BY ORDER OF THE COMMANDER
SPACE & MISSILE SYSTEMS CENTER

SPACE AND MISSILE SYSTEMS
CENTER INSTRUCTION 62-109

24 MAY 2017

Developmental Engineering

SMC CONFIGURATION MANAGEMENT (CM) PROCESS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-publishing website at **www.e-Publishing.af.mil** for downloading or ordering

RELEASABILITY: There are no restrictions on this publication

OPR: SMC/EN

Certified by: SMC/EN
(SES Thomas A. Fitzgerald)

Supersedes: SMCI 62-109, 23 May 2015

Pages: 53

This SMC Instruction (SMCI) implements Configuration Management (CM) requirements in Department of Defense Instruction (DoDI) 5000.02 *Operation of the Defense Acquisition System*, Air Force Instruction (AFI) 63-101/20-101 *Integrated Life Cycle Management*. This document uses the term "Program Manager" (PM) throughout for consistency with Department of Defense Directive (DoDD) 5000.01 although Air Force organizations, including SMC, may use "System Program Manager" (SPM) or "System Program Director" (SPD) as an equivalent. SMC Program Directorates may have several program offices with Program Managers and/or Program Directors. For the purposes of this SMCI, the abbreviation "PM" will be used for all Program Manager responsibilities, regardless of the duty title. *(**Note:** Rigorous CM, together with PM, contributes to system security by identifying and controlling all changes to the system requirements and the system throughout the lifecycle, ensuring that all changes and the identity of who made and authorized the changes are reviewed, recorded and controlled.)*

Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Air Force Information Management Tool (AF IMT) 847, Recommendation for *Change of Publication*; route AF IMT 847s from the field through the appropriate chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule.

SUMMARY OF CHANGES

This Revision 1 incorporates SMC Enterprise Systems Integration, SMC Center Commander (SMC/CC) Memo, 02 February 2016, located at: **https://insidesmc.losangeles.af.mil/u?q=3Ck**. It also updates references, and incorporates several administrative changes.

Chapter 1

CONFIGURATION MANAGEMENT OVERVIEW

1.1. Introduction. Configuration Management (CM) is a discipline to evaluate and control changes to the program technical baseline and all associated program baselines (e.g., contracts, Concept of Operations (CONOPS), budget, schedule, test, etc.), and their documentation throughout a product's life cycle. CM establishes program baselines and evaluates cost, risk, schedule, technical, and full impacts of potential changes prior to approval decision. The purpose of the CM process is to establish and maintain the integrity of all identified outputs of a project or process and make them available to stakeholders (Reference: *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) 15288). In accordance with (IAW) AFI 63-101/20-101, Integrated Life Cycle Management, para. 5.2.1.6, the PM must implement CM to establish and maintain consistency of program baselines throughout the life cycle to assure Operational Safety, Suitability, and Effectiveness (OSS&E). The primary CM industry standard adopted by the DoD is American National Standards Institute/Electronic Industries Alliance (ANSI/EIA)-649-1, *Configuration Management Requirements For Defense Contracts*. EIA 649-1 must be applied to SMC programs in conjunction with SMC Tailoring Standard SMC-T-007, SMC Tailoring of EIA-649-1: *Definition of Major (Class I) Engineering Change Proposal (ECP).* Refer to Military Handbook 61A (MIL-HDBK-61A), *Configuration Management Guidance,* for tutorial information about CM implementation.

1.2. Purpose. This instruction provides direction and references to establish a standardized, effective government CM process. This instruction mandates selected best practices from DoD, AF, and commercial CM standards to maintain consistency and synchronization between product configuration information/documentation and the physical product throughout its life cycle. This instruction describes government roles and responsibilities and serves as a complement to CM standards that specify CM standards to SMC contractors. These include SMC Standard SMC-S-002, Configuration Management, for legacy contracts. EIA-649-1 with SMC-T-007 must be used for placing tailored CM requirements on new SMC contracts.

1.3. Scope. This SMCI applies to all programs in the Air Force Program Executive Officer for Space (AFPEO/SP) portfolio at all SMC and AF locations, and to all acquisition programs executed at SMC or its Geographically Separate Units (GSUs) throughout the program system life cycle. CM must be applied to all SMC Acquisition Category (ACAT) programs (i.e. on the Acquisition Master List (AML)) and any programs or projects designated by the AFPEO/SP. Refer to AFI 63-101/20-101 for ACAT definitions. All SMC ACAT programs must be compliant with SMCI 62-109 and EIA 649-1 with SMC-T-007, and an appropriate level of CM must be applied to all SMC projects, tests, and demonstrations. At a minimum, CM must be applied to all defense program material designated as "systems" and "configuration items", including hardware, firmware, and software. *(**Note**: Direction for CM of technical Data Management (DM), technical baseline management, and Deficiency Reporting (DR) are within the scope of this instruction in the context of their relationship to CM; however, this SMCI does not provide comprehensive instruction on all DM and DR processes.)*

Chapter 2

CONFIGURATION MANAGEMENT ROLES AND RESPONSIBILITES

2.1. Government CM Roles and Responsibilities. The Government is the final CM approval authority for the systems and equipment it acquires and operates, although contractors may exercise a significant degree of authority for CM and control during any or all phases of the life cycle. This depends on such factors as type of acquisition, ownership of data, and contractual requirements. The Government must establish and control the product's functional requirements, performance requirements and has, at least, oversight and contract compliance responsibility during product development, fielding, operation, upgrade/modification, maintenance and disposal. The Government must define contractual CM terms and conditions for the contract(s) it issues through tailoring of EIA-649-1, and ensure that the contractor requires its suppliers to comply with or suitably tailor the same CM requirements that are being imposed upon the contractor. EIA-649-1 Annex A provides a Tailoring Matrix Worksheet.

2.2. SMC CM Roles and Responsibilities . Effective CM and control requires coordination across program organizational functions and levels. Table 2.1. lists mandatory CM responsibilities for key SMC Government personnel. *(**Note:** SMC program mission area Directorates may elect to define CM processes and consolidate CM issues at the Directorate level; however, program CM implementation, authority, and responsibility remain with the PM of Record, who may or may not be the Directorate Director. The SMC mission area Directorate Directors have a Center chain of command role, but have no mandated direct program CM role, other than to provide required resources to programs to support CM functions; the Directorate Director role is not included in Table 2.1. SMC CM Roles and Responsibilities.)* Additional specific Government Configuration or Change Control Board (CCB) Roles and Responsibilities are summarized in paragraph 3.4. *Configuration Change Management.*

Table 2.1. SMC CM Roles and Responsibilities.

