and 3D engineering product data such as models, drawings, schematics, illustrations and geospatial data deliverables for installations and facilities include Computer-Aided Design (CAD), Computer-Aided Manufacturing (CAM), and Computer-Aided Engineering (CAE) product data for systems and platforms as well as architecture, engineering, and construction data for facilities. In all cases, the formats/tools selected by Original Equipment Manufacturers (OEMs)/designers for digital drawing and engineering data must be based on its intended use, how and where it is to be stored and accessed, the media by which the data is delivered, and must be compatible with the software tools that the Coast Guard has available on its workstations as listed on the Command, Control Communications, Computers, Cyber, and Intelligence and Information Technology (C5I&IT) Enterprise and Special Use Information Technology (ESUIT) program CGPortal site. The PMOs, Engineering Services Division (ESD), and PLM must consider and identify one 2D and 3D software solution for their organization. All stakeholders (including Aviation Logistics Center (ALC), Surface Forces Logistics Center (SFLC), C5I&IT, and Shore Infrastructure Logistics Center (SILC) must proactively establish one Coast Guard-wide preferred software solution for 2D and 3D engineering product data. PM, ESD, and PLM can consider other software based upon program life cycle and cost-effectiveness.

(3) An MBD is an annotated 3D model that contains all required product definition information organized such that it can be read and reused by all users, including non-CAD users. MBDs replace traditional engineering drawings. The MBD evolves throughout the engineering life cycle and communicates the current design to all users (e.g., training developers, maintenance procedure developers, logisticians, etc.).

(4) MBE is defined as a fully integrated and collaborative environment founded on 3D product definition detailed and shared across the enterprise, to enable rapid, seamless, and affordable deployment of products from concept to disposal. An MBE is an organization designed and operated to leverage the advantages of MBDs throughout the enterprise and from the beginning to the end of the life cycle. MBEs. Properly implemented MBEs offer benefits including but not limited to:

(a) Enabling automatic Bill of Materials creation;

(b) Improved communications between designers, analysts, and technicians;

(c) Increased form/fit/function evaluation;

(d) Direct paths to 3D printing and assembly simulation prototyping; and,

(e) Less reliance on drafting expertise among project personnel.

l. Additive Manufacturing (AM). AM, also referred to as 3D printing, is a layer-by-layer technique of producing 3D objects directly from a digital model. AM is increasingly used for maintenance and repair of damaged parts, particularly for products where a long lead time or expense is associated with procurement of new parts.

(1) PMs and PLMs must proactively determine and accommodate planned and likely future AM requirements in the asset life cycle. AM requirements may include but are not limited to:

(a) Unique data rights requirements

(b) Unique IDE requirements

(c) Unique materials requirements

(d) Specification of different technical data elements

(e) Specification of different technical data formats

(f) Unique technical data rights.

(2) Commanding officers and the cognizant ETA must ensure that use of AM does not increase safety risks to personnel or materiel. They must ensure that all AM requirements including but not limited to material requirements, safety requirements, post-manufacture finish requirements, test and evaluation requirements, etc., are identified and documented. Only commanding officers 05 and above have approval authority for AM to be used for a given item.

(3) Stakeholders (e.g., Service Centers and Logistics Centers such as ALC, SFLC, etc.) must develop additional specific guidance on AM use to provide amplifying guidance to PMs, PLMs, and their staff.

10. <u>RESPONSIBILITIES</u>.

a. Commandant (CG-444).

(1) CM Division, Commandant (CG-444) is the technical authority governing TDM policy and processes and is responsible for all changes.

(2) Commandant (CG-444) must provide guidance, clarification, and support to Coast Guard TDM process users.

(3) Technical Data Technical Warrant Holder (TWH). The technical data TWH is the technical expert for technical data and leads technical data-related technical efforts throughout the Coast Guard, independent of organizational boundaries. The technical data TWH must:

(a) Provide safe, reliable, effective, affordable, integrated, and timely technical data engineering expertise and technical guidance in support of the needs and requirements of Coast Guard systems.

(b) Establish or adopt and maintain technical data policy, standards, tools, requirements, processes, and certification requirements in accordance with higher authority policy. This includes any standards maintained by external organizations on behalf of the Coast Guard.

(c) Provide technical data engineering expertise and technical guidance (including response to urgent technical issues) to stakeholders (e.g., acquisition PMs, PLMs, ship design managers, engineers, research & development, field units, logistics centers, service centers, operational partners, configuration control boards).

(d) When established standards are not feasible, the technical data TWH must identify and approve a range of technically acceptable options and associated technical, programmatic, and safety risks.

(e) Inform both the organizational chain of command and the ETA hierarchy of significant technical data engineering and ETA issues, including technical disagreements that cannot be resolved by the technical data TWH or lower organizational levels.

(f) Where decisions deviate from established technical standards, processes, policy, or requirements, formally document, via memorandum, the technical data TWH's concurrence or non-concurrence decision.

(g) Designate responsible organizations, commands, or individuals in writing, where appropriate, as Certification Agents to evaluate technical data products against established standards to obtain certification.

(h) Unless otherwise specified by the Warrant Owner Deputy Warrant Owner, obtain all qualifications defined in Reference (f) and maintain these qualifications while assigned as TWH.

(i) Provide leadership and be accountable for all technical data engineering and technical decision making within their purview.

(j) Interface with other TWHs to ensure consistency in selection, interpretation, and implementation of technical requirements and policies.

