NOT MEASURMENT SENSITIVE

MIL-HDBK-61B
7 April 2020

SUPERSEDING
MIL-HDBK-61A(SE)
7 February 2001

DEPARTMENT OF DEFENSE HANDBOOK

CONFIGURATION MANAGEMENT GUIDANCE

This handbook is for guidance only.
Do not cite this document as a requirement.

AMSC N/A AREA SESS

FOREWORD

1. This handbook is approved for use by all Departments and Agencies of the Department of Defense.

2. Configuration Management (CM) is a technical discipline that ensures requirements, development, and operational information remains consistent throughout the program life cycle. This handbook provides guidance to personnel assigned the responsibility of executing hardware and software configuration management processes in the design, procurement, installation, operation, maintenance, and modification of acquired products. As such, it outlines and discusses the principles of CM: configuration management planning, configuration identification, configuration change control, configuration audits, and configuration status accounting. In addition, this handbook addresses application of these principles in areas such as data management, hardware versus software configuration items, and digital versus non-digital artifacts.

3. Major changes to this document include the removal of duplicative information now contained in GEIA-HB-649A, except where clarity is required.

4. Public Law 104-113, "National Technology Transfer and Advancement Act", stipulates that Federal Agencies shall use technical standards developed or adopted by voluntary consensus standards bodies unless impractical or inconsistent with law. In accordance with P.L. 104-113, Department of Defense (DoD) standardization for Configuration Management has evolved from the use of military standards to include the use of industry standards many of which are referenced herein. While the use of industry standards on DoD acquisition contracts is not mandatory unless stipulated by statute or policy, program managers should consider whether the use of standards on their program is beneficial in establishing and maintaining an efficient and effective CM process. In order to mitigate program cost, schedule, and technical risk, this revision to MIL-HDBK-61 is being issued to provide up-to-date guidance on applying CM requirements on DoD acquisition contracts. Appendix C provides recommendations for selection and tailoring of CM elements to be applied by program type.

5. Comments, suggestions, or questions on this document should be addressed to Commander, Naval Sea Systems Command, ATTN: SEA 05S, 1333 Isaac Hull Avenue, SE, Stop 5160, Washington Navy Yard DC 20376-5160 or emailed to CommandStandards@navy.mil, with the subject line "Document Comment". Since contact information can change, you may want to verify the currency of this address information using the ASSIST Online database at https://assist.dla.mil.

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

LIST OF FIGURES

CONTENTS

LIST OF TABLES

1. SCOPE

1.1 Scope. This military handbook provides guidance and best practices on how Program Managers (PM), systems engineers, logistics managers, and other individuals assigned responsibility for Configuration Management (CM) perform and contract for CM. Its purpose is to provide for guidance in planning and implementing effective Department of Defense (DoD) CM activities and practices during the life cycle of the defense systems. This handbook is intended to cover the DoD specific management activities related to acquisition and sustainment throughout the system's lifecycle. This handbook is for guidance only and cannot be cited as a requirement.

1.1.1 Background. DoD has adopted EIA-649, Configuration Management Standard, and its suite of documents. In a collaborated effort, the DoD and industry have worked to update, consolidate, and reduce unnecessary duplication as pertaining to DoD and Industry CM standards and handbooks. This handbook refers the reader to the suite of EIA-649 standards and handbook for more in-depth descriptions of CM application. The full CM portfolio of standards is shown in figure 1. This handbook also provides tailoring recommendations when putting EIA-649-1 requirements on contract. DoD Configuration Managers, in order to interpret MIL-HDBK-61 to the fullest extent and utilize examples of how to implement each function of CM, will need to incorporate the following in their CM toolkit:

a. SAE-EIA-649

b. SAE-EIA-649-1

c. GEIA-HB-649

Appendix A provides a listing of CM references by policy, standards, and guidance.

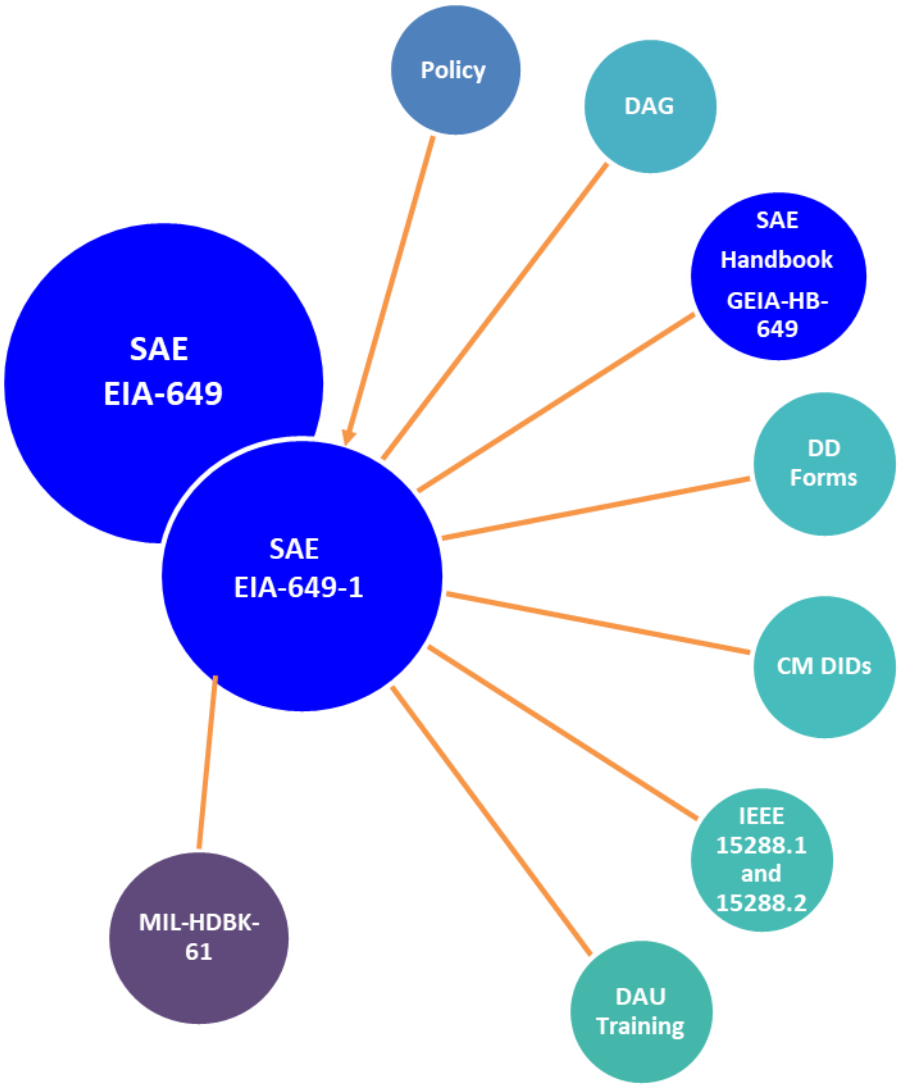

FIGURE 1. Configuration management standards.

1.1.2 CM functions. The CM process is comprised of five CM functions and the underlying CM principles that together provide a flexible implementation structure. The CM process provides consistency among the various elements of product configuration information. The five CM functions are:

a. Configuration Management and Planning
b. Configuration Identification
c. Configuration Control/Change Management
d. Configuration Status Accounting
e. Configuration Verification and Audit

The underlying CM principles are explained in detail to illustrate how they might be implemented for a configuration item (CI) (e.g., hardware, software, firmware, and associated documentation). Specific implementation examples are provided for most CM principles. The CM practitioner should determine the appropriate level of implementation.

1.1.3 CM Benefits, risks, and cost impact. CM provides knowledge of the correct current configuration of defense assets and the relationship of those assets to associated documents. The CM process efficiently manages necessary changes, ensuring that all impacts to operation and support are addressed. CM provides the following benefits:

a. Product attributes are defined. Measurable performance parameters are provided. Both buyer and seller have a common basis for acquisition and use of the product.

b. Product configuration is documented and a known basis for making changes is established. Decisions are based on correct, current information. Production repeatability is enhanced.

c. Products are labeled and correlated with their associated requirements, design, and product information. The applicable data (such as for procurement, design, or servicing the product) is accessible, avoiding guesswork and trial and error.

d. Proposed changes are identified and evaluated for impact prior to making change decisions. Downstream surprises are avoided. Cost and schedule savings are realized.

e. Change activity is managed using a defined process. Costly errors of ad hoc, erratic change management are avoided.

f. Configuration information, captured during the product definition, change management, product build, distribution, operation, and disposal processes (the equivalent of the DoD acquisition life cycle) is organized for retrieval of key information and relationships, as needed. Timely, accurate information avoids costly delays and product down time, ensures proper replacement and repair, and decreases maintenance costs.

g. Actual product configuration is verified against the required attributes. Incorporation of changes to the product is verified and recorded throughout the product life. A high level of confidence in the product information is established.

These benefits are equally applicable to Government and industry. Additionally, the effective application of CM principles to defense products contributes to and enhances the partnering environment desired between the DoD and its suppliers. In the absence of CM, or where it is ineffectual, there may be equipment failures due to incorrect part installation or replacement; schedule delays and increased cost due to unanticipated changes; operational delays due to mismatches with support assets; maintenance problems, down-time, and increased maintenance cost due to inconsistencies between equipment and its maintenance instructions; and numerous other circumstances which decrease operational effectiveness and add cost.

The severest consequence is catastrophic loss of expensive equipment and human life. However, these failures may be attributed to causes other than poor CM. The intent of CM is to avoid cost and minimize risk. Those who consider the small investment in the CM process a cost-driver may not be considering the compensating benefits of CM and may be ignoring or underestimating the cost, schedule, and technical risk of an inadequate or delayed CM process. Throughout this handbook, selection criteria are provided to aid in making choices concerning implementation of various CM activities and functions. In each applicable instance, the means to complete a benefit/risk analysis is provided.

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 handbook.

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 STANDARDS

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

MIL-STD-31000 - Technical Data Packages

(Copies of these documents are available online at https://quicksearch.dla.mil/.)

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.

DATA ITEM DESCRIPTIONS

DI-MGMT-82099 - Open Systems Management Plan

(Copies of this document are available online at https://quicksearch.dla.mil/.)

DEPARTMENT OF DEFENSE ISSUANCES

DoD Instruction 5000.02 - Operation of the Defense Acquisition System

DoD 5010.12-M - Procedures for the Acquisition and Management of Technical Data

(Copies of these documents are available online at www.esd.whs.mil/DD/.)

FEDERAL ACQUISITION REGULATION (FAR)

FAR Part 7 - Acquisition Planning

FAR Part 46 - Quality Assurance

(Copies of the Federal Acquisition Regulation (FAR) are available online at https://www.acquisition.gov/far.)

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

SAE INTERNATIONAL

SAE EIA-649 - Configuration Management Standard

SAE EIA-649-1 - Configuration Management Requirements for Defense Contracts

GEIA-HB-649 - Configuration Management Standard Implementation Guide

GEIA-859 - Data Management

(Copies of these documents are available online at www.sae.org.)

IEEE

IEEE 828 - Configuration Management in Systems and Software Engineering

(Copies of this document are available online at www.ieee.org.)

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

ISO 9000	-	Quality Management Systems - Fundamentals and Vocabulary
ISO 10007	-	Quality Management – Guidelines for Configuration Management
ISO/IEC/IEEE 12207	-	Systems and Software Engineering – Software Life Cycle Processes

(Copies of these documents are available online at www.iso.org.)

2.4 Order of precedence. In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 Definitions and terminology. Since a major goal of acquisition streamlining is to use commercial and industry practices to the greatest extent possible, there is no single correct set of CM terminology that must be rigidly adhered to. SAE EIA-649 illustrates many aliases that are commonly used in different industrial environments. It is appropriate to allow the use of terms common (local) to a given industry when dealing with that industry. The acronyms and definitions in this section are provided for reference:

3.2 Acronyms.

ACRONYM	**TERM**
AA	Application Activity
ABL	Allocated Baseline
ACD	Allocated Configuration Documentation
ACO	Administrative Contracting Officer
AECMA	Association Européenne des Constructeurs de Matériel Aérospatial (European Association of Aerospace Industries)
AIS	Automated Information System
AMSDL	Acquisition Management Systems and Data Requirements Control List
APB	Acquisition Program Baseline
CAGE	Commercial and Government Entity
CASE	Computer-Aided Software Engineering
CCB	Configuration Control Board
CDCA	Current Document Change Authority
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CI	Configuration Item
CM	Configuration Management
COTS	Commercial-Off-the-Shelf
CSA	Configuration Status Accounting
CSCI	Computer Software Configuration Item
DCMA	[U.S.] Defense Contract Management Agency
DFARS	[U.S.] Defense Department Supplement to the Federal Acquisition Regulation
DID	Data Item Description

ACRONYM	TERM
DM	Data Management
DoD	[U.S.] Department of Defense
ECP	Engineering Change Proposal
EIA	Electronic Industries Association
EMD	Engineering and Manufacturing Development
FBL	Functional Baseline
FCA	Functional Configuration Audit
FCD	Functional Configuration Documentation
FRP	Full-Rate Production
HWCI	Hardware Configuration Item
ICD	Interface Control Documentation
ICWG	Interface Control Working Group
IEEE	Institute of Electrical and Electronics Engineering
IPT	Integrated Product Team
ISO	International Standardization Organization
LRIP	Low-Rate Initial Production
MIL-STD	Military Standard
MOSA	Modular Open Systems Approach
MSA	Material Solution Analysis
NATO	North Atlantic Treaty Organization
NDI	Non-Developmental Items
NIST	[U.S.] National Institute of Standards and Technology
NOR	Notice of Revision
OEM	Original Equipment Manufacturer
PBL	Product Baseline
PCA	Physical Configuration Audit
PCD	Product Configuration Documentation
PDM	Product Data Management [System]
PIN	Part or Identifying Number
RFV	Request for Variance
SAE	Society of Automotive Engineers
SOW	Statement of Work
STANAG	Standard NATO Agreement
TDP	Technical Data Package
TMRR	Technology Maturation and Risk Reduction

3.3 Definitions. Definitions for CM terms used in this standard are consistent with Government terminology found in the Defense Acquisition Guidebook (DAG), Defense Acquisition University (DAU), and SAE EIA-649-1.

TERM	DEFINITION
Allocated Baseline (ABL)	Documentation that designates the CIs making up a system and then allocates the system function and performance requirements across the CIs. It includes all functional and interface characteristics that are allocated from those of a higher-level CI or from the system itself, derived requirements, interface requirements with other CIs, design restraints, and the verification required to demonstrate the achievement of specified functional and interface characteristics. The performance of each CI in the ABL is described in its item performance specification.
Allocated Configuration Documentation (ACD)	The documentation describing a CI's functional, performance, and interoperability requirements that are allocated from those of a system or higher-level CIs; interface requirements with interfacing CIs; and the verifications required to confirm the achievement of those specified requirements.
Application Activity (AA)	An activity that has selected an item or a document for use on programs under its control. However, it is not the current document change authority for the document(s).
Approved Document (or Data)	A document that has been approved by an appropriate authority and is the official (identified) version of the document until replaced by another approved version.
Assembly	A number of basic parts or subassemblies, or any combination thereof, joined together to perform a specific function. Typical examples include electric generators, audio-frequency amplifiers, and power supplies.
Change, Major (Class I)	An engineering change proposal (ECP) proposing a change to approved configuration documentation for which the Government is the current document change authority (CDCA) or that has been included in the contractor SOW by the tasking activity and:
	a. Affects any physical or functional requirement in approved functional or allocated configuration documentation.
	b. Affects any approved functional, allocated, or product configuration documentation and cost, warranties or contract milestones, or affects approved product configuration documentation.
Change, Minor (Class II)	An ECP proposing a change to approved configuration documentation for which the Government is the CDCA or that has been included in the contractor SOW by the tasking activity and which is not a Class I.
Component	A part, subassembly, or assembly that comprises a composite part of a higher-level CI. Components are identified in the product hierarchy, assigned nomenclature and identifiers, and defined via drawings, detailed specifications, performance specifications, commercial item definitions, or other means.
Computer Software Configuration Item (CSCI)	A CI that is computer software.
Computer Software Documentation	Technical data or information, including computer listings, regardless of media, that document the requirements, design, or details of software, explain the capabilities and limitations of the software, or provide operating instructions for using or supporting software.

TERM	DEFINITION
Configuration	A collection of an item's descriptive and governing characteristics that can be expressed in functional terms (i.e., what performance the item is expected to achieve) and in physical terms (i.e., what the item should look like and consist of when it is built). Configuration represents the requirements, architecture, design, and implementation that define a particular version of a system or system component.
Configuration Baseline (Baseline)	a. An agreed-to description of the attributes of a product, at a point in time, which serves as a basis for defining change.
	b. An approved and released document, or a set of documents, each of a specific revision; the purpose of which is to provide a defined basis for managing change.
	c. The currently approved and released configuration documentation.
	d. A released set of files comprising a software version and associated configuration documentation.
	See also: Allocated Baseline (ABL), Functional Baseline (FBL), and Product Baseline (PBL).
Configuration Control	a. A systematic process that ensures that changes to released configuration documentation are properly identified, documented, evaluated for impact, approved by an appropriate level of authority, incorporated, and verified.
	b. The CM activity concerning the systematic proposal, justification, evaluation, coordination, and disposition of proposed changes and the implementation of all approved and released changes into:
	(1) The applicable configurations of a product.
	(2) Associated product information.
	(3) Supporting and interfacing products and their associated product information.
Configuration Control Board (CCB)	An official forum composed of technical, logistics, acquisition, management, and administrative personnel who recommend approval or disapproval of proposed changes to, and variances from, an item's approved configuration documentation.
Configuration Control Board Directive (CCBD)	The document that records the ECP approval (or disapproval) decision of the CCB and provides the direction to the contracting activity either to incorporate the ECP into the contract for performing activity implementation or communicate the disapproval to the performing activity.
Configuration Documentation	Technical documentation that identifies and defines a product's performance, functional, and physical attributes (e.g., specifications, drawings). See also: allocated Configuration Documentation (ACD), Functional Configuration Documentation (FCD), and Product Configuration Documentation (PCD).
Configuration Identification	a. The systematic process of selecting the product attributes, organizing associated information about the attributes, and stating the attributes.
	b. Unique identifiers for a product and its configuration documents.
	c. The CM activity that encompasses the selection of CIs, the determination of the types of configuration documentation required for each CI, the issuance of numbers and other identifiers affixed to the CIs and to the technical documentation that defines the CI's configuration, the release of CIs and their associated configuration documentation, and the establishment of configuration baselines for CIs.
Configuration Item (CI)	a. An aggregation of hardware, software, or both that is designated for CM and treated as a single entity in the CM process.
	b. The entity within a configuration that satisfies an end use function and that can be uniquely identified at a given reference point.

TERM	DEFINITION
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.
Configuration Manager	The Government activity responsible for buying, managing, and sustaining the systems and items of hardware and software. The person(s) responsible for ensuring that the CM process is successfully executed for those systems and items is hereinafter referred to as the configuration manager.
Configuration Management Plan (CMP)	The document that defines how CM will be implemented (including policies and procedures) for a particular acquisition or program.
Configuration Status Accounting (CSA)	The CM function that formalizes the recording and reporting of the established product configuration information (including historical information), the status of proposed changes, and the implementation of approved changes and changes occurring to product units due to operation and maintenance. CSA implementation includes assurances that the information is current, accurate, and retrievable.
Contract	As used herein, denotes the document (e.g., contract, memorandum of agreement or understanding, purchase order) used to implement an agreement between a tasking activity (i.e., buyer) and a performing activity (i.e., seller).
Current Document Change Authority (CDCA)	The authority currently responsible for the content of a drawing, specification, or other document that is the sole authority for approval of changes to that document. See also: Application Activity (AA) and Approval.
Data	Information (e.g., concepts, thoughts, administrative, managerial, financial, and technical) that has been recorded in a form that is convenient to move or process regardless of medium or characteristics. Data can be tables of values of various types, numbers, characteristics, etc. See also: Data Item and Document.
Database	A collection of related data stored in one or more computerized files in a manner that can be accessed by users or computer programs via a database management system.
Data Item	A document or collection of documents that must be submitted by the performing activity to the procuring or tasking activity to fulfill a contract or tasking directive requirement for the delivery of information.
Defect	Any nonconformance of a characteristic with specified requirements.
Deficiencies	Deficiencies consist of two types:
	a. Conditions or characteristics in any item which are not in accordance with the item's current approved configuration documentation.
	b. Inadequate (or erroneous) configuration documentation which has resulted, or may result, in units of the item that do not meet the requirements for the item.
Design Change	See Engineering Change.
Digital Artifact	An artifact produced within, or generated from, the digital engineering ecosystem. These artifacts provide data for alternative views to visualize, communicate, and deliver data, information, and knowledge to stakeholders.
Digital Engineering	Information prepared by electronic means and made available to users by electronic data access, interchange, transfer, or on electronic/magnetic media.
Digital Twin	An integrated multiphysics, multiscale, probabilistic simulation of an as-built system, enabled by digital thread, that uses the best available models, sensor information, and input data to mirror and predict activities/performance over the life of its corresponding physical twin.

TERM	DEFINITION
Document	A self-contained body of information or data that can be packaged for delivery on a single medium. Examples of documents include drawings, reports, standards, databases, application software, engineering designs, and virtual part-models.
Document Representation	a. A set of digital files that, when viewed or printed together, collectively represent the entire document (e.g., a set of raster files or a set of initial graphics exchange specification files). A document may have more than one document representation.
	b. A document in a non-digital form (e.g., example, paper, punched card set, or stable-base drawing).
Engineering Change	a. A change to the current approved configuration documentation of a CI.
	b. Any alteration to a product or its released configuration documentation. Effecting an engineering change may involve modification of the product, product information, and associated interfacing products.
Engineering Change Proposal (ECP)	A proposed engineering change to the product and its configuration documentation, by which the change is described, justified, and submitted to a Configuration Approval Authority for approval/disapproval or deferral.
Firmware	The combination of a hardware device and computer instructions or computer data that reside as read only software on the hardware.
Fit	The ability of an item to physically interface or interconnect with or become an integral part of another item.
Form	The shape, size, dimensions, mass, weight, and other physical parameters that uniquely characterize an item. For software, form denotes the language and media.
Function	The action or actions that an item is designed to perform.
Functional Baseline (FBL)	The approved functional requirements for a product or system describing the functional, performance, interoperability, interface, and verification requirements established at a specific point in time and documented in the functional configuration documentation.
Functional Characteristics	Quantitative performance parameters and design constraints, including operational and logistic parameters and their respective tolerances. Functional characteristics include all performance parameters, such as range, speed, lethality, reliability, maintainability, and safety.
Functional Configuration Audit (FCA)	The formal examination of functional characteristics of a CI or system to verify that the item has achieved the requirements specified in its FCD or ACD.
Functional Configuration Documentation (FCD)	The documentation describing the system's functional, performance, interoperability, and interface requirements and the verifications required to demonstrate the achievement of those specified requirements.
Hardware	Products made of material and their components (mechanical, electrical, electronic, hydraulic, and pneumatic). Computer software and technical documentation are excluded.
Hardware Configuration Item (HWCI)	See Configuration Item (CI).
Interchangeable Item	A product which possesses such functional and physical attributes as to be equivalent in performance to another product of similar or identical purposes; and is capable of being exchanged for the other product without selection for fit or performance, and without alteration of the products themselves or of adjoining products, except for adjustment.