SMC Role	SMC CM Responsibilities
2.1.1 AFPEO/SP	AFPEO/SP will arbitrate any cases where program technical baseline changes have cross directorate impacts, which cannot be resolved by directorate level CCBs.
2.1.2 AFPEO/SP Lead System Engineer (LSE)	The AFPEO/SP Lead System Engineer (LSE) (also known as the SMC Chief Systems Engineer) must: 2.1.2.1. Provide cross-program CM and CM standardization advice to the AFPEO/SP and SMC program offices.
2.1.3 Program Manager (PM)	The PM must: 2.1.3.1 Be the final approval authority for all CM activities, issues, changes, and documentation at the program level throughout the lifecycle to end of life,

2.1.3 Program Manager (PM)	including when there is shared responsibility with the Prime Contractor as defined in the contract. 2.1.3.2 Ensure that a program Configuration Management Plan (CMP) or equivalent program document captures the results of the CM planning activity, including all required CM functions, and delegation of CM authority, including which stakeholders control the allocated, functional, and product baselines. A program CM Operating Instruction (OI) may be used in place of a program CMP. 2.1.3.3 Be the Current Document Control Authority (CDCA) for top-level performance CM (specifications) and configuration control authority for the System/Configuration Item (CI) during its life as a Government asset. This applies to top-level CIs and any other CIs the Government will maintain control for, per the CMP and contract. 2.1.3.4 Execute the CMP to ensure that all functions and activities required, including reviews, audits, and baselines, are executed and documented as required in this instruction and Higher Headquarters (HHQ) regulatory documents. 2.1.3.5 Have final approval on all Engineering Change Proposals (ECPs) and Change Requests (CRs), including those initiated by Deficiency Reports (DR) actions, reviewed by the Materiel Improvement Project Review Board (MIPRB), entered into the Joint Deficiency Report System (JDRS), and reviewed by the CCB. 2.1.3.6 Establish or designate the program CCB to ensure all changes in CIs are assessed for cross-program impacts and coordinated with all potentially affected programs. This must include, but is not limited to, establishment of a MIPRB and ensuring that its actions are integrated with CCB activities, including change assessment and approval decision, as applicable to contract. Ensure that the CCB processes, membership, roles, responsibilities, and delegation are documented in a program CCB OI. 2.1.3.7 Chair or co-chair the CCB. The PM may delegate CCB Chair authority, and if so, delegated authority must be documented in the program CCB OI. 2.1.3.8 Ensure that any changes are correctly flowed to all other program documentation due to an approved AF Form 1067, *Modification Proposals*. This includes, but is not limited to the Life Cycle Sustainment Plan (LCSP) to ensure that life cycle management issues such as supportability are addressed. 2.1.3.9 Establish and periodically review government and contractor CM process metrics to measure process effectiveness, identify CM process improvement, and implement government CM process improvement.

	2.1.3.10. Ensure that applicable CM processes and standards, tailored to the program based on factors including size and complexity, are required in the Request for Proposal (RFP) and in the contract after contract award. 2.1.3.11 Ensure that government data rights to all technical data required to produce, operate, and sustain the system are included in the RFP, contract, and contract modifications for all CIs. IAW Defense Federal Acquisition Regulations Supplement (DFARS) 227.7102-4(b), DFARS 227.7103-6(a), DFARS 212.7003(b)(1). The Data Accession List (DAL) may be a Contract Data Requirement on the Contract Data Requirement List (CDRL); however, the Government must ensure it has requirements in the RFP for electronic access and rights to the data in the contractor's electronic files. 2.1.3.12 Coordinate CM with all stakeholders defined in the CMP such as other Government agencies, prime contractors, external agencies, operating locations, other programs, and users. PM must formally coordinate technical baseline changes with all interface stakeholders, by ensuring that all relevant stakeholders participate in the CCB before approving and implementing changes. 2.1.3.13 Coordinate with Operational Commanders to assess /approve any configuration modification, maintenance procedure change, new operational change or degradation of baselined characteristics to a system or end-item. (Reference: AFI 63-101/20-101) 2.1.3.14 Approve determination of CIs and Computer Software Configuration Item (CSCIs) in conjunction with the contractor and input from the program Lead Systems Engineer (LSE). 2.1.3.15 Report program requirement changes and any significant technical configuration changes to the AFPEO/SP for reporting to the Configuration Steering Board (CSB), based on CSB criteria, including requirements and significant technical configuration changes that have potential to impact cost and schedule. CSBs must be conducted, at a minimum, annually for all ACAT I and IA programs in development starting at Milestone A, and are conducted in conjunction with the annual AFPEO/SP Portfolio Reviews and Program Management Reviews; the AFPEO/SP must meet intent of the CSB for all delegated ACAT II and ACAT III programs. (Reference: AFI 63-101/20-101) 2.1.3.16 Ensure CM is addressed in the Systems Engineering Plan (SEP); this may be accomplished by referencing the program CMP and CCB OI.

2.1.4 Directorate Chief Engineer	The Directorate Chief Engineer is responsible for CM processes within the Directorate and must: 2.1.4.1 Ensure that all programs within the Directorate comply with this SMCI and have a program CCB OI and a CMP, or a CM OI or equivalent document. If Directorate CCB or CM OIs exist, ensure that the Directorate CCB and CM OIs comply with this SMCI and that all Directorate program CCB OIs, CM OIs and CMPs comply with the Directorate OIs. Programs may use a Directorate CCB OI or CMP process, tailored to the program. The program CCB process may be part of a consolidated Directorate CCB process. Plan and provide resources for program CM execution.
2.1.5 Program LSE / Chief Engineer	The Program LSE / Chief Engineer must: 2.1.5.1 Implement the program CM effort IAW the program CMP and CCB OI. 2.1.5.2 Define and document a program CCB process and CCB membership with the PM. Chair or co-chair of the CCB, if/as delegated by the PM. 2.1.5.4 Review program CM approach for completeness and compliance in the required program documents. Support CM functions throughout the program life cycle. Provide technical assistance in identification of CIs. 2.1.5.7 Provide technical assistance to identify technical issues and plan for baseline changes requiring CM effort. 2.1.5.8 Ensure CM requirements are coordinated with government CM processes, and specified in the RFP, contract, and contractor Statement of Work (SOW). Ensure that contractors comply with CM instructions in the contract. 2.1.5.10 Co-chair principal formal technical reviews with the PM, as delegated by the PM, and ensure that configuration reviewed is current and includes all, and only approved changes. 2.1.5.11 Conduct engineering reviews, e.g., Engineering Review Boards (ERBs), prior to CCBs to ensure rigorous systems engineering evaluation of all ECPs and CRs, including, but not limited to, ECPs that are the result of DR actions entered