(k) Designate technically competent personnel to act as their representative on an Integrated Product Team (IPT), other working groups, or to provide technical data services as appropriate. Services may include but are not limited to: analysis, development of requirements, development of design alternatives, investigation, risk assessment and mitigation, and in-service support to PMs and sponsors.

(l) Establish and maintain a network of lead engineers and other engineering support to represent or otherwise support the technical data TWH as necessary.

(m) Assist Commandant (CG-444) in maintaining the technical competency, expertise, and infrastructure in the technical data arena. Create and maintain partnerships with external organizations that will increase the depth of knowledge within the technical authority structure.

(n) Identify resources needed to properly execute, steward, and sustain technical data to include identification of critical risks and prioritized options.

(o) Capture and implement technical data lessons learned and best practices.

b. Contracting Officers. Contracting Officers under Commandant (CG-9) are responsible for providing specific guidance regarding contracting law and data rights. In consultation with legal counsel, they are responsible for framing the contract documentation necessary to acquire the data and data rights needed to satisfy technical data functional requirements and ensuring that contract requirements are met.

c. Program Managers (PMs). The PM is the individual or office with overall responsibility for developing and/or acquiring assets that fulfill operational requirements within cost and schedule constraints and developing the technical data plan. PMs must comply with the requirements in this Policy and the guidance in Reference (b).

d. Product Line Managers (PLMs). PLMs are the individuals or offices responsible for sustainment of deployed assets. They are responsible for managing the data associated with their assets and ensuring that the technical data plan and technical data itself is managed in accordance with the requirements in this Policy and Reference (b).

e. Technical Data Manager. Technical data managers are individuals assigned responsibility for implementing a consistent process framework to identify, protect, and make available the technical data for an organization or project in accordance with this Policy and commensurate with the organization's or project's scope.

f. Technical Data Users. Technical data users include all Coast Guard military and civilian personnel and authorized contractors with proper clearance, bona fide need to know, and lawful justification to view or use Coast Guard technical data. Technical data users are responsible for complying with all technical data distribution markings.

11. TRAINING. TDM is a dynamic field: data types, data storage methods, data management tools and technologies, and even the kinds of data available are evolving. TDM practitioners (e.g., Technical Data Managers, PMs, etc.) must monitor developments in their field and be prepared to implement new tools and strategies to ensure that they continue to achieve the most efficient and cost effective data management program.

12. FORMS/REPORTS. None.

13. REQUEST FOR CHANGES. Recommendations for changes and improvements to this Instruction and its respective guidance must be submitted via chain of command to Technical Data Manager, Mr. Aditya Patel (Aditya.A.Patel@uscg.mil), CM Division, Commandant (CG-444).

N.A. Moore
Admiral, U.S. Coast Guard
Assistant Commandant for
Engineering and Logistics

Encl: (1) List of Acronyms and Abbreviations

This page intentionally left blank.

LIST OF ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
2D	Two-dimensional
3D	Three-dimensional
ALC	Aviation Logistics Center
AM	Additive Manufacturing
C5&IT	Command, Control, Communications, Computers, Cyber, and Information Technology
CAD	Computer-Aided Design
CAE	Computer-Aided Engineering
CAM	Computer-Aided Manufacturing
CANDI	Commercial And Non-Developmental Items
CDRL	Contract Data Requirements List
CE	Categorically Excluded
CG-LIMS	Coast Guard Logistics Management Information System
CM	Configuration Management
DCMS	Deputy Commandant for Mission Support
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DRRB	Data Requirements Review Board
DTD	Document Type Definition
ESD	Engineering Services Division
ESUIT	Enterprise and Special Use Information Technology
ETA	Engineering Technical Authority
ETM	Electronic Technical Manual
FAR	Federal Acquisition Regulation
FCA	Functional Configuration Audit
FFF	Form, Fit, and Function
HSAR	Homeland Security Acquisition Regulation
HSI	Human-System Interface
IDE	Integrated Data Environment
IETM	Interactive Electronic Technical Manual
ILA	Independent Logistics Assessment
ILS	Integrated Logistics Support
ILSMT	Integrated Logistics Support Management Team
ILSP	Integrated Logistics Support Plan
IP	Intellectual Property
IPR	In-Process Review
IPT	Integrated Product Team
IRAD	Independent Research And Development
LCI	Logistics Compliance Inspection
LRR	Logistics Readiness Review

Acronym/Abbreviation	**Definition**
MBD	Model Based Design
MBE	Model Based Enterprise
MPC	Maintenance Procedure Card
NARA	National Archives and Records Administration
NEPA	National Environmental Protection Act
OEM	Original Equipment Manufacturer
PCA	Physical Configuration Audit
PII	Personally Identifiable Information
PLM	Product Line Manager
PM	Program Manager
PMO	Program Management Office
PTD	Provisioning Technical Documentation
SBIR	Small Business Innovative Research
SBU	Sensitive But Unclassified
SFLC	Surface Forces Logistics Center
SGML	Standard Generalized Markup Language
STINFO	Scientific and Technical Information
TDM	Technical Data Management
TDRS	Technical Data Rights Strategy
TM	Technical Manual
TMCR	Technical Manual Content Requirement
TO	Technical Order
TOC	Total Ownership Cost
TWH	Technical Warrant Holder
W3C	World Wide Web Consortium
XML	Extensible Markup Language