TERM	DEFINITION
Interface	The performance, functional, and physical characteristics required to exist at a common boundary between two or more systems. An interface is a system external to the system being analyzed that provides a common boundary or service that is necessary for the other system to perform its mission. Interface characteristics may include, but are not limited to, functional, physical, mechanical, visual, thermodynamic, magnetic, electrical, electronic, electromagnetic, software, or a combination of these characteristics.
Interface Control	The process of identifying, documenting, and controlling all performance, functional and physical attributes relevant to the interfacing of two or more products provided by one or more organizations.
Interface Control Documentation (ICD)	Interface control drawing or other documentation that depicts physical, functional, performance, and test interfaces of related or co-functioning products.
Interface Control Working Group (ICWG)	For programs that encompass a system, CI, or a CSCI design cycle, an ICWG is established to control interface activity among the tasking activity, performing activities, or other agencies, including resolution of interface problems and documentation of interface agreements.
Interoperability	The ability to exchange information and operate effectively together.
Item	A nonspecific term used to denote any product, including systems, materiel, parts, subassemblies, sets, accessories, etc.
Life cycle cost	The total cost to the tasking activity of acquisition and ownership of an item over its life cycle. As applicable, it includes the cost of development, acquisition, support, and disposal.
Lot number	An identifying number consisting of alpha and numeric characters that, in conjunction with a manufacturer's identifying Commercial and Government Entity (CAGE) code and a product-tracking base-identifier, uniquely identifies a group of units of the same item which are manufactured or assembled by one producer under uniform conditions and which are expected to function in a uniform manner.
Materiel	A generic term covering military systems, equipment, stores, supplies, and spares, including related documentation, manuals, computer hardware, and software.
Modular Open Systems Approach (MOSA)	An integrated business and technical strategy that:
	a. Employs a modular design that uses major system interfaces between a major system platform and a major system component, between major system components, or between major system platforms.
	b. Is subjected to verification to ensure major system interfaces comply with, if available and suitable, widely supported and consensus-based standards.
	c. Uses a system architecture that allows severable major system components at the appropriate level to be incrementally added, removed, or replaced throughout the life cycle of a major system platform to afford opportunities for enhanced competition and innovation while yielding significant cost savings or avoidance; schedule reduction; opportunities for technical upgrades; increased interoperability, including system of systems interoperability and mission integration; or other benefits during the sustainment phase of a major system.
	d. Complies with the technical data rights set forth in Sec 2320, title 10.

TERM	DEFINITION
Nomenclature	a. The combination of a Government-assigned designation and an approved item name. In certain cases, the designation root serves as the basis for assignment of serial or lot numbers.
	b. Names assigned to kinds and groups of products.
	c. Formal designations assigned to products by customer or supplier (such as model number or model type, design differentiation, specific design series, or configuration.)
Nonconformance	The failure of a unit or product to meet a specified requirement.
Notice of Revision (NOR)	A document used to define revisions to configuration documentation that require revision after ECP approval. See also Engineering Change Proposal (ECP).
Performing activity	An activity performing any of the requirements contained in a contract or tasking directive. A performing activity can be either a contractor or Government activity.
Physical characteristics (attributes)	Quantitative and qualitative expressions of material features, such as composition, dimensions, finishes, form, fit, and their respective tolerances.
Physical Configuration Audit (PCA)	The physical examination is the actual configuration of the item being produced. It verifies that the related design documentation matches the item as specified in the contract. The system product baseline is finalized and validated at the PCA.
Product Baseline (PBL)	Documentation describing all of the necessary functional and physical characteristics of the CI, the selected functional and physical characteristics designated for production acceptance testing, and tests necessary for deployment/installation, operation, support, training, and disposal of the CI. The initial PBL is usually established and put under configuration control at each CI's critical design review (CDR), culminating in an initial PBL at the system-level CDR. The system PBL is finalized and validated at the PCA.
Product Configuration Documentation (PCD)	A CI's detail design documentation including those verifications necessary for accepting product deliveries (first article and acceptance inspections.) Based on program production/procurement strategies, the design information contained in the PCD can be as simple as identifying a specific part number or as complex as full design disclosure.
Product Definition Information	Information that defines the product's requirements, documents the product attributes, including the process information, and is the authoritative source for configuration management of the product.
Product-Tracking Base-Identifier	An unchanging identifier used as a base for the assignment of serial numbers to uniquely identify individual units of an item or lot numbers to uniquely identify groups of units of an item. The product-tracking identifier is used rather than the Part or Identifying Number (PIN) because the PIN is altered to reflect a new configuration when the item it identifies is modified. The same product-tracking base-identifier may be used for several similar items (usually defined by a common document) and requires that each such item is assigned serial or lot numbers distinct from each other such item.
Release	The designation by the originating activity that a document representation or software version is approved by the appropriate authority and is subject to configuration change management procedures.
Released Document (Data)	a. Document that has been released after review and internal approvals.
	b. Document that has been provided to others outside the originating group or team for use (as opposed to for comment).

TERM	DEFINITION
Repair	A procedure which reduces, but does not completely eliminate, a nonconformance. Repair is distinguished from rework in that the characteristic after repair still does not completely conform to the applicable drawings, specifications, or contract requirements.
Repairable item	Any part or assembly which, upon failure or malfunction, is intended to be repaired or reworked.
Replacement item	An item which is interchangeable with another item, but which differs physically from the original item in that the installation of the replacement item requires operations such as drilling, reaming, cutting, filing, shimming, etc., in addition to the normal application and methods of attachment.
Request for Variance (RFV)	The means by which a manufacturer or supplier requests permission to depart from the product definition information for a specific unit, a specific number of units, or a specific period of time without requiring revision of the product definition information.
Retrofit	The incorporation of new design parts or software code, resulting from an approved engineering change, to a product's current approved PCD and into products already delivered to and accepted by customers.
Retrofit Instruction	The document that provides specific, step-by-step instructions about the installation of the replacement parts to be installed in delivered units to bring their configuration up to that approved by an ECP. (Sometimes referred to as an alteration instruction, modification work order, technical directive, or time compliance technical order.)
Rework	A procedure applied to a product to eliminate a nonconformance to the drawings, specifications, or contract requirements that will completely eliminate the nonconformance and result in a characteristic that conforms completely.
Serial Number	A numeric or alphanumeric (except for ammunition which only uses numeric characters) sequentially issued identifier used to designate a specific instance of a product among like products. An identifying number consisting of alpha and numeric characters that is assigned sequentially in the order of manufacture or final test and that, in conjunction with a manufacturer's identifying CAGE code, uniquely identifies a single item within a group of similar items identified by a common product-tracking base-identifier.
Software	Computer programs and computer databases.
Specification	A document that explicitly states essential technical attributes and requirements for a product and procedures to determine that the product's performance meets its requirements and attributes.
Submitted Document (Data)	Released document that has been made available to customers.
Support Equipment	Equipment and computer software required to maintain, test, or operate a product or facility in its intended environment.
System	A self-sufficient unit in its intended operational environment, including all equipment, related facilities, material, software, services, and personnel required for its operation and support.
Tasking Activity	An organization that imposes the requirements contained in a contract or tasking directive on a performing activity (e.g., a Government contracting activity that awards a contract to a contractor, a Government program management office that tasks another Government activity, or a contractor that tasks a subcontractor).
Technical Data	Recorded information (regardless of the form or method of recording) of a scientific or technical nature (including computer software documentation).

TERM	DEFINITION
Technical Data Package (TDP)	The authoritative technical description of an item. This technical description supports an acquisition strategy and production, inspection, engineering, and logistics support for the item. The description defines the required design configuration, performance requirements, and procedures required to ensure adequacy of item performance. It consists of all applicable technical data such as models, engineering design data, associated lists, specifications, standards, performance requirements, quality assurance provisions, software documentation, and packaging details.
Technical Documentation	See Technical Data.
Technical Reviews	A series of system engineering activities by which the technical progress on a project is assessed relative to its technical or contractual requirements. The reviews are conducted at logical transition points in the development effort to identify and correct problems resulting from the work completed thus far before the problems can disrupt or delay the technical progress. The reviews provide a method for the performing activity and tasking activity to determine that the development of a CI and its documentation have a high probability of meeting contract requirements.
Training Equipment	All types of maintenance and operator training hardware, devices, audio-visual training aids, and related software that:
	a. Are used to train maintenance and operator personnel by depicting, simulating, or portraying the operational or maintenance characteristics of an item or facility.
	b. Are kept consistent in design, construction, and configuration with such items in order to provide required training capability.
Verification	All examinations, tests, and inspections necessary to verify that an item meets the physical and functional requirements for which it was designed; that a component, part, or subassembly will perform satisfactorily in its intended application; or that an item conforms to specified requirements.
Version	a. One of several sequentially created configurations of a data product.
	b. A supplementary identifier used to distinguish a changed body or set of computer-based data (software) from the previous configuration with the same primary identifier. Version identifiers are usually associated with data (such as files, databases, and software) used by, or maintained in, computers.
Working Document (Data)	Document that has not been released; any document that is currently controlled solely by the originator including new versions of the document that were previously released, submitted, or approved.

4. CM LIFE CYCLE MANAGEMENT AND PLANNING

4.1 General. A basic principle of management is that responsibility, unlike authority, cannot be delegated. The Government PM, supported by the configuration managers, has the responsibility to ensure that the operating forces are provided with correctly "configured" hardware and software and the information necessary to operate and maintain the end item effectively. Regardless of the acquisition life cycle phase, this responsibility cannot be delegated, nor can it be taken lightly (see figure 2).

CM program strategy	Plan CM Program	Establish CM Program	Manage CM Program	Improve CM Program
	CM requirements and planning	CM Development and implementation	CM Implementation and maintenance	CM Maintenance and Disposal
Configuration management tasks and activities (Iterative)	**Develop CMP:**	**Implement CMP:**	**Update CMP:**	**Evaluate/review CMP:**
	CM Strategy Plan	CM professional onboard	Budget requirement	Continuous process improvement edits
	CM budget requirement	Allocated baseline	Initial product baseline	Budget requirements
	CM performance metrics	Training provided	Performance metric collection	Final product baseline
	CM training plan	Continuous process improvement	Training updated	Performance metrics
	CM process improvement metrics	Supplier and acquirer coordinate CM plans	Contract deliverables	Request for change
	CM Contract requirements strategy	Design review	Trace requirements	Configuration control board
	Functional baseline	Label configuration items	Request for change	Accounting reports
	Configuration item selection criteria	Configuration control board (CCB)	Manage configuration status and accounting data	Conduct physical control audit
	Configuration control process	Capture, record, and document information	Conduct functional control audit	Integrated logistics support
	Configuration status accounting	Status reports for verification and audit	Conduct readiness tests	
	Configuration verification and audit plan			

FIGURE 2. Configuration management process implementation view.

4.1.1 Configuration documentation. The documentation acquired by the Government and the degree of the Government's detailed involvement in configuration change decisions varies with the acquisition approach being utilized. The Government assumes control of configuration documentation in three progressive baselines: FBL, ABL, and PBL. As described in the DAG, the PBL is a snapshot of the item detail specifications and TDPs. It is the bottom level of the three technical baselines. The initial PBL is usually established and put under configuration control at each CI's (hardware and software) CDR, culminating in the system PBL established at the system-level CDR. The PBL is finalized and validated at the PCA. The final PBL is used by the manufacturers for the full rate production. The baselines are controlled by the use of Government CCB approval of any class I (major) changes and Government concurrence in class II (minor) changes typically adjudicated by Defense Contract Management Agency (DCMA) representatives. By assuming control of the baselines, the Government prevents changes that are not beneficial, cannot be supported, or are too costly. The Government configuration manager fulfills their responsibility through a great deal of hands-on management and detailed decision making.

4.1.2 Industry standards. The industry standard for CM, SAE EIA-649, cites CM principles and best practices. Each design activity is required to establish, document, and execute a CM process that addresses the CM principles and practices that are applicable to their products. SAE-EIA-649-1 is utilized by the Government CM to impose appropriately tailored requirements on contracts (see appendix B for tailoring guidance).

4.2 Management and planning concepts. This section contains a description of the CM process that is shared by both the Government and its contractors, its relationships with the systems engineering and logistics management processes, and the management relationships and activities to be applied across the life cycle.

4.2.1 CM functional activity. Figure 3 is a top-level CM activity model intended to be used as a reference point to plan and implement the major CM activities (functions) over the program life cycle. It provides an overview of the entire CM process from the Government's perspective and illustrates the relationships within the process. It shows the inputs (left), outputs (right), constraints (top), and implementing tools or methods (bottom) for each functional CM activity (represented by rectangular boxes).

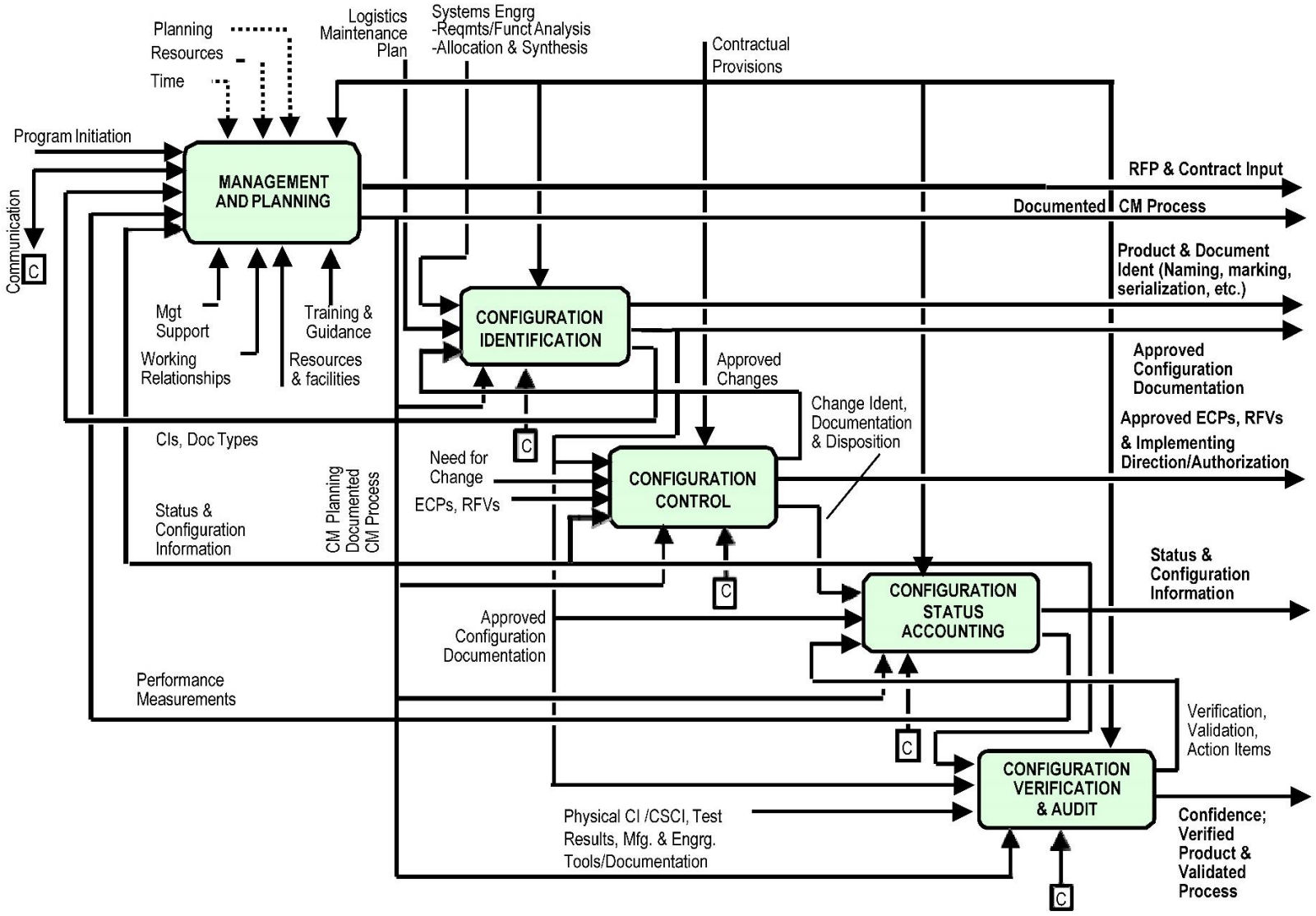

FIGURE 3. Top level configuration management activity model.

4.2.1.1 Management and planning. This block represents the core Government CM activity and its relationships to the other activities. Inputs to management and planning consist of the authorization to initiate the CM program, communications with all of the other CM activities, and selected information and performance measurements received from the status accounting activity. The activity is facilitated by the degree of management support provided, the working relationships established with such other interfacing activities such as Government program management, engineering and logistics, contractor CM, and DCMA. It is further facilitated by the resources and facilities assigned to the function including such resources as automated tools, connectivity to a shared data environment, and other infrastructure elements. Integrated product and process development and the use of Integrated Product Teams (IPT) by the Government and contractor facilitate the interaction and communications between all parties involved in a common CM process. The training and experience of the personnel and the guidance and resources they have at their disposal are also facilitators.

4.2.1.1.1 Management and planning constraints. The management and planning process may be constrained by a compressed time schedule for program execution, a lack of needed people and tools, or a lack of effective planning. It may also be constrained by contractual provisions which limit the Government configuration manager's sphere of control.

4.2.1.1.2 Management and planning outputs. The outputs from this activity consist of CM planning information and the resultant documented CM process that determine the extent of allocation of the CM functional activities to the Government and contractor. The need to perform the CM activities, described figure 3, is independent of any specific organizational structure, whether composed of IPTs or conventional functional organizations. The outputs from this activity also include SOW language and other information to be inserted in requests for proposals and contracts. If contract restrictions constrain either Government or contractor CM, it generally indicates ineffective planning and coordination of requirements, or lack of success in gaining management approval for proposed contract language.

4.2.1.2 Configuration identification. The configuration identification activity provides the foundation for all of the other Government CM functional activities. Facilitated by the documented CM process and by open communications, this activity interacts with system engineering (see 4.2.2). Through contractors, IPTs, and other means, it provides approved configuration documentation to document the physical and functional characteristics of the system and item, establishes baselines for Government and contractor configuration control, creates records in the status accounting database, and provides documentation for configuration verification and audit. In addition, product and document identifiers (nomenclature and numbering) are an important output from this activity.

Contractors are expected to have a robust configuration identification activity to define and baseline configuration documents and items at all levels, some of which may transition to Government configuration control depending upon applicable contract provisions. Although not specifically shown on figure 3, the data management (DM) activity, concerned with the identification, version/revision control, electronic access to, and distribution of all product information is implicitly related to this activity.

4.2.1.3 Configuration control. The Government configuration control process receives input from configuration identification defining the current configuration baseline. It receives and processes requests for engineering changes from Government and contractor organizations. It also receives requests for modifications to fielded items and facilities from DoD organizational units.

4.2.1.3.1 Configuration control constraints. The configuration control activity is constrained by contractual provisions, which determine the types and levels of documentation subject to Government configuration approval authority. It is facilitated by communications, the documented CM process, and information obtained from the status accounting database as needed. The CSA information includes the current implementation status of approved changes and other pertinent information concerning the configuration of items in design, in production, and in the operational inventory.

4.2.1.3.2 Configuration control documentation. The configuration control activity may communicate requests for documentation of engineering changes to contractors and Government entities. It subsequently provides for the review and approval or disapproval of proposed changes and for the necessary authorization and direction for change implementation by affected Government activities and contractors. It provides input to status accounting about change identifiers, the progress of the change documentation through the steps in the configuration control decision and authorization process, and the implementation status of authorized changes.

4.2.1.4 CSA. All other CM activities provide information to the status accounting database as a by-product of transactions that take place as the functions are performed. Limited or constrained only by contractual provisions and aided or facilitated by the documented CM process and open communications, this activity provides the visibility into status and configuration information concerning the product and its documentation.

4.2.1.4.1 CSA information. The CSA information is maintained in a CM database that may include such information as the as-designed, as-built, as-delivered, or as-modified configuration of any serial-numbered unit of the product as well as of any replaceable component within the product. Other information, such as the current status of any change, the history of any change, and the schedules for and status of configuration audits (including the status of resultant action items) can also be accessed in the database.

4.2.1.4.2 Metrics. Metrics (performance measurements) on CM activities are generated from the information in the CSA database and provided to the management and planning function for use in monitoring the process and in developing continuous improvements.

4.2.1.5 Configuration verification and audit.

4.2.1.5.1 Configuration inputs and outputs. Inputs to configuration verification and audit (FCA and PCA) include schedule information (from status accounting), configuration documentation (from configuration identification), product test results, the physical hardware or software product or its representation, manufacturing instructions, and the software engineering environment. Outputs are verification that the product's performance requirements have been achieved by the product design and the product design has been accurately documented in the configuration documentation. This process is also applied to verify the incorporation of approved engineering changes. Configuration verification should be an embedded function of the contractor's process for creating and modifying the product. Process validation by the Government in lieu of physical inspection may be appropriate.

4.2.1.5.2 Verification and audit. Successful completion of verification and audit activities results in a verified product and documentation set that may be confidently considered a PBL, as well as a validated process that will maintain the continuing consistency of product to documentation.

4.2.2 Relation to systems engineering process. CM is a key element in the systems engineering process, as illustrated on figure 3, because the system engineering process governs the product development and addresses all aspects of total system performance.

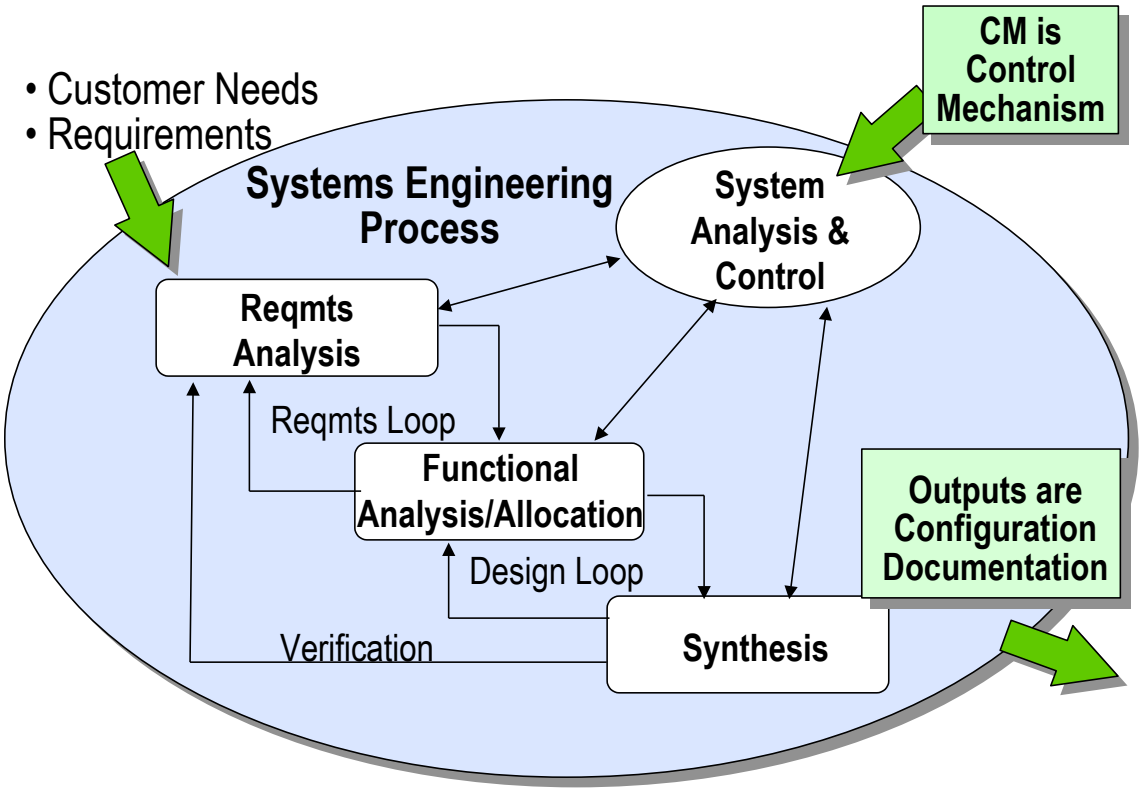

FIGURE 4. How CM relates to systems engineering.