	into JDRS and reviewed by the MIPRB prior to the CCB and PM approval/disapproval; this may include serving as a permanent member of the DR Board and MIPRB. This evaluation must include technical impacts on all cross-program and enterprise level interfaces. 2.1.5.12 Ensure that all internal and external interface requirement changes are reviewed and documented IAW the program CMP and CCB OI.
2.1.6 Engineering Directorate (EN)	The SMC Engineering Directorate (SMC/EN) is the SMC OPR for the CM process and must: 2.1.6.1 Establish and maintain SMC's CM processes. 2.1.6.2 Identify and promote SMC CM best practices and conduct training as required. 2.1.6.3 Conduct annual SMC CM Forums to share CM related policy/guidance, best practices, and metrics. 2.1.6.4 Establish and maintain a program that defines SMC compliance specifications and standards for SMC and AFPEO/SP programs.
2.1.7 Government Contracting Officer (CO)	The Government Contracting Officer (CO) is the only authorized and warranted official to obligate the Government and must: 2.1.7.1 Include EIA-649-1 and SMC-T-007, or a tailored version with SMC/EN and PM concurrence in the RFP, contract, and contract modifications (or a tailored version of SMC-S-002 Configuration Management for existing contracts). 2.1.7.2 Negotiate and incorporate approved Engineering Changes (ECs), Engineering Change Orders (ECOs), and Engineering Change Directives (ECDs) into the contract. 2.1.7.3 Determine in conjunction with SMC Judge Advocate (SMC/JA) and apply on contract all appropriate DFARS; this must include the following, or justification and SMC/JA concurrence with the rationale for not including these: 2.1.7.3.1 Acquire a license for originally developed software (i.e., Unlimited Rights or Government Purpose Rights) as those terms are defined in DFARS §§ 252.227-7013 and 252.227-7014. 2.1.7.3.2 Commercial computer software or commercial computer software documentation shall be acquired under the licenses customarily provided to the public unless such licenses are inconsistent with Federal procurement law or do not otherwise satisfy user needs. (Reference: DFARS §§ 227.7202-1(a))

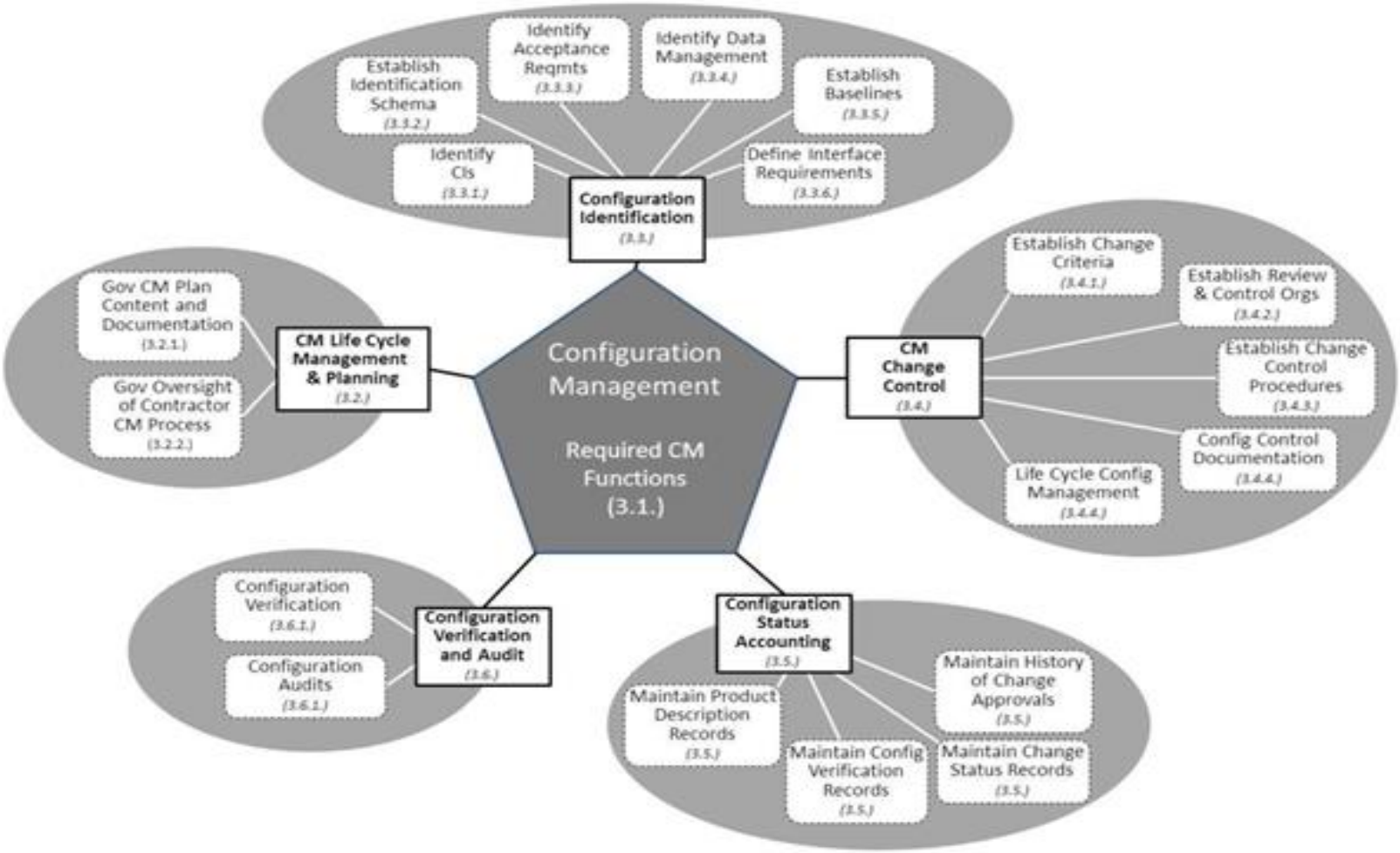
2.1.8 Product Support Manager (PSM)	The PSM must: 2.1.8.1 Provide CM product support throughout the system's life cycle. 2.1.8.2 Assume primary CM activities for CIs in sustainment after Initial Operational Capability (IOC), as delegated by the PM; however, the PM retains final change approval authority and responsibility. 2.1.8.3 Coordinate with PM on approval of AF Form 1067, *Modification Proposal(s)* and inclusion in the LCSP.

Chapter 3

CONFIGURATION MANAGEMENT FUNCTIONS

3.1. Required Configuration Management Functions. The SMC CM process requires five integrated functions as referenced in EIA-649-1: Configuration Management Planning and Management, Configuration Identification, Configuration Change Management, Configuration Status Accounting, and Configuration Verification and Audit. IAW DoDI 5000.02, the PM must use CM to establish and control product attributes and the technical baseline across the total system life cycle. The program CM activity must document, audit, and control the functional and physical characteristics of the system design; track any changes; provide an audit trail of program design decisions and design modifications; be integrated with the SEP and technical planning; and be consistent with the Intellectual Property (IP) Strategy. At completion of the system level Critical Design Review (CDR), the PM must assume control of the initial product baseline, to the extent that the competitive environment permits. *(**Note:** Software as an integral part of the overall system is subject to the same CM requirements and rigor. If a system is developed using multiple/incremental/spiral builds, each of these, as well as the total system must meet CM requirements.)* The PM must document and implement the software CM process, Deficiency Reporting (DR) process, software patch process, process to comply with security vulnerabilities, and the process to maintain Cybersecurity certifications (Reference: Air Force Pamphlet (AFPAM) 63-128 - *Guide to Acquisition and Sustainment Life Cycle Management*). Figure 3.1. depicts the five required CM functions and references the paragraphs in this document where they are described.

Figure 3.1. Required Configuration Management Functions.