4.2.2.1 Systems engineering and CM. In general, the systems engineering process is associated with operational analysis, requirements definition, and design determination. It includes defining the interfaces internal and external to the system including hardware-to-hardware, hardware-to-software, and software-to-software interfaces. The tools of systems engineering, typically exercised in an IPT environment, include:

a. Requirements analysis: used to determine system technical requirements and provide verifiable performance-based requirements in the system utilization environments and top-level functional requirements that must be met by the system.

b. Functional analysis and allocation: integrates the functional system architecture to the depth needed to support synthesis of solutions for people, products, processes, and management of risk. It is conducted iteratively to define successively lower level functions; the lowest level yields a set of requirements that must be performed by components of the system to meet the top-level requirements.

c. Synthesis: commonly understood as preliminary and detailed design, translates the functional and performance requirements into a description of the complete system that satisfies the requirements.

4.2.2.2 Systems engineering process. As shown on figure 4, the systems engineering process uses the "requirements loop" and "design loop" in an iterative analytic approach to make operational, requirements, and design decisions at successively lower levels. As the CM process iterates, requirements are defined, documented, and approved in the form of performance specifications for the FBL, and for CIs, the ABLs. Outputs of the system engineering process also include the basis for drawings or data sets that are released to produce the item and, after verification and audit, form the PBL. Thus, systems engineering is the process that produces the technical information for which the CM process provides technical control. As the CM process generates requirements for changes, the systems engineering process is exercised to define the technical basis for the change.

4.2.3 Relation to logistics process. The acquisition logistics activity is also related to systems engineering and is a strong component of the IPTs. Support and maintenance planning begins prior to engineering and manufacturing development (EMD) within each IPT and is iterated throughout the life cycle as changes in design and item performance dictate. A significant output of this process is the maintenance plan which articulates the maintenance concept for each item that requires support. Coordination with the logistics planning in general, and with the maintenance planning in particular, is essential to CM planning and implementation as illustrated on figure 5.

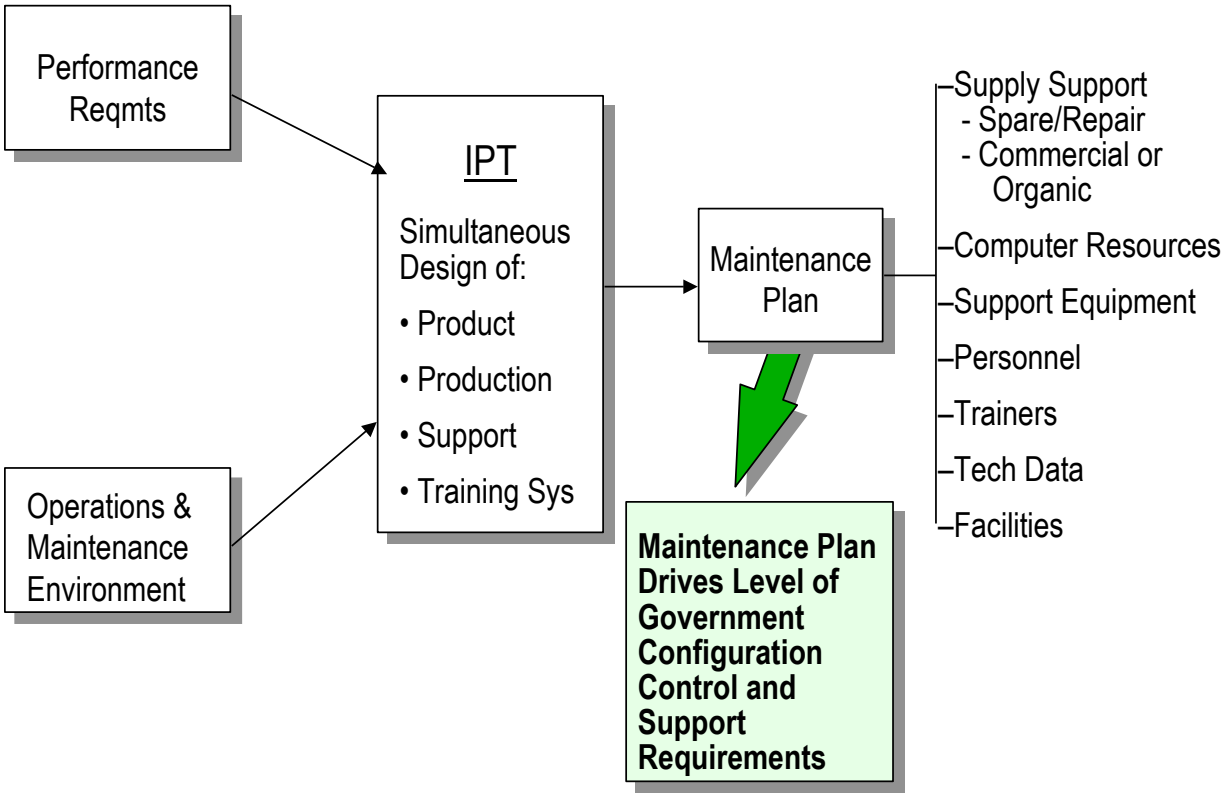

FIGURE 5. How CM relates to logistics.

4.2.3.1 Maintenance plan. The maintenance concept defines many of the factors that must be addressed in a mature logistics system. The maintenance plan is highly dependent on system and component reliability and on volatility of the technology used in the item design. These factors (and many others) are used to determine how the items, which constitute the system and component, will be supported (e.g., throw-away or repair and commercial or organic repair). The level of items that the Government decides to stock as replacement spares is the major influence on the level of Government configuration control. The maintenance plan includes the life cycle requirements for personnel, training, facilities, support equipment, supply support, and training devices and influences the information elements that may have to be provided to fully document an engineering change.

4.2.3.2 Logistics support. The goal for the Government is to create the proper mix of Government organic support and Original Equipment Manufacturer (OEM) support. The support approach should maintain the desired configuration (form, fit, function, and interface), facilitate tracking of fielded units, provide necessary spares, meet contingency requirements, maintain the technical data, and provide upgrades and improvements that enhance system availability and lower life cycle cost. The lowest equipment indenture level at which the maintenance concept determines that replacement is required, and for which the Government must order spares, determines the lowest level at which the Government needs to exercise configuration control.

4.3 Government management and planning activities. The Government's management and planning activities are common to all phases of the program life cycle, although the details upon which that management activity focuses varies from phase to phase. The global activities are illustrated on figure 6 and described below.

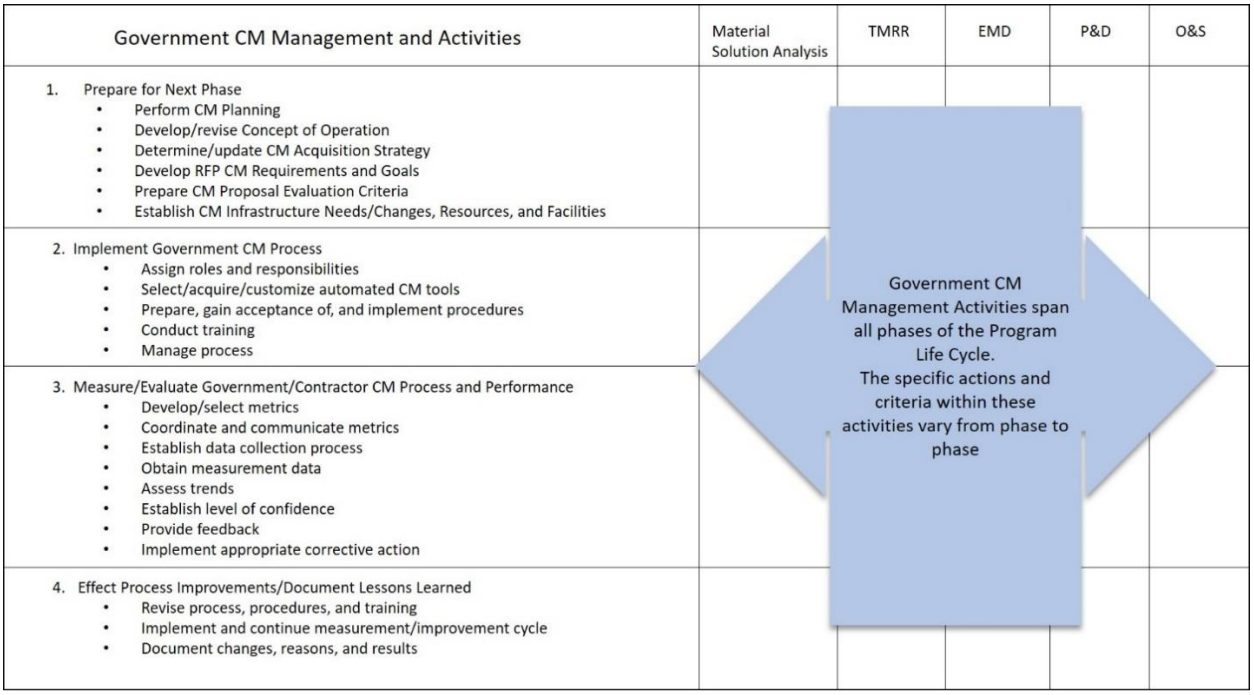

FIGURE 6. Implementations of "global" Government CM management activity.

4.3.1 Preparing for the next phase. During each phase of the program life cycle, preparation for the following phase takes place. For example, developing CM tasking for the EMD phase takes place in the Technology Maturation and Risk Reduction (TMRR) phase.

4.3.1.1 CM Planning. CM planning is a vital part of the preparation for each phase. CM planning consists of determining what the CM concept of operation and acquisition strategy for the forthcoming phase will be and preparing or revising the Government's CM Plan accordingly. Configuration managers should envision future phases and determine what information in the current and immediately following phase should be captured to meet the needs of those future phases.

4.3.1.2 CM roles and responsibilities. The roles and responsibilities of the Government CM activities and the contractor CM activities are defined by answering questions such as:

a. What information is required to support the Government CM goals for the next phase? Future phases?

b. What are the deliverables from the next program phase?

c. Which deliverables are CIs? Will contractors propose candidate CIs? How will the final listing of CIs be officially designated?

d. What is the end use of each CI?

e. How are they to be supported?

f. To what extent will the Government and the manufacturer support them?

g. To what level are performance specifications required? CIs? Repairable components? Replaceable components?

h. Will the Government prepare performance specifications, or will contractors?

i. Who in the contractor organization will be responsible for approving the performance specifications? In the Government organization?

j. What level of configuration documentation (e.g., performance specifications, detail specifications, complete TDP) will the Government and the contractor require by the end of the next phase?

k. What kinds of configuration identifiers (e.g., part numbers, serial numbers, nomenclature, National Stock Numbers) will the Government and the contractor require by the end of the next phase?

l. Which baselines (and documents) will already be subject to Government configuration control at the start of the next phase?

m. What baselines will be established by the contractor during the next phase? Functional? Allocated? Product?

n. What documents need to be included in those baselines?

o. Will control of any of the baseline documents transfer from the contractor to the Government during the next phase? When is the transfer planned to occur?

p. What status accounting will be needed in the next phase?

q. Which specific information should the Government provide? Which specific information should the contractor provide?

r. Does the program have approval to obtain the information in other than digital format? Will the Government need to have on-line access?

s. Who is the CDCA or lead subject matter expert for material identified on lower tiered documents with standing CCBs.

In addition to enabling the Government configuration manager to complete or update the CM plan, the answers to these questions also provide a rational basis for developing and coordinating CM and DM requirements to appear in requests for proposal and in formulating the criteria to be used to evaluate proposals submitted by contractors.

4.3.1.3 Request for proposal (RFP). The RFP should be compatible with the Government's CM plan; however, the CM plan should have sufficient flexibility to enable the CM strategic goals to be met with a variety of responses from contractors. The RFP also must send the message to the contractor(s) that the Government is serious about CM. It is also one of the best opportunities for the Government configuration manager to establish an environment in which contractor CM will have the support of its management. The proposal evaluation criteria (section L of the RFP) should have CM as a key management and past performance discriminator. Its weighting should reflect the significance that an effective, documented contractor CM process can have in mitigating risk.

4.3.1.4 CM analysis and justification. Preparation for the next phase is not complete until the Government configuration manager determines, and gains commitment for, the resources and facilities that will be needed to implement the Government's CM process. The infrastructure requirements must be adequate to support the program in accordance with the CM concept of operation and acquisition strategy. The goal is to perform a credible risk analysis in developing the concept of operations, which will provide convincing evidence to justify the investment in the CM process by showing that the investment will be returned many fold as a result of reduced costs for technical and logistic problems.

4.3.2 Implementing the Government CM process. During each program life cycle phase, the Government configuration manager implements the planned CM process. Preparing procedures and coordinating them with all participants in the process completes the process definition that was initiated in the CM planning activity preceding the phase each functional area must understand the particular roles and responsibilities that they have in the CM process. The tasks that they are to perform should be integrated into their workflow and given high priority. Coordinating the procedures is the initial step.

4.3.3 Measuring/evaluating Government/contractor CM process. Both the Government and the contractor CM process are measured and evaluated using metrics, program reviews, and other means such as contractor performance assessment reviews. Detailed information is contained in GEIA-HB-649 to assist in developing performance metrics as well as identifying process improvement opportunities based on captured metrics. The objectives help to focus the measurement on the most meaningful and important parameters; the metric presentation provides a level of confidence in the process being measured. Objective oriented metrics should be collected throughout the progress of the entire phase or at least until the stated objectives are realized.

4.3.3.1 DCMA. Since DCMA is the DoD agency that provides contract administration services and will interface with the contractor most directly on metrics and performance measurement issues, they should be involved as a full team member. Ideally, all should agree upon a common set of objectives.

4.3.3.2 Continuous improvement metrics. Metrics are key to continuous process improvement. Metrics constitute the data for improvement (i.e., the facts of the process). They enable problems that need attention to be quantified, stratified, and prioritized and also provide a basis for assessing the improvements and assessing trends. A properly constituted set of CM metrics supports both the CM goals and process improvement. Only a few critical items should be used at one time. They should be designed to positively motivate, rather than keep score, and should be forward focused (i.e., “where are we going”), not merely a compilation of past history.

a. A metric involves more than a measurement; it consists of:

(1) An operational definition of the metric which defines what is to be measured, why the metric is employed, when, where, and how it is used. It can also help to determine when a metric has outlived its usefulness and should be discontinued.

(2) The collection and recording of actual measurement data. In the case of the CM process, this step can often be accomplished by query to the status accounting database, which normally can provide a great deal of process flow information.

(3) The reduction of the measurement data into a presentation format (e.g., run chart, control chart, cause and effect diagram, Pareto charts, histogram) to best illuminate problems or bottlenecks and lead to the determination of root cause or largest constraint.

b. An effective metric has the following attributes:

(1) It is meaningful in terms of customer relationships (where the “customer” can be any user of information that is provided.)

(2) It relates to an organization’s goals and objective and tells how well they are being met by the process, or part of the process, being measured.

(3) It is timely, simple, logical and repeatable, unambiguously defined, economical to collect.

(4) It shows a trend over time which will drive the appropriate forward focused action which will benefit the entire organization.

4.3.3.3 CM cross functionality. CM by its very nature is cross functional. No important CM function is performed without interaction with other functional or team members. Therefore, CM objectives and measurements cannot and should not be divorced from the interacting systems engineering, design engineering, logistics, contracting and other program objectives and processes. Moreover, it is not the efficiency of CM activities, per se, that add value, but their result in contributing to overall program objectives.

Improving either the Government or industry CM process is a venture that typically requires interaction across a broad spectrum of program activities including technical, financial, and contractual. The process should be documented to a level of detail that is:

a. Easily understood by all participants in the process.

b. Focused on the key process interfaces.

c. Less detailed than the procedures used to perform the process but sufficient to determine what must be measured to obtain factual information on the process.

Refer to the latest version of GEIA-HB-649 for activity guides templates and additional information.

5. CONFIGURATION IDENTIFICATION

5.1 Configuration identification activity. Configuration identification incrementally establishes and maintains the definitive current basis for control and status accounting of a system and its CIs throughout their life cycle (development, production, deployment, and operational support until demilitarization and disposal). The configuration identification process ensures that all acquisition and sustainment management disciplines have common sets of documentation as the basis for developing a new system, modifying an existing component, buying a product for operational use, and providing support for the system and its components. The configuration identification process also includes identifiers that are shorthand references to items and their documentation. Good configuration control procedures (see section 44) assure the continuous integrity of the configuration identification. The configuration identification process includes:

a. Selecting CIs at appropriate levels of the product structure to facilitate the documentation, control, and support of the items and their documentation.

b. Determining the types of configuration documentation required for each CI to define its performance, functional, and physical attributes, including internal and external interfaces. Configuration documentation provides the basis to develop and procure software, parts, and material, fabricate and assemble parts, inspect and test items, and maintain systems.

c. Determining the appropriate configuration approval authority for each configuration document consistent with acquisition strategy and programmatic and logistic support planning for the associated CI.

d. Issuing identifiers for the CIs and the configuration documentation.

e. Maintaining the configuration identification of CIs to facilitate effective logistics support of items in service.

f. Releasing configuration documentation.

g. Establishing configuration baselines for the configuration control of CIs.

Effective configuration identification is a pre-requisite for the other CM activities (e.g., configuration control, status accounting, audit), which all use the products of configuration identification. If CIs and their associated configuration documentation are not properly identified, it is impossible to control the changes to the items' configuration, to establish accurate records and reports, or to validate the configuration through audit. Inaccurate or incomplete configuration documentation may result in defective products, schedule delays, and higher maintenance costs after delivery.

5.1.1 Basic principles of configuration identification. The basic principles of configuration identification are articulated in SAE EIA 649. It cites the following purposes and benefits of configuration identification:

a. Determines the structure (hierarchy) of a product and the organization and relationships of its configuration documentation and other product information.

b. Documents the performance, interface, and other attributes of a product.

c. Determines the appropriate level of identification marking of product and documentation.

d. Provides unique identity to a product or to a component part of a product.

e. Provides unique identity to the technical documents describing a product.

f. Modifies identification of product and documents to reflect incorporation of major changes.

g. Maintains release control of documents for baseline management.

h. Enables a user or a service person to distinguish between product versions.

i. Enables a user or a service person to correlate a product to related user or maintenance instructions.

j. Facilitates management of information including that in digital format (see 5.6).

k. Correlates individual product units to warranties and service life obligations.

l. Enables correlation of document revision level to product version/configuration.

m Provides a reference point for defining changes and corrective actions.

The basic principles guide effective configuration identification practices by both Government and industry. They are independent of specific methods of acquisition practice. A particular method of acquisition practice, such as "performance-based acquisition," influences the types of Government controlled documents selected to define systems or CIs and the delegation of responsibilities for approving changes to specifications and detailed design documentation. It also offers contractors flexibility in choosing the methods of design definition. However, it does not alter the necessity for both Government (the acquiring activity) and contractors (the performing activity) to implement practices that employ the basic configuration identification principles.

5.2 Configuration identification practices. The Government's configuration identification practices should be applied at the level necessary for effective identification and control based on the acquisition approach used and lifecycle phase. Contractor practices in accordance with SAE EIA-649 should be applied to commercial items used in Government systems; to CIs whose performance requirements are allocated, approved, and controlled only by the contractor; and to items that are within the contractor's design cognizance.

5.3 CIs. Selected items of system hardware or software (or combinations of hardware and software) in which the Government or acquiring activity has CM concern are designated as CIs.

5.3.1 CI concepts. CIs are the units of CM. They may vary widely in complexity, size, and type from an aircraft, ship, tank, electronic system, or software program to a test meter or a round of ammunition. Regardless of form, size, or complexity, the configuration of a CI is documented and controlled. CI selection separates system components into identifiable subsets for the purpose of managing further development. For each CI:

a. A unique identifier will be assigned.

b. There will be associated configuration documentation (which may range from a performance specification to a detailed drawing to a commercial item description). (See GEIA-HB-649.)

c. Configuration changes will be controlled.

d. CSA records will be maintained.

e. Configuration audits will be conducted to verify performance and product configuration (unless the CI has an already established PBL).

5.3.1.1 CI control. To define and control the performance of a system or CI does not mean that all of its hardware and software components must be designated as CIs, nor does it mean that the performance requirements for the non-CI components must be under Government control. The requirements to be met by a lower-level component (which is not designated as a CI) may be established and controlled via the Contractor's design and engineering release process. Government control typically occurs only when changes to the lower level components impact the Government-baselined performance specification for the CI.

5.3.1.2 CI selection. Initial CI selection should reflect an optimum management level during early acquisition. Initially, for EMD, the deliverable and separately installable units of the system and other items requiring significant management attention are designated as CIs. During production, fielding/deployment, and operational support, individual items required for logistics support and designated for separate procurement are also designated as CIs.

5.3.1.3 CIs for hardware and software. Computer software items are almost always designated as CIs because they typically control the functionality of a system. The term CI encompasses both hardware and software; when a statement in this handbook applies only to hardware, or only to software, the terms HWCI and CSCI are used.

5.3.1.4 Designating separate CIs. Typically, the top tier of CIs directly relate to the line items of a contract and the work breakdown structure. The determination of the need to designate them as CIs is normally simple and straight forward. However, there are many cases in which other lower-level items should also be selected based on the management needs of the program. Some of the primary reasons for designating separate CIs are:

a. Critical, new, or modified design.

b. Independent end use functions.

c. Sub-assembly factors, such as the need for separate configuration control or a separate address for the effectivity of changes.

d. Components common to several systems.

e. Interface with other systems, equipment, or software.

f. Level at which interchangeability must be maintained.

g. Separate delivery or installation requirement.

h. Separate definition of performance and test requirements.

i. High risk and critical components.

5.3.1.5 Importance of CI selection. Although the initial CI selection generally occurs early in the acquisition process, its consequences are lasting and affect many aspects of program management, systems engineering, acquisition logistics, and CM. CI selection establishes the level of Government configuration control throughout the system life cycle. Selecting CIs separates a system into individually identified components for the purpose of managing their development and support. Government CI designation should reflect the optimum level for both acquisition and support. During acquisition, this is the level at which a contracting activity specifies, contracts for, and accepts individual components of a system, and at which the logistics activities organize, assign responsibility, and report modification and maintenance actions during support.

During the MSA and TMRR phases, the system architecture is established, the program work breakdown structure is developed, and major CIs are selected. These activities provide the basis for the logistics supportability plan for the program. Development, acquisition, retrofit, and hardware and software interfaces are all affected by the breakout of the key system elements into CIs during the early stages of the development effort.

5.4 Configuration documentation. The term configuration documentation characterizes the information that defines the performance, functional, and physical attributes of a product. As described in SAE EIA-649, all other product documentation (such as operation and maintenance manuals, illustrated parts breakdowns, test plans, and procedures) are based on and relate to information in the configuration documentation. The configuration documentation associated with each CI provides the basis for configuration control, logistics support, post-deployment software support, and re-procurement.

5.4.1 Specification types. The selection of the appropriate specification document types is dependent upon a number of factors such as the maturity of the item and the context and environment in which it must operate. The new order of precedence defined by DoD policy strongly indicates preference for the use of existing commercial products, wherever possible, and the choice of products meeting performance rather than detail specifications.

Program unique specifications, of both a performance and detailed nature, are at the bottom of the preference hierarchy and are used when the other choices are not available or applicable. Nonetheless, acquisition programs dealing with the development of new systems will continue to see the use of program unique specifications where the specifications are being prepared for a single system or item and have little potential for future use except for repetitive fiscal year production and spares purchases. Both the Government and contractors should seize opportunities at lower levels of the specification tree (where developed items, referred to as non-developmental items [NDI] may be used) to select higher preference specification types, and to specify only performance and interface requirements rather than design solutions in those specifications, whenever possible.

5.4.2 Design constraints. The requirements of FBLs and ABLs are basically design constraints on the development contractor. The design solution evolves from the contractor's design and development process during the EMD phase of the life cycle. This process essentially converts the performance requirements of the baseline specification into a specific product definition that can be manufactured to produce a hardware item or compiled to produce a software item. It is documented in design documentation for the hardware and the software comprising each CI.

5.4.2.1 Drawings and models. For hardware, the design documentation may be in the form of engineering drawings and associated lists and the material and process documents that are referenced by the drawings. In the current information environment, the primary design documentation source may be in the form of two- or three-dimensional engineering models. In that case, a drawing is simply a two-dimensional view of a model that exists in a database file. Various models and product modeling tools may be employed. Engineering drawings may or may not exist as a central part of the product manufacturing process, depending on the product and the degree of automation technology employed.

5.4.2.2 Digital thread. In an automated development and production environment, an item is designed on the engineer's workstation, manufacturing instructions are added at the manufacturing planner's workstation, and the results are fed directly to automated machinery that produces the item. Commonly, items are designed using computer-aided design tools (CADAM, CATIA, AUTOCAD, etc.) and engineering drawings are plotted for human checking and review. Where engineering drawings or models are required as a contract deliverable, they should be developed and delivered in accordance with MIL-STD-31000. (See section 9).

5.4.2.3 CSCI. For software, the design evolves through a software engineering process, using a variety of integrated tools, often called the software engineering environment (e.g., computer-aided software engineering). The process results in computer based versions of documentation, source code, and executable code for every CSCI. The process the contractor employs to manage the automated software documentation (i.e., software library management and archiving) is similar to the process used to manage automated hardware documentation, although different tools may be employed. Upon close examination, it is fundamentally the same process used to manage the files, which contain software code. The same business rules apply to both software and documents in terms of their identification and relationships to other entities.

5.4.2.4 Efficient design solutions. Acquisition reform has essentially freed the contractor to implement the most efficient methodology for evolving the design solution in a way that is appropriate to the scope and complexity of the particular product or product line. It is important for the acquisition PM to recognize that there will be a great deal of diversity in the methodologies employed by various contractors, although there will also tend to be a great deal of similarities within given industry segments such as aerospace. Where it is necessary for the Government to capture the detailed design, the contractor may map the information in his or her internal databases to the appropriate fields of the Government's CM Automated Information System (AIS).

5.4.2.5 Defining configuration control. The developmental configuration documentation to be managed by the development contractor consists of the design and technical data under the contractor's internal control. Some of this data may transition to Government configuration control and some of it may remain under contractor configuration control throughout the program life cycle. The developmental CM process implemented by the development contractor consists of a formal process to control the documentation and repositories containing the elements of the developmental configuration. The contractor's engineering release system and engineering release records are an important part of this management process. Each and every version of all elements of the developmental configuration released, for whatever purpose, should be maintained along with the reasons the version was released and the rationale for superseding the previous version.

5.5 Configuration baselines.

5.5.1 Baseline concepts. The concept of baselines is central to an effective CM program; it is however, not a unique CM concept. The idea of using a known and defined point of reference is commonplace and is central to an effective management process. The essential idea of baselines is that in order to reach a destination it is necessary to know your starting point. In order to plan for, approve, or implement a configuration change, it is necessary to have a definition of the current configuration that is to be changed. In order to manage a program effectively, it is necessary to baseline the objectives for cost, schedule, and performance.

5.5.1.1 Acquisition program baseline (APB). The APB, established at Milestone A, B and C in accordance with DOD Instruction 5000.2, provides the PM with key cost, schedule, and performance objectives and thresholds which, if not met, would require a re-evaluation of alternative concepts or design approaches. This baseline bears a close relationship with the configuration baselines described in this section. The performance thresholds should be reflected in the system or top-level CI specification that constitutes the FBL for the program for those thresholds to be achieved.

5.5.1.2 Baseline representations. In CM, a configuration baseline is a fixed reference configuration established by defining and recording the approved configuration documentation for a System or CI at a milestone event or at a specified time. Configuration baselines represent:

a. Snapshots which capture the configuration or partial configuration of a CI at specific points in time.

b. Commitment points representing approval of a CI at a particular milestone in its development.

c. Control points that serve to focus management attention.

5.5.2 Major configuration baselines. Major configuration baselines known as the FBL, ABL, and PBLs, as well as the developmental configuration, are associated with milestones in the life cycle of a CI. Each of these major configuration baselines is designated when the given level of the CI's configuration documentation is deemed to be complete and correct and needs to be formally protected from unwarranted and uncontrolled change from that point forward in its life cycle. Under MIL-STD-973 and earlier CM standards, these baselines all signified departure points for Government configuration control; they must now be redefined for post-acquisition reform application because either Government or contractor configuration control may apply. The new definitions reflect the same purpose for each baseline, however the configuration control activity (which approves of changes to the baseline) is treated as a separate variable.

a. FBL: The approved configuration documentation describing a system's top-level CI's performance (functional, inter-operability, and interface characteristics) and the verification required to demonstrate the achievement of those specified characteristics.

b. ABL: The current approved performance-oriented documentation for a CI to be developed which describes the functional and interface characteristics that are allocated from those of the higher-level CI and the verification required to demonstrate achievement of those specified characteristics.

c. PBL: When used for re-procurement of a CI, the PBL documentation also includes the documentation describing the ABL (e.g., performance specifications, development specifications) to ensure that performance requirements are not compromised.

d. Development configuration: The contractor's design and associated technical documentation that defines the contractor's evolving design solution during development of a CI. The developmental configuration for a CI consists of that contractor internally released technical documentation for hardware and software design that is under the developing contractor's configuration control.

(1) All necessary physical or form, fit, and function characteristics of a CI,

(2) The selected functional characteristics designated for production acceptance testing, and

(3) The production acceptance test requirements.

5.5.2.1 Incremental baselines. Each configuration baseline serves as a point of departure for future CI changes. The current approved configuration documentation constitutes the current configuration baseline. Incremental configuration baselines occur sequentially over the life cycle of a CI as each new change is approved. Each change from the previous baseline to the current baseline occurs through a configuration control process. The audit trail of the configuration control activity from the CI's original requirements documentation to the current baseline is maintained as part of CSA.

5.5.2.2 Elements of an FBL. From a Government acquisition program perspective, the FBL is established when its associated FCD is approved by the Government. This baseline is always subject to Government configuration control. The FBL consists of the FCD, which is the initial approved technical documentation for a system or top-level CI as set forth in a system specification prescribing:

a. All necessary functional characteristics.

b. The verification required to demonstrate achievement of the specified functional characteristics.

c. The necessary interface and inter-operability characteristics with associated CIs, other system elements, and other systems.

d. Identification of lower level CIs, if any, and the configuration documentation for items (such as items separately developed or currently in the inventory) which are to be integrated or interfaced with the CI.

e. Design constraints, such as envelope dimensions, component standardization, use of inventory items, and integrated logistics support policies.

When included in the acquisition strategy, the Government's FBL is defined as a result of the concept and technology development phase. In the absence of a concept phase, the FBL is established during system development and demonstration. From a contractor's point of view, a FBL, whether formally established or not, is always in place at the inception of each phase. It is represented by whatever documentation is included or referenced by the contract to define the technical and performance requirements that the contractor's product is obligated by the contract to meet.

5.5.2.3 Elements of an ABL. The ABL can be considered a composite of a series of individual ABLs. Each ABL consists of the ACD, which is the current approved performance oriented documentation governing the development of a CI, in which each specification:

a. Defines the functional and interface characteristics that are allocated from those of the system or higher-level CI.

b. Establishes the verification required to demonstrate achievement of its functional characteristics.

c. Delineates necessary interface requirements with other associated CIs.

d. Establishes design constraints, if any, such as component standardization, use of inventory items, and integrated logistics support requirements.

The requirements in the applicable specification are the basis for the contractor's design of the CI; the quality assurance provisions in the applicable specification form the framework for the qualification-testing program for the CI. The ABL for each CI is documented in an item performance or detail specification, generally referred to as a development specification.

5.5.2.4 ABL configuration control. The specification(s) defining each ABL is subject to configuration control by either the Government or by the contractor. The configuration control activity determination is based on the acquisition approach used, lifecycle phase, logistical support requirements, and interface requirements. The Government should maintain configuration control authority only to the level necessary to ensure effective control and allow contractor configuration control authority below that level.

5.5.2.5 Established baselines. Based on the definition of the FBL, ABL, and PBLs as Government baselines, there has always been considerable confusion as to what to call the baseline established between a contractor and a sub-contractor. From the contractor's point of view, it is an ABL. From the sub-contractor's view, it is an FBL since it constitutes the top-level requirement that the sub-contractor must meet and which the sub-contractor may need to allocate further down the CI tree. Whether this baseline is considered an FBL, ABL, or a combined FBL and ABL, is immaterial so long as the configuration control requirements for the related configuration documentation are clearly established.

5.5.2.6 Interface control documents. Interface control documents are considered part of the FBL and ABLs to the extent that they are referenced in and supplement the performance specifications that constitute the applicable baselines.

5.5.2.7 Contractor design responsibilities. Contractor implementation of the FBL and ABL requirements involves the creation and release of engineering documentation that incrementally defines the configuration of the specific product. It represents the contractor's detailed design solution and may or may not include a detail specification for the product. The contractor is responsible for the configuration control of the developmental configuration and may iteratively design, release, prototype, and test until the functional and allocated requirements are satisfied. The developmental configuration will ultimately include the complete set of released and approved engineering design documents, such as the engineering drawings and associated lists for hardware and the software, interface, and database design documents for software. By reference within this documentation, it also includes test and verification documents.

5.5.2.8 PBL. The PBL is the approved documentation which completely describes the functional and physical characteristics of the CI and any required joint and combined operations interoperability characteristics of a CI (including a comprehensive summary of the other environment(s) and allied interfacing CIs or systems and equipment). It consists of the PCD, which is the current approved technical documentation describing the configuration of a CI during the production and deployment and operational support phases of its life cycle. The PBL prescribes:

a. All necessary physical or form, fit, and function characteristics of a CI.

b. The selected functional characteristics designated for production acceptance testing.

c. The production acceptance test requirements.

d. All ACD pertaining to the item, so that if the item were to be re-procured, the performance requirements for the item would also be included.

The PBL documentation includes the complete set of released and approved engineering design documents, such as the engineering models, engineering drawings, and associated lists for hardware, and the software, interface, and database design documents. These are the then current configuration of the documents that were considered the developmental configuration. The PBL may include the 2-D or 3-D engineering model of a hardware product, and for software, it includes a representation of the CSCI source code. It also includes by reference the material and process specifications invoked by the engineering documentation.

5.5.2.9 PBL configuration control. The configuration approval authority for the PBL for each CI is determined with the same supportability test as the allocated requirements, described above. The Government needs to take delivery of and control PCD at a level of detail commensurate with the operational, support, and re-procurement strategies for the given program. For repairable CIs developed wholly or partly with Government funding, design disclosure documentation is required to the lowest level at which the CI will be operated, maintained, repaired, trained, supported, and re-procured. A significant factor in this determination is data that is properly established as "Contractor proprietary". The Government will determine if it is necessary and cost effective to buy rights to the data, do without it, develop new data and CIs, or return to the original contractor whenever re-procurement or support of the CI is needed. When a CI is wholly developed with private funding and is acquired by the Government, the data normally available for the item (typically form, fit, and function documentation) is evaluated and included in the appropriate baselines.

5.5.2.10 Document order of precedence. The FCD, ACD, and PCD should be mutually consistent and compatible. Each succeeding level of configuration identification is a logical and detailed extension of its predecessor(s). The specification structure of MIL-STD-961, appendix A, facilitates this congruence since a separate specification is not created when a performance specification transitions to a detailed specification. Redundant documentation should be avoided to minimize the possibility of conflicts. If a conflict arises between levels of configuration documentation, the order of precedence is always FCD, then ACD, then PCD.

When viewed on a system basis, care should be exercised to assure that all of the top-level requirements are accounted for in individual lower-level documents. This is a key function of such reviews as system, preliminary, and critical design reviews, but is greatly facilitated by the use of automated requirements allocation and traceability tools.

5.6 Document and item identification. This section describes the concepts for the assignment of identifiers to CIs, component parts, and their associated configuration documentation. Clearly identified items and documentation are essential to effective CM throughout the life cycle, particularly during the deployment and operational support period when the marking on a part is the key to installing a correct replacement part and finding the proper installation, operation, and maintenance instructions.

5.6.1 Document identification. A document identification principle expressed in SAE EIA-649 is that each configuration document (as well as other documents) must have a unique identifier so that it can be associated correctly with the configuration of the item to which it relates. The DoD and all Military components use the following three elements to assure the unique identity of any document: CAGE code, document type, and document identifier. In addition, the revision identifier and date clearly specify a specific issue of a document.

5.6.1.1 Document representations. A document can have many representations (for example a word processor file and a paper copy or a CAD file and a representation of that CAD file inserted in a document). In addition to the identification assigned to each document, the digital files for each version of each representation of the document and its component files should be identified and managed.

5.6.1.2 Document responsibilities. It is the responsibility of each individual assigned to manage an item of configuration documentation to employ the appropriate procedures of his or her organization which ensure:

a. The assignment of identifiers to the configuration documentation, including revision and version identifiers, when appropriate, and procedures to control the engineering release of new or revised data.

b. The application of applicable restrictive markings.

5.6.2 Item identification concepts. The following principles in SAE EIA-649 apply to the identification of CIs; the terminology in parentheses are the common terms used in the defense, aerospace and electronics industries:

a. All products (CIs) are assigned unique identifiers (e.g., Nomenclature, CAGE code, Part/Item Number) so that one product can be distinguished from other products; one configuration of a product can be distinguished from another; the source of a product can be determined; and the correct product information can be retrieved.

b. Individual units of a product are assigned a unique product unit identifier (Serial Number) when there is a need to distinguish one unit of the product from another unit of the product.

c. When a product is modified, it retains its original product unit identifier (Serial Number) even though its part identifying number is altered to reflect a new configuration.

d. A series of like units of a product is assigned a unique product group identifier (Lot Number or Date Code) when it is unnecessary or impracticable to identify individual units but nonetheless necessary to correlate units to a process, date, event, or test.

5.6.2.1 Tracking identifiers. Contractors assign identifiers including serial and lot numbers to CIs and their component parts, as necessary, to establish the CI effectivity of each configuration of each item of hardware and software. Items are marked or labeled with their applicable identifiers to enable correlation between the item, its configuration documentation, and other associated data, and to track maintenance and modification actions performed. Thus, serial and lot numbers are also known as tracking identifiers. For software, applicable identifiers are embedded in source and, when required, in object code and in alterable read-only memory devices (firmware).

5.6.2.1.1 Military nomenclature and nameplates. The contract should specify requirements for the assignment of Government type designators and Nomenclature to CIs for which the Government needs to control, track and provide logistic support. Government Nomenclature is requested by a contractor and is included on CI nameplates.

5.6.2.1.2 Part or identifying numbers (PIN). The developing contractor assigns a discrete PIN, generally referred to as a part number, to each CI and its subordinate parts and assemblies. The part number of a given part is changed whenever a non-interchangeable condition is created.

a. Part number format is a contractor option and a wide variety of formats are employed. The standard constraint within the defense industry had been a limitation to no more than 15 characters including dash numbers. However, with the increasing use of commercial items that are not so limited, many current systems accommodate 52 characters. Some contractors employ a mono-detail system in which one part is detailed on one drawing, and the drawing and the part number is the same. For practical reasons, some employ a multi-detailing system in which the drawing number may detail several parts and assemblies. Others use tabulated mono-detail drawings in which a drawing includes several iterations of a part. In the latter two cases, the drawing number is a base to which dash numbers are assigned for discrete parts controlled by that drawing.

b. The significant criteria are as expressed in the principles above: The part number should uniquely identify the specific part. All CIs including parts, assemblies, units, sets and other pieces of military property are marked with their identifiers.

5.6.2.1.3 Software identifiers. For each CSCI, the software identifier consists of a name or other identifier and a version identifier, assigned by the developing contractor. The identifiers relate the software to its associated configuration documentation (software requirements specification, software design documents, etc.), revision and release date. The software and version identifiers are embedded within the source code, and are marked on media containing the software. A method is typically employed to display the identifier and version to the user of the software upon command.

a. In a structured analysis and design approach to software development, an identifier is assigned (which are usually mnemonic in form) to the software units below the CSCI level.

b. Firmware is labeled on the device or, if the device is too small, on the next higher assembly.

5.6.2.1.4 Serial and lot numbers. CIs should address the effectivity of subordinate parts and changes to subordinate parts. This means that the effectivity of a part is expressed in terms of the range of serial numbers of the CI end item into which it is assembled.

NOTE: There are other ways of expressing the effectivity, particularly in commercial industry, but whether lot, block, fiscal year contract, date, or other term is used, it should translate as closely as possible to which serial numbered CIs will have the part installed.

5.6.2.1.4.1 Serial numbers. There are also several kinds of related serial numbers that are employed in a CI production phase. The Government normally identifies the serial numbers to be affixed by the contractor on Government designated deliverable CIs. Government serial numbers are in a variety of formats depending upon the type of equipment and the policy of the acquisition command. The issuance of Government serial numbers should be avoided where the contractor has an acceptable process for assigning unique serial numbers.

5.6.2.1.4.2 Shop numbers. Contractors assign serial numbers (sometimes referred to as shop numbers) to units in production. All engineering, manufacturing, and quality data will refer to the shop numbers. These shop serial numbers may or may not correspond directly to the serial numbers to be marked on parts or nameplates (delivery numbers), because for various reasons the shop units may not complete the manufacturing process in sequence, or some units in the flow may be sent to another customer. (For example, two out of every three units of a system are supplied to the US Army, but the third unit is supplied to a foreign Government under a foreign military sale contract.)

5.6.2.1.4.3 Lot numbers. Where impractical to serialize individual units, because of quantity or composition of the part or material, lot numbers are employed to identify a group of identical parts. Typically, lot numbers are employed for subordinate parts below the CI level, but occasionally they are appropriate at the CI level (for example, with rounds of ammunition). The lot numbers are controlled and are subject to the same constraints as the serial numbers. The important factors, in evaluating a contractor's system of item identification is that:

a. There is an effective process for controlling the effectivity of parts by serial number (either shop number or delivery number).

b. A comprehensive cross-reference is maintained between the shop number of an item and its delivery serial number, or for lot-controlled items, between the manufacturing lot and the delivery lot.

5.7 Engineering release. Engineering release is an action that makes configuration documentation available for its intended use and subject to configuration control procedures.

5.7.1 Class I changes. The contractor's engineering release process should prevent all engineering releases related to a class I change to a Government approved document from being released until the Government has approved the class I change.

5.7.2 Engineering release records. Acquisition PMs should ensure that both Government activities and contractors follow engineering release procedures which record the release and retain records of approved configuration documentation (engineering release records). These records provide:

a. An audit trail of CI documentation status and history.

b. Verification that engineering documentation has been changed to reflect the incorporation of approved changes and to satisfy the requirements for traceability of variances and engineering changes.

c. A means to reconcile engineering and manufacturing data to assure that engineering changes have been accomplished and incorporated into deliverable units of the CIs.

5.7.3 Revision traceability. It is probable that during development, prior to product baseline approval, contractors would release versions of specifications and drawings to their various functional areas or IPTs or to the Government (e.g., for technical reviews, progress reports). It is important that the Government understands which versions were released prior to Government approval and product baseline release. It may be that the revision level at release is higher than the initial release of a "rev dash" or may be a format that the Government and supplier have agreed to (e.g., putting the letter "X" in front of the revision until Government approval and release of product baseline).

5.7.4 Release records. Detail design documents under contractor control should be kept current with all changes, modifications, and releases, including changes occurring as a result of test activity. The record of prior release and use history of configuration documentation represents the developmental history of the CI and may be needed to support cost trade-offs and the rationale for changes to design constraints. Release records should indicate superseded as well as superseding requirements at least until superseded configurations no longer exist. Superseded requirements may then be retained as historical information.

5.7.5 Engineering change process. All approved class I and II engineering changes released for production are identified by change identifiers. The change is documented and released prior to formal acceptance of the deliverable unit in which the engineering change is first installed. The contractor's release process should verify the approval/concurrence status of each class I or II change prior to the release of the related documentation for use in the generation of deliverable units. The release process and released documentation should identify engineering changes, and retain a record of superseded configuration requirements which are/were incorporated into delivered CIs.

Each approved engineering change is incorporated into all units, or into complete blocks of units, within one mission, design, series or type, model, series of the CIs affected. Verification of the production incorporation of authorized engineering changes is accomplished for all CIs. Documentation of the actual released configuration for each CI at the time of its formal acceptance is retained in release records. This information is of particular importance, especially if there are warranties associated with the CI or its components. Methods to ensure acceptable contractor engineering release systems include prior knowledge (through past performance) of the contractor's existing procedures, prior certification of the contractor's procedures, and a contractor's CM plan delineating his or her procedures.

5.7.6 Design disclosure. During the operational support period, the Government will need design disclosure information on all CIs down to the level that will be supported by the Government. In addition, the Government may need additional design details prior to or at the end of production, depending upon a number of factors such as:

a. The need for continued support of operational items to be considered for service life and disposal.

b. The type of specification to be used for re-procurement if re-procurement is anticipated.

5.7.7 Government data repository. In an integrated data environment, selected information in a contractor's release record may be shared by the Government or downloaded to a CM AIS. The actual documents also may be downloaded to the Government data repository. Until the transition to these standard systems is completed, a variety of methods are being employed to populate the databases being used by the various services. There is currently no standard engineering release system used by all Government activities.

5.8 Interface management. Another aspect of configuration identification to be considered during development is interface management, also referred to as interface control. Acquisition PMs responsible for new systems may have interfaces with other systems. Those interfaces constitute design constraints imposed on the programs. As the system is defined, other interfaces between system components become apparent. All of the interfaces between co-functioning items need to be identified and documented so that their integrity may be maintained through a disciplined configuration control process. In some cases, a formal interface management process should be employed in order to define and document the interface.

5.8.1 Interface management activities. Interfaces are the functional and physical characteristics that exist at a common boundary with co-functioning items and allow systems, equipment, software, and data to be compatible. The purpose of all interface management activity is that:

a. The detailed design of each of the co-functioning items contains the necessary information to assure that the items, when individually designed and produced, will work together (for example, the 115-volt plug to the 115-volt electrical outlet), and

b. If either item needs to be changed for any reason, its performance, functional, or physical attributes that are involved in the interface act as constraints on the design change.

5.8.1.1 Interface categorization. During development, part of the contractor's design effort is to arrive at and document external interface agreements, as well as to identify, define, control, and integrate all lower-level (i.e., detailed design) interfaces. To understand how a particular interface should be defined and managed, it is necessary to categorize the interface in a number of ways:

a. Contractual relationship: Are the items supplied by the same contractor or by different contractors? If different contractors, is there, or will there be, a contractual relationship (such as a subcontract or purchase order) between the parties to the interface?

b. Customer relationship (acquisition activity[ies]): Is the same acquisition activity responsible for both interfacing entities or are different activities or even services involved?

c. Hierarchical relationship: Is the interface at the system, CI, assembly, or part level?

d. Type(s) and complexity of technical interface attribute(s) involved: Is the interface mechanical, electrical, electronic, installation, data, language, power, hydraulic, pneumatic, space, operating range, frequency, transmission rate, capacity, etc. (to name a few)?

e. Developmental status: Is one, both, or none of the interfacing items an NDI? Do the interfacing items require parallel design and development?

Categorizing the interface in this manner defines the context and environment of the interface and enables the appropriate measures to be taken to define and control it. Each interface should be defined and documented; the documentation varies from performance or detailed specifications to item, assembly, or installation drawings to interface control documents/drawings. Some interfaces are completely managed within the design process, others require specific types of formal interface management activity. The simplest and most straightforward approach that will satisfy the above objective should always be chosen. Extravagant and complex interface management activity should only be undertaken when other methods are inappropriate.