3.2. CM Life Cycle Management and Planning. The PM must ensure the acquisition strategy documentation defines the program CM approach and that the results of the CM planning activity are documented in a CMP, or other equivalent document hereafter referred to as "CMP," that complies with DoD, Air Force (AF), SMC, and any Directorate CM policy or OI. The CMP must document how the program will implement CM throughout the product life cycle to synchronize and provide consistency among the product requirements, product architecture, product configuration documentation, and the product. The SMC Configuration Management Plan Template v2.0, and the SMC Configuration Control Board OI Template v2.0, are located at: **https://insidesmc.losangeles.af.mil/u?q=3Cj**. The PM must ensure that the SEP documents which artifacts (e.g., product and software data) make up the technical baseline and that these artifacts are aligned with requirements in other program documents including, but not limited to the Acquisition Strategy (AS) and RFP. The SEP must include a process diagram of how the program will maintain configuration control of its baselines and when the program assumes initial and full configuration control of its baselines (Reference: AFPAM 63-128, *Guide to Acquisition and Sustainment Life Cycle Management).*

3.2.1. **Government CM Planning and Documentation.** The PM must ensure that the CM planning activity documents the CM operations in the acquisition strategy including CM processes, procedures, audits, training, tools, metrics, organization, roles, responsibility, authority, and accountability. These must be documented in the program CMP. "The PM must ensure key CM practices and responsibilities are summarized in the SEP as specified in the DoD SEP Outline," IAW AFI 63-101/20-101, para. 5.2.1.6.4. The PM must ensure that CM roles, responsibilities, and procedures for change control are documented in the CMP and implemented, and that Cybersecurity and all specialty engineering requirements and specifications are included in the CM controlled baseline and documentation. The PM must ensure that the Government's CMP is reviewed annually, at a minimum, and before each phase of the program life cycle, revised as necessary and that the annual review is recorded in a Memo for Record (MFR) or on an AF673 Form, *Air Force Publication/Form Action Request.*

3.2.2. **Government Oversight of Contractor CM Process** . The Government must require a CMP from the contractor to include CM management of suppliers, sub-suppliers and vendors, must ensure that the contractor defines and uses methods to ensure the CM effectiveness of its suppliers, sub-suppliers and vendors, and may cite Data Item-Systems Engineering Specifications and Standards (DI-SESS)-80858 *Supplier's Configuration Management Plan*, and DI-MISC-80508 Technical Report–Study/Services, for specifying the delivery of data to meet this requirement. The Government must ensure an approved tailored version of EIA-649-1 with SMC-T-007 for new contractual actions (or SMC-S-002 *Configuration Management,* for legacy contracts), or equivalent contractor command media is on contract. The PM must approve the tailored EIA-649-1 with SMC-T-007 for new contractual actions with input from the Program LSE and SMC/EN. The CO is the only one authorized to put the tailored ANSI/EIA-649-1 for new contractual actions on contract. As an alternative, programs may put contractor command media on contract if it meets EIA 649-1 with SMC-T-007 or SMC-S-002 requirements, as tailored for the program. The program must perform a gap analysis to determine if contractor command media is sufficient to meet the program tailored EIA 649-1 with SMC-T-007 or SMC-S-002 requirements. All

documents approved by the Government for use on programs (e.g. CDRLs), including equivalent contractor command media, placed on contract must be under contractor CM, remain equivalent throughout the program life cycle and all contract(s) periods of performance, and the PM must ensure that the contractor reports all command media changes to the Government when they are approved. The Government must oversee contractor's CM processes and metrics using defined audit schedules and criteria documented in the program CMP.

3.3. Configuration Identification . The PM must ensure that the Government documents the establishment of identification schema, acceptance criteria, DM, technical baselines, and definition of interfaces as part of the Configuration Identification activity. The PM must ensure the SEP identifies all top-level and critical CIs, and that this top-level identification is included in the RFP. Lower-level CIs may be selected by the Contactor, but must be approved by the PM. The PM must ensure the Contractor documents selection of the top-level CIs and lower-level Cis (e.g., Hardware Configuration Items (HWCIs), Computer Software Configuration Items (CSCIs), and Critical Safety Items (CSIs)) to be controlled, level of control, and when they will be placed under control in the Contractor CMP CDRL prior to Government approval. The PM must track the identified CIs with their required attributes (e.g., physical, functional, and performance) throughout the development lifecycle in delivered specifications, and throughout the entire lifecycle.

3.3.1. **Identify CIs** . The PM must ensure that Configuration Identification includes the selection of CIs at the appropriate levels to facilitate the management, control and support of the items and their documentation, including system, subsystem, assembly, component and interface specifications. The Government, usually in the RFP, must identify top-level and critical CIs; lower level CIs may be identified by the Contractor and agreed to by the Government. All CIs must be agreed to by the Government and Contractor. Table 3.1. is a list of selected example criteria for identifying CIs. For CSCIs, the CM process must ensure that the contractor has identified and provided project unique identifiers for entities to be controlled, and indicate at what level and when they are to be controlled (e.g., computer files, electronic media, documents, executable software, data formats, configuration files, database schemas, etc.).

Table 3.1. CI Identification Criteria (Reference: MIL-HDBK-61A).

CI Parameter	CI Identification Criteria
Design	Critical, new or modified design or new technology
Independence	Independent end use functions
Effectivity	Sub-assembly factors such as the need for separate configuration control or a separate address for the effectivity of changes
Common components	Components common to several systems
Interfaces	Interface with other systems, equipment or software
Interchangeability	Level at which interchangeability must be maintained
Separate delivery or installation	Separate delivery or installation requirement; software release is as example of separate delivery or installation.
Separate performance or test	Separate definition of performance and test requirements
Risk	High risk and critical components
Safety	High safety concern
Computer software/Firmware	Computer software items, because they typically control the functionality of a system, are usually designated as CIs; they are referred to as Computer Software Configuration Items (CSCIs), e.g., computer files, executable software, data formats, configuration files, database schemas, electronic media, and documents.
Databases	E.g., risk, telemetry limit sets, command & telemetry list
Facilities	E.g., test beds, control rooms
Documentation	E.g., plans, schedules, cost estimates

3.3.2. **Establish Identification Schema.** The PM must ensure that the Government establishes a Configuration Identification numbering schema to identify and track applicable major end items, configuration-controlled items, and Government Furnished Property (GFP), and that Item Unique Identification (IUIDs) are integrated in configuration and documentation management (Refer to AFPAM 63-128, for additional IUID guidance and templates.) Item unique identification planning and implementation must be documented in an Item Unique Identification Implementation Plan linked to the program's SEP. DoD Instruction 8320.04, *Item Unique Identification (IUID) Standards for Tangible Personal Property,* provides the standards for unique item identifiers. The PM must ensure that specific attributes for each system and CI are identified, specified, approved, baselined, and documented in specifications. The PM must ensure that the product structure is documented to include the identifiers, internal structure, relationship of system components, and associated configuration documentation, and is the result of functional analysis and the allocation process of system engineering; this may be depicted as an indentured listing or graphic. Sources of additional guidance for implementing the identification schema are: Military Standard 196E (MIL-STD-196E), *Department of Defense Standard Practice Joint Electronics Type Designation System*, which standardizes the assignment of type designations for electronic items under the Joint Electronics Type Designation System (JETDS); TO 00-5-16 Methods and Procedures Software Managers and Users Model for the United States Air Force (USAF) *Automated Computer Program Identification Number System (ACPINS),* which provides guidance about identifiers for CSCIs; and AFI 16-401,

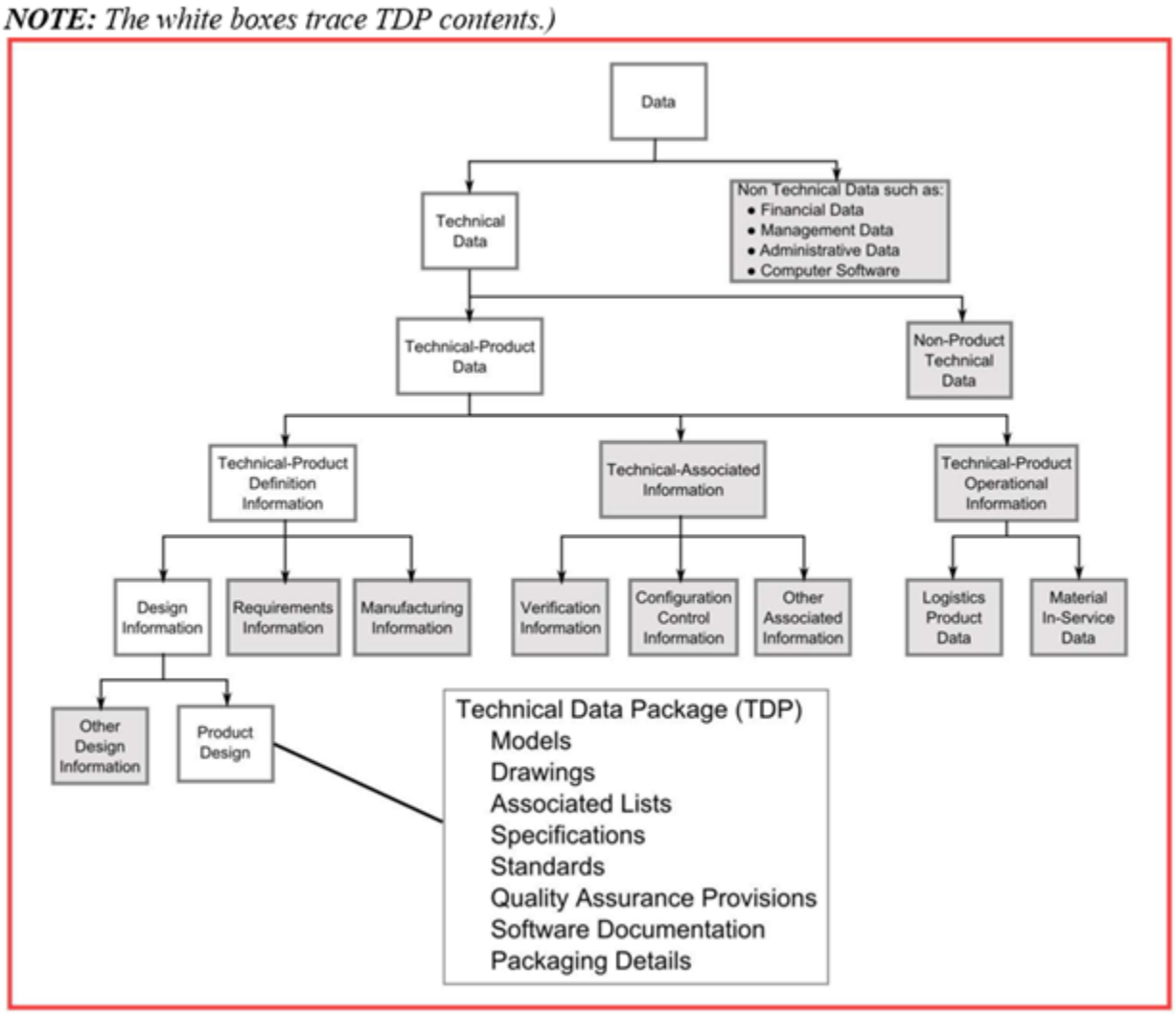
Designing and Naming Defense Military Aerospace Vehicles, which applies to identifiers of military aerospace vehicles (e.g., spacecraft, rockets, and missiles).

3.3.3. **Identify Acceptance Requirements.** The PM must ensure that the CI identification activity documents acceptance criteria in specifications or other descriptive documents. The PM must ensure that the contractor identifies all CIs including their sets, groups, units, assemblies, subassemblies, parts or other items by marking in accordance with MIL-STD-130, Identification Marking of U.S. Military Property IC 1; MIL-STD-1285D, *Department of Defense Standard Practice: Marking of Electrical and Electronic Part*s; or MIL-STD-13231, *Department of Defense Standard Practice: Marking of Electronic Item IC 1* as applicable.

3.3.4. **Identify Data Management (DM).** In the context of CM, the PM must ensure that data required to manage and support a system throughout its life cycle is identified, acquired, managed, and maintained, and that the Government DM activity provides access to the required data and computer software and documentation if maintained by the contractor (Reference: AFI 63-101/20-101, para. 5.2.1.7).

3.3.4.1. **Data and Data Rights.** In the context of CM, the PM must ensure that the Government assesses long-term data and data rights requirements in support of CM requirements and controlling the baseline. The PM must ensure that acquisition strategies prior to initiating an RFP, including the Performance Work Statement (PWS) or SOW, to acquire systems, subsystems, or end-items include the DM and IP strategy providing for rights, access, or delivery of data that the Government requires for systems sustainment, system integrity, sustaining engineering, reliability management, OSS&E assurance, and CM throughout the life cycle (Reference: AFI 63-101/20-101, para. 4.7.1.). Figure 3.2., Data Taxonomy, provides context for data relationships and CM information (Reference: MIL-STD-31000, Technical Data Packages, Revision A. *(**Note:** Detailed DM instruction is outside the scope of this CM SMCI and is included here only in the context of data's relationship to CM; DM references are cited and included in Attachment 1.)*