5.8.1.2 Contractual relationships. Whether formal or informal interface management is employed, it is necessary that there be a legal responsibility on the part of the interfacing parties, since even the best intentioned technical agreements can break down in the face of fiscal pressure. If there is a contractual relationship, including a teaming arrangement between two or more parties to an interface, there is already a vehicle for definition and control. However, where there is no contractual relationship, a separate interface agreement may be necessary to define the interface process and provide protection of proprietary information. When the agreement involves two or more contractors, it is referred to as an associate contractor agreement; when two or more Government activities are the parties to the agreement, a Memorandum of Understanding (MOU) is generally used.

5.8.1.3 IPTs. Within an organization, and often with subcontractors, IPTs may be used to establish interfaces. Some interfaces should be defined through a formal interface management process involving ICWGs. An ICWG is a specialized IPT comprised of appropriate technical representatives from the interfacing activities. Its sole purpose is to solve interface issues that surface and cannot be resolved through simple engineer-to-engineer interaction.

Once interfaces have been agreed to by the parties concerned, they should be detailed at the appropriate level to constrain the design of each item and baseline the configuration documentation so that the normal configuration control process will maintain the integrity of the interface. Then it may be necessary to convene an ICWG or other mechanism on rare occasions to resolve change issues in a satisfactory manner. The Government lead is the arbitrator of issues that cannot be resolved by an ICWG or IPT, such as those issues that involve contractual matters requiring contract changes and agreement between different acquisition activities.

Refer to GEIA-HB-649 for activity guides templates and additional information.

6. CONFIGURATION CONTROL

6.1 Configuration control activity. Configuration control is perhaps the most visible element of CM. It is the process used by contractors and Government program offices to manage preparation, justification, evaluation, coordination, disposition, and implementation of proposed engineering changes and variances to affected CIs and baselined configuration documentation.

6.1.1 Configuration control objectives. The primary objective of configuration control is to establish and maintain a systematic change management process that regulates life-cycle costs and:

a. Allows optimum design and development latitude with the appropriate degree and depth of configuration change control procedures during the life cycle of a system/CI.

b. Provides efficient processing and implementation of configuration changes that maintain or enhance operational readiness, supportability, interchangeability, and interoperability.

c. Ensures complete, accurate, and timely changes to configuration documentation maintained under appropriate configuration approval authority.

d. Eliminates unnecessary change proliferation.

e. Ensures accurate documentation of the initial and change product configurations, along with records of the effectivity of the change in both documentation and actual product units.

f. Ensure coordination with CDCA for sub tier documents.

6.1.1.1 Span of configuration control. The span of configuration control begins for the Government once the first configuration document is approved and baselined. This normally occurs when the functional configuration baseline is established for a system or CI. At that point, complementary Government and contractor change management procedures are employed to systematically evaluate each proposed engineering change or requested variance to baselined documentation to assess the total change impact (including costs) through coordination with affected functional activities, to disposition the change or variance and provide timely approval or disapproval, and to assure timely implementation of approved changes by both parties. Configuration control is an essential discipline throughout the program life cycle.

6.1.1.2 Configuration control changes. Changes may be needed for a variety of reasons, such as to counter a new threat, insert new technology, and respond to technical and operational tests and evaluations or to correct problems. The Government activity responsible for configuration control (based on current information and contractor interface, where appropriate) confirms the need for change; sets thresholds for performance, cost, and schedule for the proposed change; determines that the change is technically achievable and affordable; and prepares a request for a change action. Depending on program life cycle, the change action could be prepared by the contractor or Government activity. One of the most significant contributors to configuration control efficiency and effectiveness is clear and concise communication between the Government, the CDCA, and the contractor prior to the formal request for the ECP. Ideally this occurs in an IPT environment.

6.1.1.3 Government change approval. The change approval decision is made by the Government when:

a. The change is to a requirement of a baselined configuration document controlled by the Government, or

b. A change to a configuration document controlled by the contractor has an impact on specified performance, supportability, and other contractually specified requirements pertaining to the CI and documentation controlled by the Government.

6.1.1.4 Contractor change approval. The change approval decision is made by the contractor when the change is to items/configuration documentation for which it is the configuration approval authority, provided those changes do not impact the Government's baselines.

6.1.1.5 Configuration control risks. An effective, well-defined configuration control process assures the Government program office that all changes to Government-controlled baselines, no matter how small or seemingly insignificant, are reviewed by the applicable configuration approval authority. Without an effective configuration control process, the program office runs the risk of delivering CIs with configurations that:

a. Are technically inadequate and fail to meet specified performance requirements.

b. Are not logistically supportable.

c. May be unsafe.

d. Result in wasted resources.

e. Do not provide an accurate historical record as a basis for future change.

6.1.2 Configuration control general concepts and principles. Configuration control of baselined configuration documentation is an integrated change management process including both supplier (generally a contractor) and acquirer (generally the Government) responsibilities for change preparation, justification, evaluation, coordination, disposition, and implementation. Through the configuration control process, the resulting impacts of the approved engineering changes and variances are identified and accounted for in their implementation.

6.1.2.1 Configuration control process evolution. The configuration control process evolves from a less formal process in the early phases of a program to a very disciplined and formal process during the EMD, Production and Deployment and Operations and Support System Development and Demonstration, Production and Deployment, and Operation and Support phases.

6.1.2.2 TMRR phase. In the TMRR phase (if applicable), when the program definition documents are being developed, the configuration control process is also less encompassing. As part of the systems engineering control process in this phase, there may be several informal requirements definition baselines established for convenience in assuring that all program participants are on the same page. An informal configuration control procedure is helpful in this phase for the review and coordination of changes to the evolving system level specifications.

6.1.2.3 EMD, production and deployment, and operation and support phases. During the EMD, Production and Deployment, and Operation and Support phases, a formal configuration control process is essential. The informal document change control that was practiced previously is insufficient for systems acquisition and sustainment. As the product is being developed and produced, configuration control focuses on the documentation defining performance, physical and functional characteristics, and the configuration of the product. While this top-level macro view appears simple and straight forward, a micro level view of the configuration control process can be considerably more complex.

6.1.3 Configuration approval authority. The contractual configuration approval authority approving the implementation of a change to a product (system/CI) may initially reside with a contractor or with the Government. It may transfer from the contractor to the Government or may continue to reside with the contractor throughout the life cycle of the CI. This authority is technically responsible for the performance of the product as well as fiscally responsible for funding changes to the product.

6.1.3.1 Government configuration control. The level of Government configuration control is generally determined as part of CI selection. During an acquisition program, it is the levels at which the Government specifies, contracts for, accepts, and plans to procure and logistically support the individual components of a system or CIs. Government configuration control always addresses the FBL and the ABLs established for lower level CIs whose specifications have been issued by or approved by the Government. Similar and related contractor configuration control practices also apply to CIs and component parts below the level of Government configuration control.

a. CDCA. The CDCA is the organization that has the decision authority over the contents of the document, reflecting proprietary or data rights to the information that the document contains. The CDCA may be a Government activity or a contractor, and its authority may be transferred. However, there is only one CDCA for a document at a time.

b. AA. There may be multiple configuration control authorities for a product with more than one user, each being a configuration approval authority for a given contract. If the configuration approval authority for one contract is the CDCA for the system/CI performance specification for the product, then the other configuration control authorities are considered application activities because their authority extends only to the use of the product and its documentation. They cannot authorize change to either, but they may participate in the change control process if asked for input by either the configuration approval authority that is the CDCA or by the Government lead AA.

6.1.3.2 Contractual configuration approval authority. The contractual configuration approval authority addresses the total set of documents that are baselined for the product controlled by that authority for a specific contract. This authority can be the CDCA for individual documents that require change (e.g., a system or CI performance specification). If it is not the CDCA for a given document, it does not have the authority to approve a proposed change to that document and, therefore, should solicit ECP approval from the applicable CDCA or select an alternate design.

6.1.4 Change classification. ECPs required to be submitted to the Government are classified as either class I or II. A class I ECP is approved by the Government's CCB and authorized with a contract modification. Unless otherwise specified in the contract, a class II change is typically reviewed for concurrence in classification by the local Government representative. For detailed classification criteria, see DD Form 1692 instruction sheet and GEIA-HB-649.

6.1.5 CCB. Government CCBs are established for all acquisition programs. (Contractors also employ a similar process for their internal configuration control.) CCBs are usually comprised of the joint command or agency body chartered to act on class I ECPs and requests for major or critical variances. The PM is responsible for disposition of changes at the CCB. They may delegate this authority. The CCB is a program management process used by the PM to ascertain all the benefits and the impacts of the change before the decision is made. When a decision is rendered, the CCB chairperson approves a CCB directive or equivalent letter/memorandum directing the appropriate implementing actions to be completed.

6.2 RFV. Variances are requested by producers (typically contractors) prior to manufacture, during manufacture, or after an item has been submitted for Government inspection and acceptance.[1] In order to be tendered for delivery or to be installed in an item to be tendered for delivery, the deviant item should be suitable for use.

[1] A variance requested during or after manufacture was formerly called a deviation or waiver. However, the processing rules for an RFV are identical to those for a deviation and waiver.

6.2.1 RFV concepts and principles. RFVs are most often used for production CIs delivered as a part of a production contract. RFVs are typically associated with current or future delivery of items that do not or will not conform to the Government-baselined configuration documentation. An RFV is submitted if during design and development the contractor determines that, for a valid reason (such as long lead time), a Government-required performance attribute will not be met or verified before scheduled delivery of a limited number of production units. An RFV is also submitted when prior to the beginning of the final assembly of the first affected serial-numbered unit of a CI, the contractor finds it necessary to deliver one or more parts in a configuration other than that described by the item's baselined documentation.

Action should be taken by the Government to ensure that approved RFVs are rarely submitted on a recurring basis. Recurring RFVs for the same item characteristic or issue should trigger Government concern that either corrective manufacturing action needs to be implemented by the contractor or that the CI's technical requirements may be too stringent. In the case of the latter, the Government should request a class I (major) ECP from the contractor for revising the CI's current technical documentation.

6.2.1.1 RFV classification. RFVs are classified by their originators as either minor, major, or critical, unless the contract specifies that a Government's technical representative is responsible for assigning the classification. For detailed classification criteria, see DD Form 1694 instructions sheet and GEIA-HB-649.

6.2.1.2 RFV approval. RFVs are normally processed for the benefit of the contractor since the Government wants the contractually specified configuration. The FAR (46.407) specifies that the Government should accept "non-conforming material" only when it is in the Government's best interests and there is appropriate consideration. Therefore, if the RFV is approved, it is imperative that the Government contracting officer negotiate an equitable consideration from the contractor based on either the quantity of CIs affected by the RFV or the extent the affected CIs do not meet the Government's contractual requirements (or both). Based on the CCB review, the appropriate consideration to the Government resulting from RFV approval should be estimated and furnished to the contracting office for negotiation.

NOTE: Minor RFVs are normally approved by the Government CO or other representative identified in the contract. The FAR (7.503) stipulates that approval of all RFVs (minor, major, or critical) is an inherently Governmental function and should not be delegated to Government support or defense contractors.

CIs tendered for delivery with either approved Government or contractor RFVs should be suitable for their intended use without requiring subsequent repair or restoration at Government expense.

6.3 NOR. A NOR is an ancillary document to the ECP, which conveys the specific change to a specific document. A NOR is required when it's necessary to specify the specific changes to the affected documents. For ECPs to documents that are controlled by the ECP originator, a NOR may be used at contractor option. Alternatively, the originator may describe the change to each document within the ECP. NORs are prepared and submitted to the Government in accordance with the configuration requirements of the applicable contract SOW and Contract Data Requirements List (CDRL)/DD Form 1423.

Refer to GEIA-HB-649 for activity guides templates and additional information.

7. CONFIGURATION STATUS ACCOUNTING (CSA)

7.1 CSA activity. CSA is the process of creating and organizing the knowledge base necessary for the performance of CM. In addition to facilitating CM, the purpose of CSA is to provide a highly reliable source of configuration information to support all program/project activities including program management, systems engineering, manufacturing, software development and maintenance, logistic support, modification, and maintenance.

7.2 CSA inputs and outputs. Because the complexion of the objects about which status accounting information is collected changes during the item life cycle, the specific outputs will vary. The inputs and outputs may be thought of as generic categories for which there are different specifics in each phase (see figure 7).

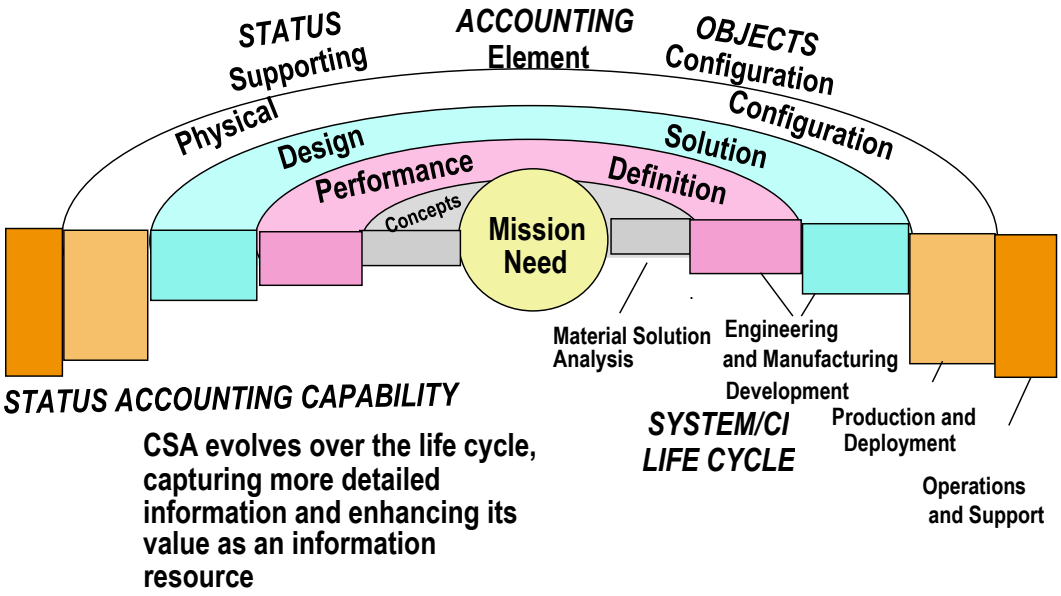

FIGURE 7. Status accounting objects.

7.2.1 CSA process. The high-level summary of CSA tasks reflects the functional performance capabilities of a complete CSA process which includes both Government and contractor activity (figure 8).

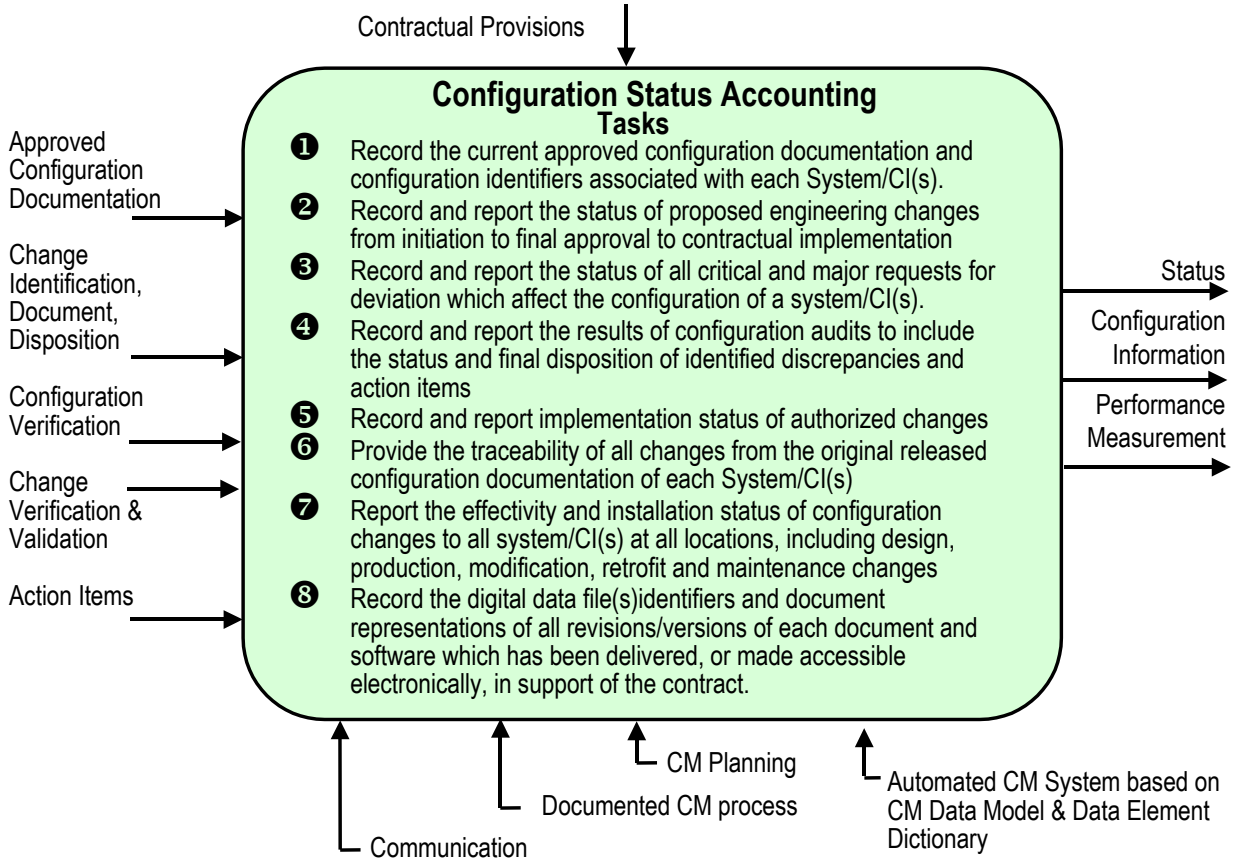

FIGURE 8. Configuration status accounting tasks.

7.2.2 CSA tools. All of the information required to accomplish the complete CSA function can be captured and supplied using commercial CM and product DM tools. With appropriate links to logistics and maintenance systems, the evolution of CSA information is possible over the life cycle.

7.2.3 CSA data. The Government's range of CSA information is normally limited to data for which they have configuration control and data for items for which they provide logistic support. The contractor normally monitors the data for those items it supports. Some of the CSA information that often must be shared between the Government and contractors concerns items under warranty. It is important for the Government to know what the warranty period is on each item that needs repair, as well as the date that the warranty began for each serial number. A ready reference to this data by logistics support personnel could result in cost savings to the Government if it is used to determine the priority used to ship items back to the manufacturer for repair. This is an instance of the Government adapting to standard industry practice. Typical SI information over the life cycle is found in table I.

TABLE I. Typical CSA information over the acquisition program life cycle.

Program Phase	Typical Information Sources	Typical Outputs
MSA/ TMRR Phase	• Mission need statements • Baseline performance/cost/schedule goals • System requirements documents for alternative configurations • Preliminary system performance specifications for selected configuration • ECPs or contract change proposals, as applicable	• Current revision of each document • CDCA and approval status for each document
EMD Phase	• System performance specification • CI performance specifications • CI detailed specifications • Engineering drawings and associated lists • CAD files • Test plans/procedures and results • Audit plans • Audit reports • Audit certifications • ECPs • RFV • NORS • Engineering orders, change notices, etc. • Installation and as-built verification • Removal and re-installation	• CDCA release and approval status of each document • Current (Government and contractor) FBLs, ABLs, and PBLs • Baselines as of any prior date • As-designed configuration, current, and as of any prior date • As-built configuration, current up to time of delivery and any prior date • As-delivered configuration • Status of ECPs, RFVs in process by contractor, by Government • Effectivity and incorporation status of approved ECPs, RFVs, including retrofit effectivity • Test and certification requirements to be completed prior to milestones such as reviews, demonstrations, tests, trials, and delivery • Verification and audit status and action items

TABLE I. Typical CSA information over the acquisition program life cycle – Continued.

Program Phase	Typical Information Sources	Typical Outputs
Production and Deployment	• All development phase items • System CI location by serial number • Support equipment and software • Spares • Trainers • Training materiel • Operating and maintenance manuals, IPBs • CI delivery dates and warranty data • Shelf life or operating limits on components with limited life or limited activations, etc. • Operational history (e.g., for aircraft take-offs and landings) • Verification/validation of retrofit instructions, retrofit kits • Incorporation of retrofit kits • Installation of spares, replacements by maintenance action	• All development phase items • Current configuration of all Systems/CIs in all locations (as-modified/as-maintained) • Required and on-board configuration of all Support equipment, spares, trainers, training, manuals, software, facilities needed to operate and maintain all systems/CIs at all sites • Status of all requested, in process, and approved changes and RFVs • Authorization and ordering actions required to implement approved changes, including recurring retrofit • Warranty status of all CIs • Predicted replacement date for critical components • Retrofit actions necessary to bring any serial numbered CI to the current or any prior configuration
Operational Support	• All production and deployment phase items	• All production and deployment phase items

Refer to GEIA-HB-649, Configuration Status Accounting Function, for activity guides templates and additional information.

8. CONFIGURATION VERIFICATION AND AUDIT

8.1 Configuration verification and audit activity. The configuration verification and audit process includes:

a. Configuration verification of the initial configuration of a CI, and the incorporation of approved engineering changes, to assure that the CI meets its required performance and documented configuration requirements.

b. Configuration audit of configuration verification records and physical product to validate that a development program has achieved its performance requirements and configuration documentation or the system or CI being audited is consistent with the product meeting the requirements.

8.1.1 Configuration verification and audit activity inputs. The common objective is to establish a high level of confidence in the configuration documentation used as the basis for configuration control and support of the product throughout its life cycle. Configuration verification should be an imbedded function of the contractor's process for creating and modifying the CI or CSCI. Validation of this process by the Government may be employed in lieu of physical inspection where appropriate. Inputs to the configuration verification and audit activity are:

a. Configuration, status, and schedule information from status accounting.

b. Approved configuration documentation (which is a product of the configuration identification process).

c. The results of testing and verification.

d. The physical hardware CI or software CSCI and its representation.

e. Manufacturing and build instructions and engineering tools, including the software engineering environment, used to develop, produce, test, and verify the product.

8.1.2 Configuration verification and audit activity completion. Successful completion of verification and audit activities results in a verified system/CI(s) and a documentation set that may be confidently considered a PBL. It also results in a validated process to maintain the continuing consistency of product to documentation.

8.2 Configuration verification and audit concepts and principles. There is a functional and a physical attribute to both configuration verification and configuration audit. Configuration verification is an on-going process. The more confidence the Government has in a contractor's configuration verification process, the easier the configuration audit process becomes. The reward for effective release, baselining, and configuration/change verification is delivery of a known configuration that is consistent with its documentation and meets its performance requirements. These are precisely the attributes needed to satisfy the ISO 9000 series requirements for design verification and design validation as well as the ISO 10007 requirement for configuration audit.

8.2.1 Configuration verification process. Configuration verification is a process that is common to CM, systems engineering, design engineering, manufacturing, and quality assurance. It is the means by which a contractor verifies his or her design solution. The functional aspect of configuration verification encompasses all of the tests and demonstrations performed to meet the quality assurance sections of the applicable performance specifications. The tests include verification and qualification tests performed on a selected unit or units of the CI and repetitive acceptance testing performed on each deliverable CI or on a sampling from each lot of CIs, as applicable. The physical aspect of configuration verification establishes that the as-built configuration is in conformance with the as-designed configuration. The contractor accomplishes this verification by physical inspection, process control, or a combination of both.

8.2.1.1 Change verification. Once the initial configuration has been verified, approved changes to the configuration should also be verified. Change verification may involve a detailed audit, a series of tests, a validation of operation, maintenance, installation, or modification instructions, or a simple inspection. The choice of the appropriate method depends upon the nature of the CI, the complexity of the change, and upon the support commodities that the change impacts. If the change is being introduced into a production line, and all future units will have the change incorporated via the production process, it is normally sufficient to ensure that:

a. Manufacturing instructions contain the change and are released for use (as with a work order), and

b. The first articles produced are inspected for compliance.