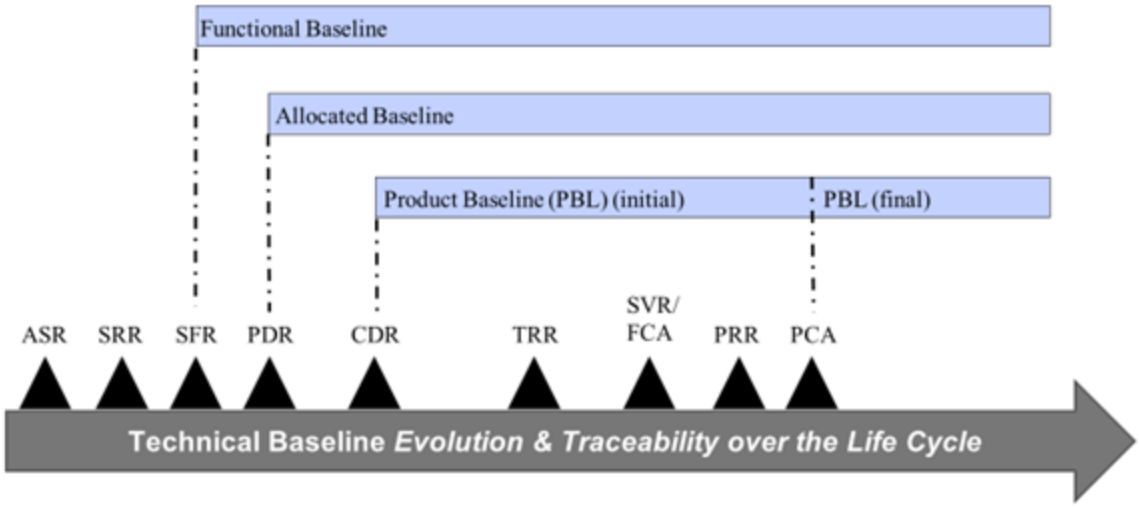
Figure 3.2. Data Taxonomy (Reference MIL-STD-31000 Technical Data Packages, Rev A)



3.3.5. **Establish Baselines** . A baseline includes agreed upon product attribute descriptions at a point in time and serves as the basis for change. Products include hardware, software, firmware, processed materials (e.g., lubricant), documentation (e.g., specifications, drawings, models, test procedures, publications, version description documents, etc.), services (e.g., transport services), and facilities (e.g., laboratory, machine shop). The PM must ensure sufficient Government knowledge, insight, and oversight of the baseline to be able to make informed decisions through control of the composition of the baselines and formal configuration control of approved baselines to identify, control, and track changes to system technical and program baselines, ensuring that changes occur only after thorough assessment of performance, cost, schedule, and risks. The PM must ensure that the Risk Management Plan (RMP) specifies how configuration control will be maintained, format and data elements for tracking risks, how the list will be maintained, who the RMP will be shared with, and how often it will be reviewed and updated (Reference: AFPAM 63-128).

3.3.5.1. **Technical Baselines.** The PM must ensure that the Government establishes the following formal technical baselines, as a minimum: the Functional (requirements), Allocated (design), and Product (as-built). For complex systems, the allocated baseline may require a Preliminary Design Review (PDR) to be conducted incrementally for each CI, and the PM may require interim baselines and that incremental reviews be conducted, leading to an overall system level PDR. The CMP must identify any required additional or interim baselines. The PM must ensure that the Allocated Baseline is established at the PDR during Technology Maturation and Risk Reduction (TMRR), and that the initial Product Baseline for all CIs is established during Engineering and Manufacturing Development (EMD) IAW DoDI 5000.02. The final systems level Functional Configuration Audit (FCA) establishes the final functional configuration. The initial Product Baseline must be established at CDR and the final Product Baseline must be established at Physical Configuration Audit (PCA). Refer to para. 3.3.5.1.4. for baseline documentation requirements. Figure 3.3 depicts technical baseline evolution across the life cycle.

Figure 3.3. Relationship of Technical Baseline with Technical Reviews and Audits.



Adapted from IEEE15288-2-2014 Figure 1

3.3.5.1.1. At completion of the system level CDR, the PM must assume control of the initial product baseline, to the extent that the competitive environment permits. IAW AFI 63-101/20-101, para. 5.2.1.6., "The PM must use CM to establish and control product attributes and technical baselines across the total system life cycle". Programs using incremental and agile development lifecycles must document in the CMP how they intend to meet the intent of this requirement. Though changes potentially occur more quickly and more often in agile, rapid acquisition, and incremental processes, accurate comprehensive CM is critical and required CM processes must clearly be documented in the program CMP and CCB OI. The PM must ensure that the Government assesses and approves the technical baseline at all milestones, technical reviews, and audits throughout the system life cycle. The PM must ensure that technical reviews are event-driven and that entrance and exit criteria or acceptance criteria are established and identified in the SEP, and that baselines are

updated to reflect any approved modifications or changes to the product, system or end-item. SMC program audits, technical reviews and readiness reviews for SMC programs are depicted in Figure 3.4. AFI 63-101/20-101, para. 5.2.1.3.1. states that the PM and the program LSE co-chair principal formal technical reviews. The PM must ensure that CM processes are equally applied to space system training systems (Reference: AFPAM 63-128). The test baseline must define development, integration and qualification test at unit, subsystem, and system levels of the product. The as-built and operations baselines are specific cases of the Product Baseline. Figure 3.5 is a summary of the Integrated CM Life Cycle, indicating SMC technical reviews, readiness reviews and audits with relationships to the technical baseline.

3.3.5.1.1.1. **Test Baseline.** The PM must ensure that the test baseline defines development, integration, qualification, acceptance and operational test at unit, subsystem, and system level to provide the highest probability of meeting specification requirements reliably under all operational conditions. A deficiency is a functional or structural anomaly or failure, which indicates a possible deviation from specification requirements for the test item and the PM must ensure that all deficiencies are documented in DRs, resolved, and tracked in JDRS. The Operational Test & Evaluation (OT&E) activity identifies, evaluates and documents system configuration changes that alter system performance. A deficiency is any result from a Government test (Developmental Test (DT) or Operational Test (OT)) affecting system operational capacity and is required to be reported, tracked, investigated and resolved. DR processes are defined by Technical Order (TO) 00-35D-54 TECHNICAL MANUAL USAF *Deficiency Reporting, Investigation, and Resolution*; however, this CM SMCI must be applied to any technical baseline changes resulting from DR actions. DR resolution actions recommended by the MIPRB can directly impact baseline configurations and all DR actions that may impact the technical baseline must be reviewed by the CCB and approved by the PM or by the CCB Chair if the PM has delegated CCB Chair authority in the program CCB OI.

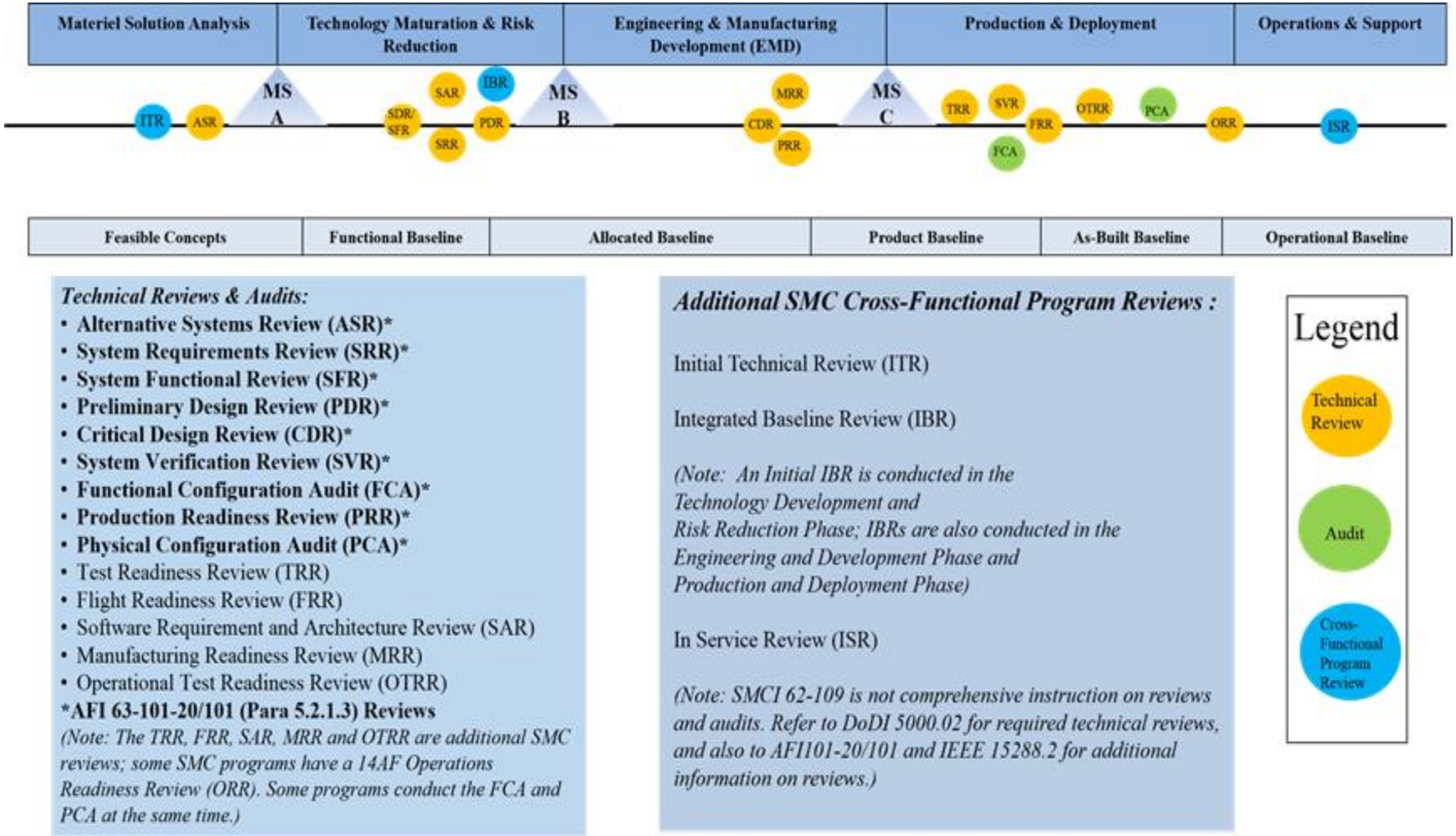
3.3.5.1.2. **As-Built Baseline.** The As-built Baseline is a specific case of the product baseline; the as-delivered and as-maintained configurations must reflect controlled modification of the as- built configuration during operations and sustainment. The PM must ensure that the Product (As-Built) Baseline (PBL) and the Final As-Built Configuration (FABC) for all Space Vehicles (SVs), Launch Vehicles (LVs) or Launch Services (LSs), and Ground Segments (GSs) are established, documented, under configuration control, and archived by either the acquisition program office or by the prime contractor with access provided to the Government. The FABC must include the PBL, established at PCA, and all government approved changes and/or approved deviations/waivers made to any parts, assemblies, subassemblies, interface documents, after the PCA and before launch or deployment. All FABCs must include individual CI Serial Numbers (S/Ns) or UIDs, and all approved changes to the CI since the approved product baseline. The PM must ensure that the Government assesses and obtains adequate contractual technical data rights to these configurations for the life of the system. *(**Note**: this SMCI mandates the intent of SMC/CC Guidance Memorandum, Product (As-Built) Baseline and Final As-Built Configuration for*

SMC. Additional Reference: DoD Open Systems Architecture (OSA) Contract Guidebook for Program Managers, v.1.1)

3.3.5.1.3. **Operations Baseline.** The operations baseline is a specific case of the product baseline – it is the system "as deployed or operated". To assure the preservation of baselined characteristics to a system or end-item, the PM must coordinate with the Major Command (MAJCOM) to approve any configuration modification or maintenance procedure change associated with a modification, by using the program CMP change control process including CCB review. The PM must also assess any new operational change or degradation of baselined characteristics to a system or end-item. The PM must analyze the program's CONOPS and capability document to identify external dependencies and interoperability needs and ensure that they are integrated into the program's requirements decomposition, risk management, interface management, architecture, verification, validation and other processes. SV systems rarely have changes after initial deployment other than potential software changes; any changes must be captured as "as-flown" configurations, and are specific cases of the product baseline. LVs are uniquely configured single use vehicles at this time, and SVs are usually only subject to software upgrades that can be uploaded during the Operations & Support (O&S) phase. However, GSs are subject to a myriad of changes throughout the life cycle including the O&S phase. The PM must approve any change that is outside the documented operating parameters defined in the operations baseline for all systems segments, by using the program CMP change control process including CCB review.

3.3.5.1.4. **Baseline Documentation** . The PM must ensure documentation of the Functional Baseline (FBL) in the Functional Configuration Documentation (FCD) to include functional, performance, interoperability and interface requirements, and verifications required to demonstrate achievement of requirements. The PM must ensure documentation of the Allocated Baseline (ABL) in the Allocated Configuration Documentation (ACD) includes functional, performance, and interoperability requirements that are allocated from those of a system or higher level configuration item; interface requirements with interfacing configuration items, and verification (e.g., plans, procedures, results) required to demonstrate achievement of requirements. The PM must ensure the documentation of the PBL in the Product Configuration Documentation (PCD) includes detailed design including necessary physical (form, fit, and function) characteristics and selected functional characteristics designated for production, acceptance testing and production test requirements, verifications necessary for accepting product deliveries (first article and acceptance instructions). The PCD must also contain any special tooling, software, equipment and facilities required to manufacture, operate, maintain, calibrate, or inspect items contained in the design, any special packaging parts required to package the CI, any quality assurance provisions required to accept deliveries of the CI (first article or acceptance inspection), any unique process specifications required to manufacture, operate, maintain, or calibrate items contained in the design, technical data which provides instructions for the installation, operation, maintenance, training, and support of a system or equipment. The FCD, ACD and PCD must be consistent and traceable to each other, and to any interface documents.

Figure 3.4. Integrated Configuration Management Life Cycle.



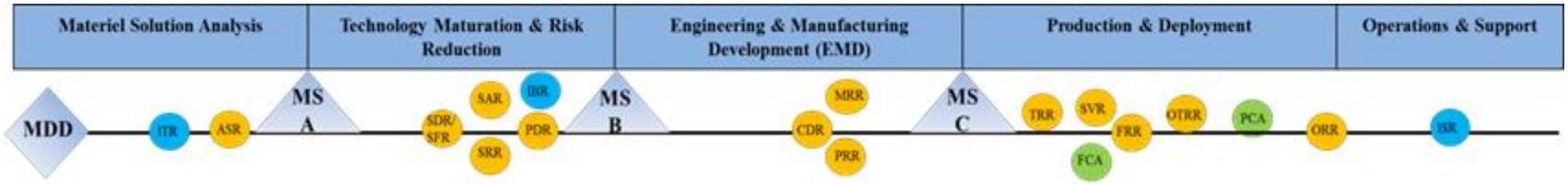
3.3.5.2. **Acquisition Program Baseline (APB).** The PM must implement Acquisition Program Baseline (APB) Management to establish, monitor, and report program progress in achieving cost, schedule, and performance objectives in the APB. A change in any one of these objectives may significantly impact any of the others; to mitigate, configuration control must be maintained within and among all cost, schedule, performance, and contract baselines.