8.2.1.2 Change implementation. If support elements are impacted, or the change requires incremental retrofit to many units, complete implementation and verification of the change can be a lengthy process. Under these circumstances, implementation planning should define the extent to which the change to each unit and support commodity is to be verified and the records to be maintained. When materials, parts, or retrofit kits are ordered in incremental stages (e.g., per year, per month), the incremental ordering and supply actions should also be verified. Retrofit changes to organically supported items are verified and reported to the Government's status accounting system by the activity given installation and checkout responsibility for the retrofit. Changes retrofit by the contractor for contractor supported items are verified by the contractor.

8.2.2 Configuration audits. The dictionary definition of the word "audit" as a final accounting gives some insight into the value of conducting configuration audits. As has been discussed earlier in this handbook, CM is used to define and control the configuration baselines for the CIs and the system. In general, a performance specification is used to define the essential performance requirements and constraints that the CI must meet. When a performance specification is baselined by the Government, those requirements are contractual, so it is prudent for the Government to ascertain that the contractor has provided the expected performance capabilities. For complex systems and CIs, a "performance" audit is necessary to make this determination. Also, since development of an item involves the generation of product documentation, it is prudent to ascertain that the documentation is an accurate representation of the design being delivered. To the extent that the Government is buying the CIs to approved detail specifications, the Government would perform this kind of "design" audit. However, the design activity should perform both performance (FCA) and design (PCA) audits on all CIs in the deliverable product, especially if the Government does not intend to conduct audits on those particular CIs (usually because the applicable configuration documentation is not [will not be] under Government configuration control). If the design activity is a Government entity, audits should be performed as all CIs will be under Government control. The operation and life cycle support of the CI is based on this documentation. To fail to assure its accuracy can result in acceptance of items that will not perform as specified, or to greatly complicate future logistics support of the CI.

8.2.2.1 Configuration audit activity. Configuration audits provide the framework and detailed requirements for verifying that the contractor's development effort has successfully achieved all of the requirements specified in the configuration baselines. If there are any problems, it is the auditing activity's responsibility to ensure that all action items are identified, addressed, and closed out before the design activity can be deemed to have successfully fulfilled the requirements.

8.2.2.1.1 Configuration audit phase. There are three phases to the audit process, and each is very important. The pre-audit part of the process is the first phase and sets the schedule, agenda, facilities, and the rules of conduct and identifies the participants for the audit. The actual audit itself is the second phase, and the third is the post-audit phase in which diligent follow-up of the audit action items should take place. For complex products such as major weapon systems, the configuration audit process is a series of sequential and parallel audits of various CIs and the system to Government-controlled system and CI performance specifications conducted over a period of time to verify all relevant elements in the weapon system product structure. Audit of a CI may include incremental audits of lower-level items to assess the degree of achievement of requirements defined in specifications and documentation not controlled by the Government.

8.2.2.1.2 Configuration audit process. The audit process will normally involve audits conducted by prime contractors on subcontracted items at subcontractor facilities with or without Government participation (at Government option) and audits of prime contractor developed items conducted by the Government at the contractor's facility. Each item may be subjected to separate functional and physical audits, or both audits may be conducted at the same time.

8.2.2.2 FCA. The FCA is used to verify that the actual performance of the CI meets the requirements stated in its performance specification. In some cases, especially for very large, complex CIs and systems, the audits may be accomplished in increments. Each increment may address a specific functional area of the system/CI and will document any discrepancies that are found in the performance capabilities of that increment. After all of the increments have been completed, a final (summary) FCA may be held to address the status of all of the action items that have been identified by the incremental meetings and to document the status of the FCA for the system or CI in the minutes and certifications. In this way, the audit is effectively accomplished with a minimum of complications.

Although an FCA is only required once for each CI or system, a number of FCA-like activities may be accomplished at other times during the life cycle of the CI or system.

a. Many class I ECPs incorporate new design elements into the baselined design. The performance of each new design element should be verified to ensure that it will not degrade performance of the CI or system below the performance specified by its Government-controlled performance specification. The degree and type of verification will be included as part of the ECP; it may vary from a simple analysis of the similarity to the old design to a lengthy program of testing similar to the original verification testing accomplished during the EMD phase. However, it is important to understand that a complete retest and FCA are not required for each ECP; only the verifications specified in the ECP are required.

b. If the Government is controlling the detailed design, a production contract may require a "first article" inspection to be accomplished. This would include more comprehensive "testing" than the normal production acceptance tests, and the test data resulting from the "first article" would be subject to a review process not unlike an FCA.

c. An ECP or a new contract may call for the development of a new CI(s) and incorporation of the new CI into the system via a modification program. The expected performance of the new CI would commonly be defined in a performance specification, and the results of the verification testing of the CI would be checked at an FCA for the new CI. In addition, some retesting of the existing system elements with the new CI incorporated would normally be required, and those results would also be subject to a review similar to an FCA.

8.2.2.3 PCA. The PCA is used to examine the actual configuration of the CI that is representative of the product configuration in order to verify that the related design documentation matches the design of the deliverable CI. It is also used to validate many of the supporting processes that the contractor uses in the production of the CI. The PCA is also used to verify that any elements of the CI that were redesigned after the completion of the FCA also meet the requirements of the CI's performance specification. In cases where the Government does not plan to control the detail design, it is still essential that the contractor conduct an internal PCA to define the starting point for controlling the production design and to establish a PBL. Additional PCAs may be accomplished later during CI production if circumstances such as the following apply:

a. The original production line is "shut down" for several years and then production is restarted.

b. The production contract for manufacture of a CI with a fairly complex, or difficult-to-manufacture, design is awarded to a new contractor or vendor.

This re-auditing in these circumstances is advisable regardless of whether the contractor or the Government controls the detail production design.

8.2.2.4 Application of audits during life cycle. It is extremely unlikely that FCAs or PCAs will be accomplished during the MSA and the TMRR phase of the life cycle. Audits are intended to address the acceptability of a final, production-ready design and that is hardly the case for any design developed this early in the life cycle.

NOTE: An activity similar to the FCA (and sometimes the PCA) might be accomplished during the TMMR phase as a part of the completion of a competitive prototyping effort to facilitate the evaluation of the results of the competition.

a. During the EMD phase, the final, production, operationally ready design is developed. Thus, this phase is normally the focus for the auditing activity. Either the Government or the contractor will conduct a PCA for each CI that has completed the FCA process to "lock down" the detail design by establishing a PBL. CIs built during this phase are sometimes "pre-production prototypes" and are not necessarily representative of the production hardware. Therefore, it is very common for the PCAs to be delayed until early in the production phase of the program.

b. Requirements to accomplish FCAs for systems and CIs are included in the SOW tasking. The FCA is accomplished to verify that the requirements in the system and CI performance specifications have been achieved in the design. It does not focus on the results of the operational testing that is often accomplished by operational testing organizations in the services, although some of the findings from the operational testing may highlight performance requirements in the baselined specification that have not been achieved. Deficiencies in performance capability, as defined in the baselined specification, result in FCA action items requiring correction without a change to the contract. Deficiencies in the operational capability, as defined in user-prepared need documents, usually result in ECPs or contract changes to incorporate revised requirements into the baselined specifications or to fund the development of new or revised designs to achieve the operational capability.

c. It is normal that the first production units in the production, fielding and deployment, and operational support phase would be subjected to a PCA, which, depending on whether the acquisition strategy was performance or detail design based, would be conducted by the contractor or by the Government, respectively. This PCA allows the establishment of a PBL for the CI reflecting the design that will be delivered to the field and will require support. From a logistics support standpoint, it is essential that the support activity have an accurate picture of the exact configuration. If it does not, it is likely that the wrong spares will be acquired or redesign of the CI will be based on inaccurate information, leading to problems in the operation and support of the CI.

d. During a PCA, the representative deliverable item (hardware or software) is compared to the PCD to ensure that the documentation matches the design. This ensures that the exact design that will require support is documented. In some situations, a unit cannot be maintained or modified until its configuration is determined. In these kind of circumstances, it is often necessary to inspect the unit against approved PCD, as in a PCA, to determine where differences exist. Then the unit can be brought back into conformance with the documentation, or the records can be corrected to reflect the actual unit configuration.

8.2.2.5 Auditing in the performance-based acquisition environment. As discussed above, configuration audits address two major concerns:

a. The ability of the developed design to meet the specified performance requirements. The FCA addresses this concern.

b. The accuracy of the documentation reflecting the production design. This PCA addresses this concern.

8.2.2.5.1 Audit certifications. Over the years, prior to acquisition reform, the DoD developed hardware and software audit topics that were to be addressed by the FCA and the PCA, respectively. To document acceptability of a contractor's accomplishments in the FCA topic area, a series of certifications were established. Similarly, another series of certifications were established for the PCA topic areas. The audit teams completed the certifications that were applicable to the type of audit they were performing. Because the Government typically took control of the detail design, it conducted both FCA and PCA for each CI. The Government teams eventually addressed all the audit topic areas that were applicable to the type of item (hardware or software) being audited.

8.2.2.5.2 Audit certifications before acquisition reform. Acquisition reform policy requires acquisition of deliverable products based on performance specifications rather than detail specifications unless it is essential to buy an identical item. Using the certifications as they existed before acquisition reform would mean that:

a. The Government would normally conduct FCAs for the system and CIs with Government controlled performance specifications and would, thus, address (and certify) the FCA topics.

b. The contractor would normally conduct PCAs without any Government involvement. Thus, the Government would not address (and certify) any of the Government's PCA concerns. Therefore, because some PCA topics have applicability even in a performance-based acquisition, this handbook no longer attributes the topics of concern and the certifications specifically to either an FCA or a PCA.

Refer to GEIA-HB-649, Configuration Verification and Audits Function, for activity guides and additional information.

9. DATA MANAGEMENT (DM)

9.1 Description of DM. DM addresses the creation and management of all data and includes the activities of data requirements determination, data creation (from the data generator perspective), data acquisition (from the customer perspective), determination of data or Intellectual Property (IP) rights for technical data, data delivery, and the storage, management, and use of the data. The spectrum of data to be addressed includes both digital- and paper-based data and data regardless of its functional purpose.

9.2 Relationship to CM. DM is a parallel discipline to CM, but with a different focus. CM practices are applied to data that describes the item's functional or physical configuration or changes thereto. It usually includes design and functional requirements information such as TDPs or performance specifications, but often excludes logistics product data such as provisioning or maintenance planning data or other non-design data. But all product related data should be determined to be required, then acquired, stored, and made available for use by Government employees and others. Hence, it requires DM practices.

The interrelationship between CM and DM is such that most current CM guidance assumes that the CM data in the possession of the user and then describes how to use it to control item configurations. However, the CM guidance doesn't address how to acquire the CM data in the first place, nor considerations as to the IP rights the Government has for using the CM data. DM addresses the missing gaps of deciding what CM data is needed, acquiring this data from OEMs via contracts, determining and confirming the needed IP rights for Government use of this data, and the storage and use of the data by authorized users. This is an important distinction between DM and CM. DM addresses the entire life cycle of data and not all data is used for or placed under CM control.

9.3 DM activities. The intent of this section is not to provide an exhaustive description of how to perform the various DM activities. Such guidance already exists in various industry and DoD publications. Rather, this section will highlight key points or factors to consider about each of the activities and reference the applicable industry or DoD guidance documents for more details.

9.3.1 DM cost drives. Within DoD, the lack of good DM practices tends to manifest itself in one of three ways:

a. Not acquiring the data (and associated data rights) needed to support life assessment of materials or disposal;

b. Asking for too much data or, due to not understanding the true data needs and how we will use the data,

c. An inability to gain access to needed data, especially if the data is in the physical possession of the OEM.

As shown in figure 9, each of the above drive up life cycle weapon system acquisition and sustainment costs, which should be considered any time trade-off decisions are made relative to the acquisition of needed data. These issues and suggested best practices for avoiding them are discussed below.

FIGURE 9. DM life cycle costs.

NOTE: For more details about DM principles, methods, and tools, see GEIA-859.

9.3.1.1 Key DM activities. Key DM activities that affect product CM include:

a. Data requirements determination. For any new start development program, and even any life cycle phase contract within a program, the PM and functional area IPTs should determine the data needed to enable the performance of the various life cycle activities associated with that product. These life cycle activities include product development, test, manufacture, acquisition, logistics support, maintenance, operation, and disposal. Each functional area can identify the data needed by their practitioners to perform their set of functional life cycle activities.

b. Data call process. The data call process is used to solicit data inputs from the various functional areas.

c. Data requirements review. Data requirements review is used to review all collected data requirements, remove duplications, and validate need.

9.3.1.2 Key DM points. Key points to consider in a DM activity include:

a. Ensure all functional areas are surveyed for their data needs.

b. Consider all data that may be required. This will be more than just the traditional TDP.

c. Consider the content and form/format of the needed data. Today, most or all of the data will be digital, but determinations of 2D vs. 3D representation and formats usable by authoring tools available to the Government are important. An example of the latter would be a need to obtain design information in 3D CAD model form (native or translated format). Each 3D CAD authoring tool generates its models in a different and usually proprietary format. The Government should ensure it has the appropriate authoring tool software needed to open, read, and manipulate the models. This is also true for other types of product simulations and models.

Reference for further information: See DoD 5010.12-M for a more detailed discussion of data requirements determination.

9.3.2 Data acquisition. Most of the data about DoD weapon systems and components is generated by OEMs as part of one or more development contracts. In order for the DoD to legally acquire this data, it should be properly ordered as part of the development contract. DoD policy directs the use of Data Item Descriptions (DID) and CDRLs to order technical data in contracts. Each data item should have its own CDRL listing and if possible its own DID that describes the content and format of the data. Each CDRL data delivery should have one or more corresponding contract SOW work tasks that cause the generation of the data deliverable.

References for further information: See DoD 5010.12-M for a more detailed discussion of the use of DIDs and CDRLs. All existing DIDs can be found in the DoD Acquisition Specification and Standards Information System (ASSIST).

9.3.3 Data/IP rights. In recent years, DoD policy has encouraged the application of existing commercial or previously and privately developed technologies into its products. This approach can significantly reduce product development time and cost; however, the data relating to privately developed technologies is considered the IP of the OEM and gives them a competitive advantage over other contractors. In many cases, the Government wishes to have and use this data to either perform various life cycle activities or to have the ability to seek competitive sources for accomplishment of the activities. Ordering of the data in the contract alone does not ensure the Government will have the appropriate IP rights to use the data as intended. During contract negotiations, the Government should require any bidders to clearly identify any restrictions to the Government's use of the ordered data, and any differences between the needed IP rights and those offered by the bidders should be resolved. Below are some key points to remember about data rights:

a. The ordering of data in the contract does not in and of itself determine the Government's rights to use the data.

b. Use of DoD FAR Supplement (DFARS) clause 252.227-7017 in the RFP requires any bidder to identify any restrictions to the Government's use of the data ordered in the CDRL portion of the contract as part of their proposal. These restrictions should be known, validated, and resolved prior to contract award.

c. The Government is entitled to certain types of data automatically with unlimited rights. These types of data include Form, Fit, or Function (FFF) data and Operation, Maintenance, Installation, or Training (OMIT) data.

d. If the item or technology in question is considered non-commercial, and the data desired by the Government does not fall into the FFF or OMIT categories above, then the sources of funds used for the development of the item or technology will determine the Government's rights for use of the data. In general, the Government's standard rights are:

(1) Unlimited rights to any data associated with an item or technology funded 100 percent by the Government.

(2) Government purpose rights to any data funded by any mixture of Government and private funds.

(3) Limited or restricted rights to any data funded solely by private funds.

e. The Government can seek additional rights above the standard levels via negotiations with the OEMs.

References for further information: The DoD FAR Supplement (DFARS) Parts 27 and 52 define the rules regarding the Government rights to use technical data and computer software generated by or used in DoD contracts. The DoD FAR Supplement (DFARS) Parts 27 and 52 define the rules regarding the Government rights to use technical data and computer software generated by or used in DoD contracts.

9.3.4 Data access vs. data delivery. A concept that surfaced back in the 1990's was that the Government could save money by not actually "ordering" data in contracts, but rather just asking for the contractors to provide the Government "access" to the data stored in contractor IT systems. The theoretical benefit of this concept was that by not actually ordering the data, the Government would not have to pay the costs of data delivery or data rights (true). However, the resulting significant negative associated with this concept is that as a result of not ordering the data the Government has no legal rights to use the data and no way to ensure it is available except at the discretion of the developing contractor. Any data ordered on contracts for delivery to the Government should be reviewed for compliance with contract requirements and accepted or rejected. Some key points to consider regarding data delivery include:

a. "Delivery" usually means that the customer takes possession of the information.

b. "Access" allows the customer to gain access to data that are stored electronically at a contractor's or subcontractor's facility.

c. Contractually required "access" (i.e., "formal delivery") should be via a CDRL and DID.

d. Informal access via technical liaison does not equal "delivery."

e. By law, any enforceable right to see/access/have a copy of data requires an OMB approved DID or FAR/DFARS clause.

f. By contract terms, only "deliverable" data is subject to the DFARS Part 227 clauses requiring data rights assertions, markings, and justifications.

g. DoD has no useable rights (as a practical outcome) in data which is informally provided unless explicitly granted by the contractor and reviewed by legal counsel. Copyrights and typical proprietary markings bar any DoD use of that data.

h. DO NOT SUBSTITUTE ACCESS FOR DELIVERY!

i. Government review of submitted data deliverable for acceptance should include assessment of data content, format, and data rights markings. Only if all three are found to be in compliance with contract and specification requirements should the Government accept the data deliverable.

References for further information: Paperwork Reduction Act at 44 U.S.C. 3512, DoD 5010.12-M, section C3.3, and DFARS 215.470(b) regarding use of DD 1423 CDRL

9.3.5 Data storage. Once received, the data (CM or otherwise) should be stored and managed in an IT system, preferably some type of product DM system containing CM functionality. The services each have several Government operated Product Data Management (PDM) systems with these capabilities. Some OEMs offer PMs the option to store the data in their IT systems with the claim it will be cheaper for the Government. There are three fallacies with this approach to long-term, post contract end data storage and management by contractors:

a. Having a contractor store and manage Government owned data is not free. The Government should have a contract vehicle in place and fund the contractor to provide that service. It is usually costlier than storing the data in a Government owned DM system.

b. If the data resides only in the contractor's IT system, there is no guarantee nor often any safeguards to ensure the data or data rights markings on the data are not subsequently changed or modified. Only by having the "official" copy in Government possession can it be ensured no unauthorized changes occur.

c. If the Government contracts with a contractor to store our data and then the contract ends for any reason, the Government may have a very short period of time and limited ability to prepare for transferring the data to an organic DM system. Such a data transfer is a significant undertaking!

9.3.5.1 Master data sources. The existence of multiple data storage and management systems causes problems with respect to both cost of operation and difficulty of exchanging data between IT systems. Within each service, the lack of a single, common PDM-type system means that multiple systems with similar capabilities should be funded and operated. This drives up the cost of operating and maintaining those systems, and violates the DoD CIO IT system portfolio management guidelines of reducing and eliminating redundant or duplicative IT systems. The lack of standard PDM-type systems also makes it difficult or impossible to achieve the DoD digital engineering goal of integrating data, both within and between weapon systems, that is housed in different IT systems. It is costly and time consuming to build and maintain interfaces between different PDM-type systems to allow such data exchange and integration. Both of these problems get worse if PMs allow OEMs to store and manage weapon system technical data in their PDM-type systems, which can be different yet from any service PDM systems and over which we have no control or influence

Reference for further information: DAG, Technical Data Management section.

9.3.6 DM and use. Historically, weapon system PMs and IPTs have been fairly territorial about access to and use of technical data about their products. They usually allow personnel directly involved with the development or production of the product to access and use the data, but sometimes downstream functional organizations (logisticians) are not provided the same level of access, and personnel from other program offices usually have no access to, or even knowledge of, this data that they may find useful. Technical data about a product should be viewed as a DoD “corporate asset”, not just a “program asset”!

Providing access to, and use of, the same technical data by all functional areas involved in the life cycle activities of the product enables consistent use of the same data by the multiple disciplines and activities (i.e., a single source of truth). Allowing awareness of and approved access to data by other DoD personnel can save the Government significant time and money by allowing reuse of the data and avoiding the time spent searching for data when its location isn’t known, or recreating the data because personnel aren’t aware it exists and is already in the Government’s possession.

Reference for further information: DAG, Technical Data Management section.

9.3.7 Master DM. The DOD digital engineering strategy lays out goals for better usage and management of weapon system technical data. It correctly identifies the situation where multiple copies of a given data set may exist in different IT systems and be used or modified by different people for different reasons. It is, therefore, critical from a CM standpoint to know which instance of the data set is to be considered the “master” or “authoritative source” and which others are considered “copies.” All master instances of the data should be identified as such and configuration controlled. Any change to the master should be communicated to the owners of any copies so they can determine the impact of the changed master to their data copy.

A similar situation exists whenever new data is created by deriving or transforming it from an existing set of data. An example of derived data could be when provisioners use engineering drawings to create provisioning plans and lists. Changes to the engineering parts structure can impact and result in associated changes to the provisioning bill of materials, but only if the provisioning community is made aware of such changes to the “master” set of data. An example of transformed data could be the case of using a 3D CAD model to generate a 2D drawing representation, and offering both as part of the TDP used for item procurement and sustainment. Any changes made to the “master” CAD model should result in the transformed 2D drawing representation being regenerated so both forms of the data are kept in sync.

10. EMERGING TECHNOLOGIES

10.1 Introduction of emerging technology influencing CM and DM. CM principles identified in this handbook, when applied, ensure a comprehensive process for consistently documenting and maintaining any product’s performance, functional, and physical attributes with its requirements, design, and operational information. As the DoD moves from traditional paper and electronic media into the age of modeling, simulation, and digitalized artifacts, the need for application of CM principles remain unchanged if not increased. This section has been developed to introduce new types or forms of data that may be encountered and provides guidance for contracting and managing artifacts resulting from this technology.

10.2 Need for updating engineering practice. To ensure continued technological superiority and increased speed of delivery of ever-changing systems to the warfighter, the DoD is transforming the current document-based practice (both paper and digitized documents) to a model-based approach. Models incorporating a variety of product information will be used as the basis for information exchange rather than the current separate domain and review-specific documents. The new approach will utilize advancements in technology, computing power, and storage capacity to create integrated information-rich models of the product that can be used throughout the life cycle. This is a paradigm shift from the traditional acquisition methodology.

As the acquisition process adopts model-based approaches, there will be a need to access greater amounts of data during the system(s) life cycle. The shift will bring new software, incorporating increasing amounts of data, and new challenges for CM, and will necessitate the creation of shared resources that model a digital representation of physical and functional characteristics of a system from concept to disposal.

10.3 CM for digital environment. To advance the engineering practice to better equip the warfighter, the current infrastructure and IT environments will need to move toward a more consolidated, collaborative, and trusted environment. This environment will create challenges as new digital artifacts will utilize a wide range of software and hardware currently not in use by engineering activities, and should be able to operate in a DoD IT infrastructure and be accessible by multiple organizations across the country and possibly worldwide. The approach will make defense systems more effective and more reliable, expedite engineering activities, conserve resources, and reduce risks.

10.3.1 Digital environments. Digital environments will rely on technologies to increase their storage, communication, and collaboration abilities across different engineering disciplines. These technologies become a necessity as the volume of digital data about the product will continue to increase during the life cycle, posing constant challenges to data storage and network accessibility. The digital environment needs to be designed, realized, and deployed in a manner that enables it to be ever increasingly integrated, flexible, adaptable, and maintainable. These engineering environments may be unique to programs, but they also may be unique to an enterprise. In a digital environment, CM will need to address:

a. Models, viewpoints, and datasets.

b. Digital artifacts.

c. Processes, algorithms, and computations.

10.3.2 Modeling in a digital environment. Models provide a data-rich and digitally precise representation at a point in time of a system throughout all phases of acquisition. As models mature in the digital environment, they will evolve, and their behavior and performance will become indistinguishable from their physical counterparts and form the basis of the digital twin. An important aspect of the digital twin is the viewable datasets and viewpoints used to produce products and deliverables for the customer. The viewpoint is the location of the data in the model used to produce an artifact. For example, in systems modeling language (SysML), the viewpoint would be the data in a diagram (e.g., parametric diagram, requirements diagram, etc.). Artifacts can come in many forms, from 2D CAD to 3D .pdf. If the viewpoints remain in the digital environment, CM controls should be in place to maintain continuity of the dataset contained in that particular viewpoint to ensure proper continuity of the model. Models used in engineering activities will contain data for, but not limited to:

a. Systems and system requirements.

b. Management of changes within engineering, including requests and orders, their urgency and impact, and change processes.

c. Production planning, including order effectivity.

10.3.3 Approving changes. CM is focused on controlling and managing changes to the master data set, also referred to as the authoritative source of truth. CM must therefore include a formal change management process that provides traceability of any changes made to a data set. This process is necessary to ensure engineers are accessing the most up-to-date version of the modeled system.

10.3.4 Inserting changes. Traceability of changes during life cycle activities will allow clear communication between engineering disciplines. Proper version control of the system following changes will create a more accurate digital representation, thus limiting errors during production of the physical system.

10.3.5 Digital twin. A digital twin uses the best available models, sensor information, and input data to mirror and predict activities and performance over the life of its corresponding physical twin. From a CM standpoint, this means not only are acquisition and management of the product design (the "as designed" configuration) a concern, but also the "as built" configuration of each physical instance of the product that roles off the production line and in turn, the "as maintained" configuration of those same physical instances during their field lifespan as modifications are made and approved ECPs incorporated. These sets of product configuration identification information ("as built" and "as maintained" configurations) have not historically been ordered from producers or captured or managed by CM practitioners, except in certain circumstances such as airworthiness and flight safety concerns for aircraft. The CM and PM communities should recognize this new data need and work with our industry partners to develop methods to acquire, manage, and maintain this new and very voluminous set of product configuration information to enable the life cycle digital thread benefits.

10.4 CM for digital artifacts (tracking digital views [prepared deliverables for the customer]). Digital artifacts are defined as any digital item(s) that contains data and information and forms part of the digital representation of an engineered system. Generally, these artifacts will be used at reviews and milestones to visualize, communicate, and deliver data, information, and knowledge to stakeholders. The use of static artifacts increases the challenges of CM. Static artifacts include any data or physical documents extracted from the digital environment. Approved changes should be applied to the baseline digital environment to maintain configuration control. This will ensure new or re-generation of static artifacts, if required, are representative of the approved baseline configuration. CM processes are required to ensure traceability of changes between the baseline model and any static artifacts and reflect the current configuration baseline.

Reference for further information: IEEE 828.

10.5 CM for processes, algorithms, and computations (data). In a digital environment, processes, algorithms, and computations can be reused to increase productivity of engineering activities. For models, libraries can extend to form catalogs available for reuse across the development of systems of interest. Libraries can be built that bind the complexity of the configuration task, improving the quality and efficiency of the systems engineering process. Managing this information will help ensure continuity and prevent errors. Software tools can be used to handle version control, parallel development, workspace management, process configurability, and build management.

Reference for further information: STAR JPSS Algorithms Integration Team Configuration Management Plan, NOAA NESDIS STAR Center for Satellite Applications and Research.

10.6 MOSA.

10.6.1 MOSA in DoD defense systems. The DoD strives to affordably address emerging threats, evolving technology, component obsolescence, continued sustainment, and security challenges when acquiring defense systems. When practicably applied, design modularity and open business practices are effective methods to address these and other challenges. However, stakeholder interdependencies and respective processes can impact the effectiveness of MOSA implementations. Successful implementations of MOSA should be coupled with the ability for acquisition professionals to clearly understand the respective acquisition processes, cultural behaviors, and desired outcomes across multiple domains.

In defense systems, MOSA has multiple, similar definitions. MOSA is defined for the DoD as "an integrated business and technical strategy for competitive and affordable acquisition and sustainment of a new or legacy system (or a component within a new or legacy system) over the system life cycle." The modular approach uses an architecture that separates the system into major functions and elements, which work together across interfaces based on widely supported, consensus-based standards for which the program can verify conformance.

10.6.2 Consideration of commercial-off-the-shelf (COTS) for MOSA solutions. The use of COTS/NDI can provide significant opportunities for efficiencies during system development but can also introduce certain issues regarding intellectual property rights, single sources of supply, and possible future parts obsolescence that should be considered and mitigated for programs to realize expected benefits. There is difficulty in finding suitable replacements or alternate items if COTS vendors stop manufacturing products or changes configurations drastically, requiring the need to maintain different configurations of a single product. Successful implementation of a program's MOSA strategy facilitates the identification of the required technical data and software deliverables necessary to field and maintain products.

a. When utilizing COTS products as a MOSA solution, CM is needed to provide awareness of upgrades or changes to system features and functions (see DAG, Commercial-Off-the-Shelf, Chapter 3 "Systems Engineering" and Chapter 4 "Life Cycle Sustainment").

b. MOSA should be included as one of the evaluation criteria for contract proposals.

c. RFPs and other contract language can be leveraged to obtain appropriate data and data rights in support of a program's MOSA implementation strategy and should be facilitated by CM.

d. Technical baselines are established for modular architectures and require configuration control.

e. See DI-MGMT-82099 for more details on the open systems management plan.

10.6.3 MOSA hardware and software reuse considerations. MOSA enables reuse of system, hardware, firmware, or software throughout the acquisition life cycle.

10.6.4 MOSA architecture considerations. The architecture and design of modular, open systems is integral to ensuring that multiple well-supported solutions are considered. It is imperative for system architectures to be placed under configuration control and maintained with appropriate architecture descriptions and its relationships to each of the architecture baselines. Standards-based interfaces allow individual architecture elements to evolve separately and with minimal impact to other elements in the systems. MOSA couples the technical design with open business practices, such as access to appropriate data, to create opportunities for improved warfighting ability of the system, lessened sustainment burden, and increased competition among suppliers.

a. CM considerations include the control of MOSA CI form, fit, function, and interface characteristics.

b. CI level requirements addressing the control of documents describing interfaces is required such as interface specifications, interface standards, and interface control drawings.

c. CI level requirements addressing interfaces that compose the system for each build or increment should be managed.

d. Framework and interfaces for MOSA architecture may be considered when establishing CIs.

e. DM is needed to align MOSA and the functional architecture to SOW requirements, DIDs, and CDRL items consistently across the enterprise.

f. Hardware-dominant programs should consider addressing requirements and interface specifications for CSCI, computer software components, and computer software units as reviewable artifacts in support of system technical design reviews, such as the preliminary design review.

g. Software-dominant programs will need to consider CM and associated change control and review boards can facilitate the management of build and increment information.

h. Digital engineering promotes the use of data and models as a continuum to support life cycle activities from concept through disposal. These functions of digital engineering can assist MOSA to enable a program to respond to change with accuracy and in a timely manner. Digital engineering can be used to digitally capture, as part of its technical data, the interfaces between and within platforms and components.

10.6.4.1 MOSA interface management. There are multiple ways to implement MOSA, but each contains various elements of technical and business enablers. It is important to determine expected outcomes up front in order to determine which elements of business and technical enablers to employ. For instance, if the user or sustainment stakeholders desire reconfigurable and interchangeable components, then defining modular interfaces with widely accepted standards would drive design implementations and interoperability opportunities. Employing MOSA enables the sharing of modular components across products, accompanied by appropriate data, easing the sustainment and parts procurement burdens.

a. CM will be needed to facilitate the synchronized acquisition of data for modular open systems and interfacing architecture elements.

b. The interface management process is an integral part of CM, as it is critical to the success of the integration process. Interface control specifications or interface control documents should be confirmed early and placed under strict configuration control.

c. All of the program's external interfaces and dependencies should be documented and controlled. When a system is designed into components and interfaces, there is an advantage to specifying interfaces using widely used, consensus-based standards. The question of whether to subscribe to open or not fully open interfaces with the use of consensus-based standards is the dilemma most DoD acquisition programs face. There are advantages to engaging with cooperative efforts, or consortiums, to shape standards development that address domain or community-wide technological issues. The standards championed are typically industry interface standards for hardware or software, and are not specifically designated as MOSA.

10.6.4.2 MOSA systems dependencies and interdependencies.System interoperability has long been an issue for realizing new, complex military capabilities and one that lends itself to MOSA implementations. Interoperability as a general practice is achieved by recognizing where intersystem dependencies exist, negotiating standards between systems or groups of systems as necessary to achieve that interoperability, and then testing and fielding the relevant system implementations to the field. Sharing a set of MOSA's best practices to support the DoD business model of enabling military interoperability as those practices permeate both Government and industry engineering activities is imperative.

10.6.4.3 DM access. Unintended consequences arise from a lack of understanding related dependencies and interdependencies and their associated shared CM impacts. Challenges arise from not monitoring interdependent programs and mitigating CM and DM risks associated with interacting individual systems, the system of systems, and other constituent systems relying on shared data sources.

Related CM and DM activities to ensure access to standards and rights include the following:

a. Obtaining and securing available standards.

b. Gaining access to data regarding standards.

c. Managing appropriate standards documentation and maintain the necessary licenses.

d. Securing and managing the appropriate data rights.

e. Obtaining the appropriate access to storage, maintenance, control, use and exchange of data.

11. NOTES

11.1 Intended use. This military handbook provides guidance and information to DoD acquisition managers, logistics managers, and other individuals who are assigned responsibility for CM. Its purpose is to assist them in planning for and implementing effective DoD CM activities and practices during all life cycle phases of defense systems and CIs. It supports acquisition based on performance specifications and the use of industry standards and methods to the greatest practicable extent. This handbook has been revised to remove duplication of the industry handbook SAE-GEIA-HB0649. Throughout this document there are references to sections in the industry handbook where low level details may be found in the execution of CM.

11.2 Subject term (key word) listing.

Allocated baseline

Application activity

Computer software configuration item

Configuration baseline

Configuration control

Configuration control board

Configuration documentation

Configuration identification

Configuration item

Configuration management

Configuration status accounting

Current document change authority

Data management

Engineering change proposal

Engineering drawings

Functional baseline

Functional configuration audit

Physical configuration audit

Product baseline

Request for variance

Specifications

11.3 Changes from previous issue. Marginal notations are not used in this revision to identify changes with respect to the previous issue due to the extent of the changes.

CONFIGURATION MANAGEMENT DOCUMENTATION

A.1 SCOPE

A.1.1 Scope. This appendix includes a listing of major configuration documentation and configuration management considerations for international acquisition and exportability.

TABLE A-1. Configuration management documents (not exhaustive).

	DoD	Industry	Other U.S. Govt	Intergovernmental
Policy	DoDD 5000.01 DoDI 5000.02	N/A	N/A	NATO STANAG 4427 1/, 2/ NATO ACMP-2000 1/
Standards	N/A	SAE EIA-649B 3/ SAE EIA-649-1 3/ IEEE 828 1/ IEEE 12207 1/ ISO/IEC 12207 1/	N/A	NATO STANAG 4427 1/, 2/ NATO ACMP-2100 1/
Guidance, Including Handbooks	DAG, Chapter 3 MIL-HDBK-61	GEIA-649HB 3/ ISO 10007 1/	NIST SP 800-128 1/	NATO STANAG 4427 1/, 2/ NATO ACMP-2009 1/

FOOTNOTES:

1/ Not extensively covered in MIL-HDBK-61.

2/ Strictly speaking, a Standard NATO Agreement (STANAG) is not a standard, but rather an agreement to use standards, and other documents, that are listed in body of STANAG.

3/ Adopted by DoD, but use not mandated in policy.

NOTE: Titles of documents in table are as follows:

Defense Acquisition Guidebook (DAG), Chapter 3, Systems Engineering

DoDD 5000.01, The Defense Acquisition System

DoDI 5000.02, Operation of the Defense Acquisition System

SAE EIA-649, Configuration Management Standard

SAE EIA-649-1, Configuration Management Requirements for Defense Contracts

GEIA-HB-649, Configuration Management Standard Implementation Guide

IEEE 828, Configuration Management in Systems and Software Engineering

ISO 10007, Quality Management – Guidelines for Configuration Management

ISO/IEC/IEEE 12207, Systems and Software Engineering – Software Life Cycle Processes

NATO ACMP-2000, Policy on Configuration Management

NATO ACMP-2100, The Core Set of Configuration Management Contractual Requirements

NATO ACMP-2009, Guidance on Configuration Management

NATO STANAG 4427, Configuration Management in System Life Cycle Management

NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems

A.1.2 Configuration management considerations for international acquisition and exportability. PMs should consider the potential demand and likelihood of cooperative development or production, direct commercial sales, or foreign military sales early in the acquisition planning process. When PMs consider it appropriate, the use of international or intergovernmental standards and guidance may be beneficial, especially for enhancing international cooperation and interoperability.

SAE EIA-649-1 TAILORING GUIDANCE

B.1 SCOPE

B.1.1 Scope. This appendix covers how acquisition is applied though all CM acquisition design phases.

B.2 GUIDANCE CRITERIA.

B.2.1 CM for DoD contracts. The purpose of figure B-1 is to provide guidance to the acquirer in selecting the appropriate configuration management activities during each lifecycle phase of a program. Specific tailoring will be accomplished utilizing EIA-649-1, Annex A – Tailoring Worksheet. For further EIA-649-1 tailoring assistance, please review GEIA-HB-649A.

Requirements	EIA 649-1 Paragraphs	MSA TMR	EMD	LRIP	FRP	Service Spares	DLA Spares	CLS/PBL
GENERAL	3	T	R	R	R	R	R	R
CMP	3.1	T	R	R	T	NR	T	T
CI	3.2	T	R	NR	NR	NR	T	T
SW	3.2(4),3.2.4.2	T	T	T	NR	NR	T	NR
CHG MGT	3.3	T	R	R	T	T	T	T
ECP	3.3.1,3.3.3,3.3.4	NR	R	R	R	R	R	R
RFV	3.3.2	NR	R	R	R	R	T	T
CSA	3.4	NR	R	R	T	T	R	T
AUDIT	3.5	NR	R	R	T	NR	T	NR
FCA	3.5.2	NR	T	NR	NR	NR	T	NR
PCA	3.5.3	NR	NR	T	T	NR	T	NR
		R-Recommended; T-Tailorable; NR- Not Recomended						

CMP - Configuration Management Plan
CI - Configuration Identification
SW - Software
CHG MGT - Change Management
ECP - Engineering Change Proposal
RFV - Request for Variance
CSA - Configuration Status Accounting
FCA - Functional Configuration Audit
PCA - Physical Configuration Audit

FIGURE B-1. Configuration management for DoD Contracts.

B.2.2 Tailoring guidance. EIA-649-1 is applicable only to the extent specified in the tasking directive or contract. The acquirer utilizing the tailoring worksheet (ANNEX A of EIA-649-1) will select the appropriate requirements for their specific program. The tailoring worksheet is provided as a tool to aid the acquirer in tailoring their CM requirements on their program contracts. The requirements listed are not intended to be placed on contract in their entirely, but rather help the acquirer conceptually with selecting the appropriate requirements needed. Factors that influence the tailoring include: the program's life cycle phase, contract type and structure, acquisition or procurement method, complexity, size, intended use, mission criticality, and logistics support requirements of the affected CI (hardware and software).

B.2.3 Copyright guidance. The EIA-649-1 principles listed in figure B-1 are copyright-protected by SAE International. Except as permitted under the applicable laws of the user's country, neither the EIA-649 principles nor any extract may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, photocopying, recording. or otherwise) without prior written permission being secured; they are intended to be for reference only. However, EIA-649-1, Annex A – Tailoring Worksheet may be used and quoted in contracts.

B.2.4 Statement of work guidance. When developing their contract statement of work requirements, the acquirer will formulate their own "shall statements" or tailor the existing "shall statements" identified within EIA-649-1 that best summarize their CM requirements. Failure to tailor the EIA-649-1 "shall statements" requirements will drive unnecessary requirements and cost to the program.

B.2.5 Life cycle applicability guidance. Figure B-1 is a quick reference that allows the acquirer to review CM requirements that are Recommended (R), Tailorable (T), or Non-Applicable (NA) for each program's lifecycle phase. For example, a supplier's general CM requirements would be tailorable during a program's Material Solution and Technology lifecycle phase; however, during the EMD and low-rate initial production (LRIP) lifecycles, the CM requirements would be required. Whether it's tailored or required, planning for the CM requirements are very important. Tailoring the application of those CM requirements is very important. GEIA-HB-649A, Table 3 - Tailoring considerations provides examples of CM processes and resource tailoring considerations. Care should be exercised to ensure that the tailored CM practices are appropriate for the complexity of the product.

B.3 CM REQUIREMENTS.

B.3.1 CM lifecycle requirements. Once the life-cycle phase has been determined, begin reviewing the requirements (i.e., "shall" statements) in SAE EIA-649-1. Ensure that only the statements that are required or desired for this phase are selected, as these statements are requirements and drive cost. Figure B-1 shows the high-level process for selecting the correct tailoring requirements for the phase of program being executed.

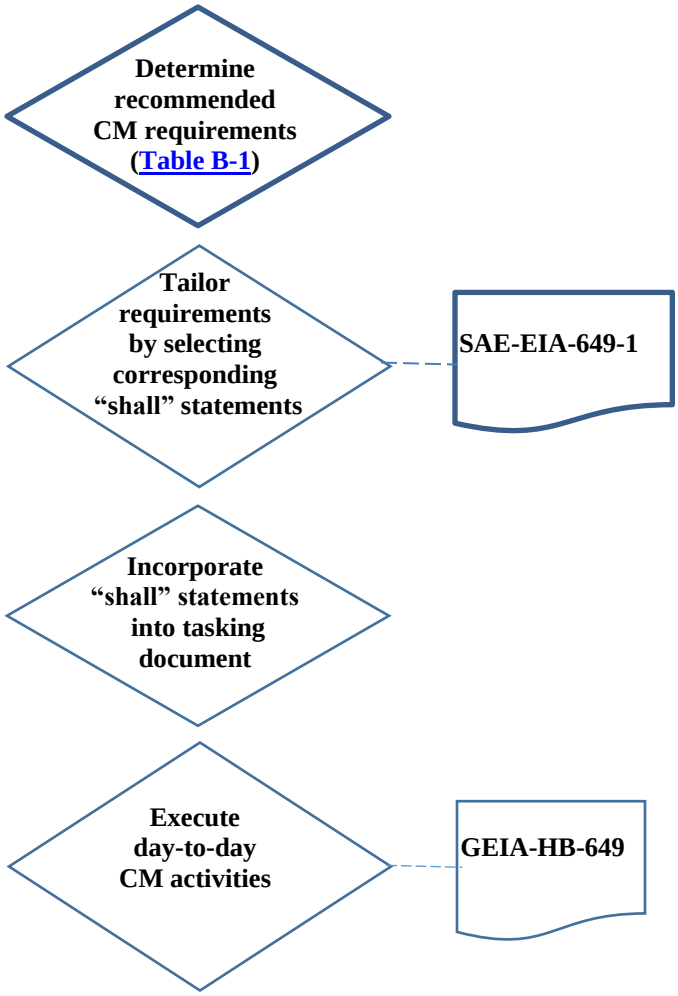

FIGURE B-2. CM lifecycle requirements flow chart.

B.3.2 CM requirements selection process. Utilizing table B-1 and figure B-2 will allow for optimized CM requirements that provide the information and process application to ensure configuration management is properly applied.

CM TEMPLATES

C.1 SCOPE

C.1.1 Scope. This appendix consists of a series of templates, one for each life cycle phase, that collectively provide a road map for the CM process. Figures C-1 through C-4 portray CM objectives, typical metrics, activities, actions, benefits, and risks. Because material solutions analysis occurs prior to Milestone A in accordance with DOD Instruction 5000.2, CM activities are not applicable during this phase.

<table>
<tr><th colspan="2">CM Objectives</th></tr>
<tr><td colspan="2"><u>Government</u>
♦Access to current versions of study reports
♦Defined acquisition strategy and Government CM plan
<u>Government and Contractor</u>
♦Define alternative performance requirements with comparable associated life cycle cost, interoperability, and risk assessment data
♦Access to associated current versions of risk reduction studies and test reports
♦Clear coordinated plans for the system acquisition phases
<u>Contractor(s)</u>
Defined CM process for system acquisition phases</td></tr>
<tr><th colspan="2">ACTIVITY: Planning</th></tr>
<tr><th>Actions</th><th>Benefits/Risks</th></tr>
<tr><td><u>Government</u>
♦Develop concept of operation and acquisition strategy for CM in system acquisition
♦Prepare, coordinate, and release procedures implementing the Government CM process; conduct training (See Government activities below)
♦Measure/evaluate contractor CM process
<u>Government and Contractor</u>
♦Prepare and coordinate configuration management plans
♦Define data interface and requirements
♦Document lessons learned
<u>Contractor</u>
♦Prepare, coordinate, and release procedures to implement contractor CM support of systems engineering; conduct training (See activities below)
♦Develop CM requirements, information and data, and metrics to be negotiated with potential subcontractors</td><td>♦Benefit:
– The appropriate level of resources and the right information to efficiently and effectively conduct CM
♦Risks if not done:
– Incompatible Government and contractor CM systems
– Inadequate or excessive resources
– Inability to perform effectively due to lack of timely information</td></tr>
</table>

FIGURE C-1. TMRR phase.

ACTIVITY: Configuration Identification	
Actions	**Benefits/Risks**
Government • Implement identification method and review process to review concept exploration studies and draft RFP material **Government and Contractor** ♦Participate in program management and systems engineering IPTs **Contractor** ♦Maintain a defined document identification and release process for systems engineering products such as concept study and associated reference documentation ♦Establish audit trail of decisions and document iterations	♦**Benefits:** – Efficient management of information – Access to correct, current data – Effective information-sharing among IPTs and between Government and contractor ♦**Risks if not done:** – Lack of an audit trail of decisions – Incorrect revisions used – IPTs may not be working to a common reference
ACTIVITY: Configuration Control	
Actions	**Benefits/Risks**
Government and Contractor ♦Establish process for version control of concept study data files and document representations ♦Implement common process to review and coordinate iterations of concept evaluation data	♦**Benefit:** – Efficient review – Assurance that all functional groups or IPTs are working to a common reference ♦**Risk if not done**: – Inconsistent or unreliable analyses, reports, and conclusions
ACTIVITY: Configuration Status Accounting	
Actions	**Benefits/Risks**
Government and Contractor ♦Record and report status of management and technical decisions including designation of individual IPTs responsible for their implementation ♦Provide traceability of all decisions to revisions in concept study documents and requirements documentation ♦Record unique identifiers for the digital data files and document representations of each document and each hardware model or software package released for use on the program	♦**Benefits:** – Single information source – Always current reference – Common basis for decision – Access for all with a need-to-know ♦**Risks if not done**: – Lack of decision audit trail – Redundant document storage – Decisions based on obsolete data
ACTIVITY: Configuration Audits	
Configuration Audits are not applicable in this phase	

FIGURE C-1. TMRR phase – Continued.

ACTIVITY: Management and Planning	
Actions	**Benefits/Risks**
Government ♦ Develop concept of operation and acquisition strategy CM ♦ Prepare, coordinate, and release procedures implementing the Government CM process; conduct training. (See Govt. configuration identification, control, and status accounting activities below.) ♦ Measure and evaluate contractor CM process **Government and Contractor** ♦ Jointly participate in program management and systems engineering IPTs ♦ Prepare and coordinate configuration management plans ♦ Define digital data interface and data requirements ♦ Effect process improvements and document lessons learned during EMD and system demonstrations **Contractor** ♦ Prepare, coordinate, and release procedures to implement the contractor CM process; conduct necessary training. (See contractor configuration identification, control, and status accounting activities below.) ♦ Finalize subcontractor CM requirements including information, data, and metrics	♦ **Benefit:** – The appropriate level of resources and the right information to efficiently and effectively conduct CM ♦ **Risks if not done:** – Incompatible Government and contractor CM systems – Inadequate or excessive resources – Inability to perform effectively for lack of timely information – Loss of configuration control – Poor supportability – Excessive configuration documentation ordered that is not necessary for program management or sustainment
ACTIVITY: Configuration Identification	
Actions	**Benefits/Risks**
Government ♦ Establish interface memoranda of understanding with associated Government programs and commands, as applicable ♦ Implement identification method and release process for Government requirements and directive documentation ♦ Approve system specification establishing FBL ♦ Concur with contractor specification types ♦ Approve top-level and lower-level CI performance specifications for which the Government has configuration approval authority, establishing an (Government) ABL for each CI ♦ For CIs for which Government is configuration approval authority at detail design level, establish (Government) Product Baseline (after CI performance verification and documentation/product consistency) ♦ Assign nomenclature, where appropriate ♦ Assign representatives and establish and operate interface management boards or other mechanisms to coordinate contractual and technical interface issues among related service components and commands ♦ Participate in contractor ICWG activity	♦ **Benefits:** – Known structure (hierarchy) of system/CI to which configuration documentation and other information is related – Performance, interface and other attributes are clearly documented – Items are identified and marked appropriately – Effective information-sharing and coordination among various IPTs and between Government and contractor – Identification of product and documentation is modified as significant changes are incorporated – Release of configuration documents is control-led, and configuration baselines are established and maintained – Configuration documentation, user, and maintenance information correlates to product versions

FIGURE C-2. EMD phase.

ACTIVITY: Configuration Identification – Continued	
Actions	**Benefits/Risks**
Government and Contractor ♦Internally control requirements for alternative solutions through a defined document release and control process ♦Establish requirements traceability from top-level to allocated requirements definitions ♦Prepare, review, and provide system and top-level CI performance specifications to the Government ♦Capture configuration definitions of simulation software, prototypes, and engineering models through release and control of configuration documents ♦Establish interface agreements and ICWGs for interface management. ♦Determine configuration approval authority for configuration documentation for each CI based on maintenance and support plans and CM plans **Contractor** ♦Define product structure identifying CIs and configuration documentation ♦Assign CI identifiers and nomenclature ♦Determine type of specification(s) for each CI (see criteria for types and order of precedence) ♦Assign specification identifiers ♦Define interfaces using ICWGs/ICDs as applicable ♦Prepare and coordinate CI specifications and obtain approval by all affected functional organizations and teams ♦Approve CI performance or detail specification for each CI for which the contractor has configuration approval authority, establishing a (contractor) ABL ♦Assign part, item, and software identifiers ♦Define traceable items and prescribe method of tracking identification (serial or lot control) ♦Release engineering design data (engineering drawings, computer models, software design documents) ♦Maintain design release baseline (also referred to as developmental configuration and release record) and baseline for each software version ♦For CIs for which the contractor is the configuration approval authority at the detail design level, establish (contractor) PBL (after verifying CI performance and CI documentation/product consistency)	♦**Risks if not done:** – Poor correlation between requirements documents and test results – Incorrect revisions used – IPTs not working to a common reference – Inaccurate, incomplete interface data – Inability to assess requirements iterations on interfaces – Incomplete documentation – Inadequate or incorrect product identification and marking – Inconsistency between product and documentation – Inability to validate performance and interface attributes – Inability to distinguish between product versions – Inadequate basis for defining changes and corrective actions – Configuration control authorities not established or defined inappropriately – Uncertain configuration control decisions – Inability to provide efficient product support after production and deployment

FIGURE C-2. EMD phase – Continued.

ACTIVITY: Configuration Control	
Actions	**Benefits/Risks**
Government ♦ Establish Government configuration control process and procedures for development and demonstration, including change initiation, evaluation, and disposition ♦ Establish CCB using CCB charter, assign membership, provide operating procedures ♦ Evaluate contractor configuration control process ♦ When necessary or beneficial to the Government, initiate requests for Class I ECPs to FBL configuration documentation and ABL configuration documentation for which the Government is the configuration approval authority ♦ Determine desired change effectivity ♦ Coordinate, evaluate, and disposition contractor's Class I ECPs and NORs, as applicable ♦ Direct contractual implementation of approved ECPs, in accordance with the approved effectivity, into configuration documentation, system, CIs, and all supporting commodities and services that are affected by the ECP ♦ Review and approve or disapprove contractor RFVs from Government approved configuration documents **Government and Contractor** ♦ Communicate on status and content of changes and RFVs planned and in process **Contractor** ♦ Establish contractor configuration control process and procedures including CCB, change identification, change evaluation and coordination, and approved change implementation and verification ♦ Evaluate subcontractor configuration control process ♦ Process proposed changes to approved baseline configuration documentation: – Identify, classify, and document change – Evaluate and coordinate change – Assess change impact – Determine proposed effectivity, schedule, and cost – For proposed changes to the FBL, submit Class I ECPs with attached NORs, if applicable – For proposed changes to an ABL • Where the Government is the configuration approval authority, submit Class I ECPs with attached NORs, if applicable • Where the contractor is the configuration approval authority, obtain a change approval decision from the appropriate organizational level with authority to commit resources to implement the change ♦ For design changes to developmental configuration, assess the change as part of the release process to assure that FBLs or ABLs are not impacted ♦ Plan change implementation ♦ Implement change and verify re-established consistency of product, documentation operation, and maintenance resources ♦ If necessary to depart temporarily from Government-approved configuration documents, process and submit RFVs, as required	♦ **Benefits:** – Efficient change processing and orderly communication of change information – Change decisions based on knowledge of change impact – Changes limited to those necessary or beneficial – Evaluation of cost, savings, and tradeoffs facilitated – Consistency between product and documentation – Configuration control preserved at system interfaces – Current baselines enable supportability – Variances are documented and limited ♦ **Risks if not done:** – Chaotic, ad-hoc change management – Changes approved without knowledge of significant impacts – Changes that are not necessary or offer no benefit – Lack of confidence in cost and schedule estimates – No assurance of product to document consistency – Uncertainty at system interfaces – Inconsistent basis for supportability – No control of variances – Ineffective program management – Lack of confidence in both Government and contractor processes – Essentially, technical anarchy

FIGURE C-2. EMD phase – Continued.

ACTIVITY: Configuration Control – Continued	
Actions	
<u>Contractor</u> – Continued • Classify as major or minor • Document and submit to the configuration control process • Obtain approval decision from the appropriate authority: – The Government if it is a major variance from a Government approved configuration document (i.e., performance or detail specifications) – DCMA (or other contractually designated authority) if it is a minor variance from a Government-approved configuration document – The appropriate contractor internal authority if the variance is from contractor baselined configuration documentation	

ACTIVITY: Configuration Status Accounting	
Actions	**Benefits/Risks**
<u>Government</u> ♦Select and tailor information to be provided by the contractor ♦Establish procedures and screens for interacting with a Government CM AIS ♦Test and assure the integrity of the configuration information in the Government database(s); verify that CM business rules have been correctly applied ♦Evaluate contractor CSA process **<u>Government and Contractor</u>** ♦Record and report the current performance requirement documentation ♦Correlate definition of simulation software, prototype, or engineering model configurations to applicable test results, analyses, and trade studies ♦Record and report status of proposed requirement changes including the status of incorporation into the work scope of individual IPTs ♦Record all authorized changes to requirements documentation ♦Provide traceability of requirements from the top-level documentation through all subordinate levels ♦Provide controlled access to the digital data files and document representations of each document and software item released for use on the program ♦Identify the current approved configuration documentation and configuration identifiers associated with each system or CI(s). ♦Identify the digital data file(s) and document representations of all revisions or versions of each document and software delivered or made accessible electronically in support of the contract. ♦Record and report the results of configuration audits, including the status and final disposition of identified discrepancies and action items ♦Record and report the status of proposed engineering changes from initiation to final approval to contractual implementation ♦Record and report the status of all critical and major RFVs that affect the configuration of a system or CI(s).	♦**Benefits:** – Single information source providing consistency – Always current reference – Common basis for change decisions – Access for all with a need-to-know – Correct, timely configuration information, when needed to facilitate decision making on changes, deployment of assets, determining applicable replacements, and performing updates or upgrades. ♦**Risks if not done:** – Redundant document storage and retrieval – Costly searches for information and status – Improper decisions made based on obsolete data. – The risk of inadequate status accounting may result in improper decisions about change effectivity, retrofit requirements, and deployment of items requiring support assets that are not in place, all of which contribute to avoidable cost.

FIGURE C-2. <u>EMD phase</u> – Continued.

ACTIVITY: Configuration Status Accounting – Continued	
Actions	
Contractor ♦Capture and report information about: – Product configuration status – Configuration documentation – Current baselines – Historic baselines – Change requests – Change proposals – Change notices – Variances – Warranty data and history – Replacements by maintenance action – Configuration verification and audit status and action item close-out ♦Report the effectivity and installation status of configuration changes to all systems or CI(s) ♦Provide traceability of all changes from the original released configuration documentation of each system or CI(s) ♦Record and report implementation status of authorized changes Evaluate sub-contractor CSA process	
ACTIVITY: Configuration Audits	
Actions	**Benefits/Risks**
Government ♦Establish interface memoranda of understanding with associated Government programs and commands, as applicable ♦Assign audit co-chair for each audit ♦Approve audit agenda(s) ♦Approve minutes ♦Certify that contractors' processes for engineering release, configuration control, and status accounting will maintain baseline control **Government and Contractor** ♦Perform audit planning and pre-audit preparation ♦Conduct formal audit when required ♦Review performance requirements, test plans, results, and other evidence to determine whether the product performs as specified, warranted, and advertised ♦Perform physical inspection of product and design information; ensure accuracy, consistency, and conformance with acceptable practice ♦Record discrepancies; review to close out or determine action; record action items ♦Track action items to closure via status accounting **Contractor** ♦Verify product within normal course of process flow ♦Ensure consistency of release information and production/modification information ♦Assign audit co-chair ♦Prepare audit agendas ♦Prepare audit minutes	♦**Benefit:** – Known structure (hierarchy) of system or CI to which configuration documentation and other information are related ♦**Benefit:** – Verified configuration and documentation consistent with operational and support requirements – Reliable and dependable baselines ♦**Risks if not done:** – Unnecessary and avoidable support costs – Inaccurate technical manuals – Replacement parts that do not fit – Loss of confidence in supplier

FIGURE C-2. EMD phase – Continued.

ACTIVITY: Management and Planning	
Actions	**Benefits/Risks**
Government ♦Prepare, coordinate, and release procedures implementing the Government CM process; conduct training. (See Government configuration identification, control, status accounting, and audit activities below.) ♦ Measure and evaluate the contractor CM process **Government and Contractor** ♦Update CM planning, as required, to reflect process improvements, new deployment information, changes in support or maintenance planning, major modifications, etc. ♦Plan for end of production, sustainment, demilitarization, and disposal **Contractor** ♦Prepare, coordinate, and release procedures to implement the contractor CM process and conduct necessary training. (See contractor configuration identification, control, status accounting, and audit activities below.) ♦Measure and evaluate sub-contractor CM process	♦**Benefit:** – Appropriate level of resources and the right information to efficiently and effectively conduct CM ♦**Risks if not done:** – Inadequate resources to accomplish essential tasks late in program – Poor supportability at a time of aging assets
ACTIVITY: Configuration Identification	
Actions	**Benefits/Risks**
Government ♦Perform basic configuration identification actions for documentation, hardware, and software created or revised as a result of approved engineering changes ♦Where the Government is the design activity, authorize release of documents and document revisions ♦Maintain current FBL and Government ABLs ♦For CIs for which Government is configuration approval authority at the detail design level, maintain a (Government) PBL ♦Assign Government nomenclature, where appropriate **Government and Contractor** ♦If maintenance plan is affected by a change, ensure that level of performance specification for the new configuration remains consistent with revised maintenance planning **Contractor** ♦ Perform basic configuration identification actions for documentation, hardware and software created or revised as a result of approved engineering changes, i.e.: • Assign CI, document, part or item, and software identifiers • Revise interfaces using ICWGs and ICDs, as applicable • Prepare and coordinate CI specification revisions • Approve CI performance or detail specification revision for CIs for which contractor has configuration approval authority, establishing a new current (contractor) ABL • Track traceable items via serial number or lot number • Release engineering design data (engineering drawings, computer models, software design documents) • Maintain design release (release record) • For CIs for which the contractor is configuration approval authority for detail design, maintain (contractor) PBL	♦**Benefits:** – Performance, interface, and other attributes are clearly documented and used as basis for configuration control – Items are appropriately identified and marked – Re-identification occurs as significant changes are incorporated – Release controls and configuration baselines are maintained – Users and maintenance personnel can locate information correlated to correct product versions ♦**Risks if not done:** – Inability to provide efficient product support after production and deployment – Inadequate or incorrect product identification and marking, resulting in incorrect replacement parts – Inability to distinguish between product versions, resulting in deployment of assets requiring excessive support capability and assets without the functional capability needed for assigned missions – Inadequate basis for defining changes and corrective actions – Uncertain, wasteful, and costly configuration control decisions

FIGURE C-3. Production and deployment phase.

ACTIVITY: Configuration Control	
Actions	**Benefits/Risks**
Government ♦ Establish Government configuration control procedures, including change initiation and CCB operating procedures for change evaluation and disposition ♦ Evaluate contractor configuration control process ♦ Identify need for changes requested by Government activities and when necessary or beneficial to the Government; initiate requests for Class I ECPs; determine desired effectivity of requested change ♦ Coordinate, evaluate, and disposition contractor's Class I ECPs with attached NORs, as applicable ♦ Direct contractual implementation of approved ECPs, in accordance with the approved effectivity, into configuration documentation, system, CIs, and all supporting commodities and services that are affected by the ECP ♦ Review and approve or disapprove contractor RFVs from Government approved configuration documents ♦ Document local engineering changes and ensure that they do not impact current baselines, prior to approving their implementation. Request contractor review when necessary **Government and Contractor** ♦ Communicate on status and content of changes and RFVs, contemplated and in process **Contractor** ♦ Establish contractor configuration control process and procedures, including change identification, change evaluation and coordination, and approved change implementation and verification ♦ Evaluate subcontractor configuration control process ♦ Process proposed changes to approved baseline configuration documentation: • Identify, classify, and document change • Evaluate and coordinate change • Assess change impact • Determine proposed effectivity, schedule, and cost • For proposed changes to the FBL, submit Class I ECPs • For proposed changes to an ABL or PBL: – Where the Government is the configuration approval authority, submit Class I ECPs with attached NORs, if applicable – Where the contractor is the configuration approval authority, obtain a change approval decision from the appropriate organizational level with authority to commit resources to implement the change ♦ Plan change implementation ♦ Implement change and verify re-established consistency of product, documentation, operation, and maintenance resources ♦ If necessary to depart temporarily from Government-approved configuration documents, process and submit RFVs as required	♦ **Benefits:** – Efficient change processing and orderly communication of change information – Change decisions based on knowledge of change impact – Changes limited to those necessary or beneficial – Evaluation of cost, savings, and tradeoffs facilitated – Consistency between product and documentation – Configuration control preserved at system interfaces – Current baselines enable supportability – Variances are documented and limited ♦ **Risks if not done:** – Chaotic, ad-hoc change management – Changes approved without knowledge of significant impacts – Changes that are not necessary or offer no benefit – Lack of confidence in accurate cost and schedule estimates – No assurance of product to document consistency – Uncertainty at system interfaces – Inconsistent basis for supportability – No control of variances – Ineffective program management – Lack of confidence in both Government and contractor processes – Essentially, technical anarchy

FIGURE C-3. Production and deployment phase – Continued.

ACTIVITY: Configuration Control -- Continued	
Actions	
Contractor – Continued: • Classify as major or minor • Document and submit to the configuration control process • Obtain approval decision from the appropriate authority – The Government if it is a major variance to a Government-approved configuration document – The DCMA (or other contractually designated authority) if it is a minor variance to a Government-approved configuration document – The appropriate contractor internal authority if the variance is to contractor-baselined configuration documentation	
ACTIVITY: Configuration Status Accounting	
Actions	**Benefits/Risks**
Government ♦Establish procedures for interacting with the Government database(s) ♦Test the integrity of the configuration information in the Government database(s); verify that CM business rules have been correctly applied ♦Evaluate contractor CSA process **Government and Contractor.** ♦Identify the current approved configuration documentation and configuration identifiers associated with each system or CI(s). ♦Identify data file(s) and document representations of revisions or versions of each document or software delivered or made accessible electronically ♦Record and report the results of configuration audits, including the status and final disposition of identified discrepancies and action items ♦Record and report the status of proposed engineering changes from initiation to final approval to contractual implementation ♦Record and report the status of all critical and major RFVs that affect the configuration of a system or CI(s). ♦Report the effectivity and installation status of configuration changes to all system or CI(s) ♦Provide the traceability of all changes from the original released configuration documentation of each system or CI(s) ♦Record and report configuration changes resulting from retrofit and by replacements through maintenance action ♦Retain information about: – Product configuration status – Configuration documentation – Current baselines – Historic baselines – Change requests – Change proposals – Change notices – Variances – Warranty data and history – Configuration verification and audit status/action item close-out **Contractor** ♦Evaluate sub-contractor CSA process	♦**Benefit:** – Correct, timely configuration information when needed to facilitate decision making on changes, deployment of assets, determining applicable replacements, performing updates/upgrades. ♦**Risk if not done** – Inadequate status accounting may result in improper decisions about change effectivity, retrofit requirements, deployment of items requiring support assets that are not in place; all of which contribute to avoidable cost.

FIGURE C-3. Production and deployment phase – Continued.

ACTIVITY: Configuration Audit	
Actions	**Benefits/Risks**
Government ♦ Assign audit co-chair for each audit ♦ Approve audit agenda(s) ♦ Approve minutes ♦ Certify that contractors' processes for engineering release, configuration control, and status accounting will maintain baseline control **Government and Contractor** ♦ Conduct formal audit when required ♦ Review performance requirements, test plans, results, and other evidence to determine whether product performs as specified, warranted, and advertised ♦ Perform physical inspection of product and design information; ensure accuracy, consistency, and conformance with acceptable practice ♦ Record discrepancies; review to close out or determine action; record action items ♦ Track action items to closure via status accounting **Contractor** ♦ Verify product within normal course of process flow ♦ Ensure consistency of release information and production or modification information ♦ Assign audit co-chair ♦ Prepare audit agendas ♦ Prepare audit minutes	♦ **Benefits:** – Verified configuration and documentation consistent with operational and support requirements – Reliable and dependable baselines ♦ **Risks if not done:** – Unnecessary and avoidable support costs – Inaccurate technical manuals – Replacement parts that do not fit – Loss of confidence in supplier

FIGURE C-3. Production and deployment phase – Continued.

<table>
<tr><th colspan="2">CM Objectives</th></tr>
<tr><td colspan="2"><u>Government</u>
♦Known configuration of all CIs in operational inventory (down to lowest organically replaceable parts)
♦Present and planned allocation of CI assets by serial number to operational sites, squadrons, wings, corps, etc.
♦Access to operation and maintenance information for the current configuration (down to the lowest organically replaceable parts) of each deployed CI or CSCI version; knowledge as to approved ECPs incorporated
♦Reference to correct configuration of support assets (support equipment, test program sets, trainers, and associated software) required for each operational configuration of each CI to the extent that it is organically supported
♦Ability to determine the current mission capability of each CI serial number reflected by installed software version, ECP (and modification kit) incorporation, and local insertion of mission data
♦Known configuration, (quantities and location) of spare and replacement parts for current configuration, and mod kits to upgrade to new (baseline) configuration
♦Access to design disclosure data for spare parts to be re-procured to detailed design rather than performance data

<u>Government and Contractor</u>
♦Efficient, timely processing of ECPs and RFVs
♦Approved Class I ECP implementing actions scheduled and completed
♦
<u>Contractor</u>
♦Verified validated retrofit kit deliveries to satisfy retrofit effectivity
Reference to the correct configuration of support assets (support equipment, test program sets, trainers, manuals, and associated software) needed to maintain each operational configuration of each CI that is contractor-supported</td></tr>
<tr><th colspan="2">ACTIVITY: Management and Planning</th></tr>
<tr><th>Actions</th><th>Benefits/Risks</th></tr>
<tr><td><u>Government</u>
♦Continue procedures implementing Government CM process
<u>Government and Contractor</u>
♦Update CM Planning, as required, to reflect new deployment information, changes in support and maintenance planning, major modifications, etc.
♦Plan for demilitarization and disposal</td><td>♦Benefit:
– Appropriate level of resources and the right information to efficiently and effectively conduct CM
♦Risks if not done:
– Inadequate resources to accomplish essential tasks late in program
– Poor supportability at a time of aging assets</td></tr>
</table>

FIGURE C-4. Operations and support phase.

ACTIVITY: Configuration Identification	
Actions	**Benefits/Risks**
Government and Contractor ♦ Perform basic configuration identification actions for documentation, hardware, and software created or revised as a result of approved engineering changes ♦ If maintenance plan is affected by a change, ensure that level of performance specification for the new configuration remains consistent with revised maintenance planning ♦ Track traceable items via serial number or lot number	♦ **Benefits:** – Re-identification occurs as significant changes are incorporated – Users and maintenance personnel can locate correct information for product versions ♦ **Risk if not done:** – Inability to distinguish between product versions, resulting in deployment of assets with incorrect or excessive support assets, or without the functional capability needed for assigned missions
ACTIVITY: Configuration Control	
Actions	**Benefits/Risks**
Government and Contractor ♦ Continue configuration control procedures including change initiation and CCB operating procedures for change evaluation and disposition ♦ Document local engineering changes and ensure that they do not impact current baselines, prior to approving their implementation. Request contractor review when necessary ♦ Communicate on status and content of changes and RFVs contemplated and in process ♦ Process proposed changes to approved baseline configuration documentation ♦ Implement change and verify re-established consistency of product, documentation, operation and maintenance resources	♦ **Benefits:** – Consistency between product and documentation – Current baselines enable supportability ♦ **Risks if not done:** – No assurance of product to document consistency – Inconsistent basis for supportability
ACTIVITY: Configuration Status Accounting	
Actions	**Benefits/Risks**
Government/Contractor (based on contractual division of responsibility) ♦ Establish procedures for interacting with the Government database(s) ♦ Test the integrity of the configuration information in the Government database(s); verify that CM business rules have been correctly applied ♦ Record and report configuration changes resulting from retrofit and by replacements through maintenance action	♦ **Benefit:** – Correct, timely information for decision-making on changes, deployment of assets, applicable replacements, performing updates/upgrades ♦ **Risk if not done** – Improper decisions about change effectivity, retrofit requirements, and deployment of items requiring support assets that are not in place, all of which contribute to avoidable cost
ACTIVITY: Configuration Audit	
Actions	**Benefits/Risks**
Formal configuration audit activity is generally not applicable in the Operations and Support phase.	

FIGURE C-4. Operations and support phase – Continued.

CONCLUDING MATERIAL

Custodians:
- Army – AR
- Navy – NM
- Air Force – 11
- OSD – SE

Review activity:
- DLA – CC

Preparing activity:
- Navy – NM

(Project SESS-2020-012)

NOTE: The activities listed above were interested in this document as of the date of this document. Since organizations and responsibilities can change, you should verify the currency of the information above using the ASSIST Online database at https://assist.dla.mil.