3.3.5.2.1. **Cost Baseline.** The PM must ensure that the Cost Baseline includes the Life Cycle Cost Estimate (LCCE) and threshold and objective values for the minimum number of cost attributes over the program life cycle, as well as, the actuals.

3.3.5.2.2. **Schedule Baseline.** The PM must ensure that the Schedule Baseline includes the Integrated Master Schedule (IMS), Schedule Baseline includes the Integrated Master Plan (IMP), and threshold and objective values for the minimum number of schedule attributes over the program life cycle, and that the IMS includes critical path analysis.

3.3.5.2.3. **Performance Baseline** . The Performance Baseline must include the Capability Development Document (CDD), Key Performance Parameters (KPPs), Capability Production Document (CPD), Key System Attributes (KSAs), and threshold and objective values for the minimum number of performance attributes over the program life cycle. Although HQ Air Force Space Command (AFSPC) is the sponsor of the CDD, KPP, CPD, and KSAs, the SMC Program Office must maintain this documentation as part of the Program Baseline and ensure that the APB remains synchronized with them, even though SMC is not directly responsible for their configuration control and management. Refer to DoDI 5000.02 and Joint Capabilities Integration Development System (JCIDS) Manual, for capabilities development process.

Figure 3.5. Integrated Configuration Management Life Cycle.



	Feasible Concepts	Functional Baseline (Requirements)	Allocated Baseline (Design)	Product Baseline	As-Built Baseline	Operational Baseline
Government Products	**Major Architectural Aspects of Design Completed** **Initial Technical Review (ITR)** Required Documentation at MDD: Initial Capability Document (ICD) Identify Critical Technologies (CTEs) AoA Study Guidance & AoA Study Plan Required Documentation at MS-A AoA Study Results (includes Reliability Availability Maintainability-Cost (RAM-C) Draft Capabilities Dev Doc (CDD) Preferred Materiel Solution Acquisition Strategy (AS) Prelim. Sys Spec SEP, TEMP, Sys Safety Anal, Prod Supp Strat Clinger Cohen Act (CCA) Info Support Plan (ISP) Program Protection Plan (PPP) Life Cycle Sustainment Plan LCSP Decision Database Integrated Logistics Assessment (ILA) Industrial capabilities Assessment (ICA)	**Major Architectural Aspects of Design Completed** Required Documentation at SDR (SFR): Design Description Doc Functional Baseline traceability between Tech Req doc (TRD)/Sys Perf Spec/draft CDD Prelim allocated baseline through analysis Decision Database System/subsys Spec (SSS) Software Requirements Spec (SRS) Interface Req Spec (IRS) System Threat Analysis Report (STAR) before MS-B ILA, ICA Material Fielding Plan (MFP) prior to MS-B; updated at MS-C and as needed throughout Life Cycle **Acquisition Product Baseline (APB)**	**Implementation aspects of Design Completed** **Integrated Baseline Review (IBR). APB** Required Documentation at PDR: PDR Rpt &: Allocated Baseline under CM System-level functional performance decomposed External interfaces documented verification requirement document Required Documentation at CDR: CDR Rpt & System, Segment, Subsystem, CI specs Interface Control Doc (ICD) Design drawings & associated docs Decision Database Cost Analy Req Description (CARD, TEMP, SOW, SEP, LCSP, SW DEV Plan (SDP) System/Subsystem Design Description (SSDD) Software Design Description (SDD) Interface Design Description (IDD) Data Base Design Description (DBDD) Capabilities Production Document (CPD) STAR Before MS C Nat'l Environmental Policy Act (NEPA) Prog. Environ, Safety & Occupational Health Eval (PESHE) **Technology Readiness Review (TRA)** ILA, ICA Human System Integration (HSI) plan MFP updated prior to MS-C	**Design Realization** **IBR** Initial Product Baseline - Parts, Material and Process Baseline Capability Production Doc (CPD) at MS-C FCA verifies Allocated and Functional Baselines; and detailed Interfaces Design drawings & associated docs Manufacturing documentation and associated lists All Certifications, supporting data and waivers. Licenses Decision Database SW Product Specification (SPS) ILA, ICA **APB**	**FCA/PCA** **IBR** Allocated Baseline under Govt. control after SVR Product Baseline Approved after PCA All specifications Design drawings & associated docs Validated analytical & empirical data supporting reqts. Verif. Supporting test plans and procedures As designed/as built data base CSCI Version Description Document (VDD) equivalent of a release record for hardware for SW **APB**	**System Fielded** **In Service Review** Typical Documentation Product Support (PBL) under CM Tech Manuals Training, Repair & Oper. Manuals Repair history & Failure Rate Data (LCSP) **APB**
Contractor Products	**Typical Documentation** Program Characterization / Implementation Analysis	**Typical Documentation** Applicable SMC Specs/Stds (tailored) (or Contractor (Ktr) equiv stds) in TRD and SOW Preliminary Verification Plan System/subsys Spec (SSS) Interface Req Spec (IRS)	**Typical Documentation** Allocation of applicable SMC Specs/Stds (and/or Ktr equiv. stds.) in appropriate documentation (e.g., lower level specs, design, manuf., & test planning) SDD, IDD CI Functional specs into Product (build to) documentation and verification plan	**Typical Documentation** Allocated applicable SMC Specs/Stds Contractor tech data package artifacts , e.g., drawings, associated lists, models, etc. Contractor process specs SW Product Specification (SPS)	**Typical Documentation** Allocated applicable SMC Specs/Stds Contractor tech data package artifacts , e.g., drawings, associated lists, models, etc. Contractor process specs	**Typical Documentation** Allocated applicable SMC Specs/Stds Contractor tech data package artifacts , e.g., drawings, associated lists, models, etc. Contractor process specs

3.3.6. **Define Interface Requirements.** Interfaces are common boundaries with characteristics that may include, but are not limited to, functional, physical, and operational interfaces, such as mechanical, visual, thermodynamic, magnetic, electrical, electronic, electromagnetic, software, and contamination interfaces. Interface requirements must be defined as part of the system engineering process, controlled by the Government during the development of the system, and incorporated into the FCD and/or ACD. The FCD, ACD, and PCD may be comprised of multiple documents, but all interfaces must be documented, and the FCD, ACD, and PCD must be consistent with and traceable to each other. The PM must ensure that IAW AFI 63-101/20-101, para. 5.2.1.8., "The Interface Management (IM) process must ensure interface definition and compliance among the internal elements that comprise a system, as well as, with other systems. The LSE must ensure that all internal and external interface requirement changes are documented in accordance with the program's CMP".

3.3.6.1. **Interface Control Document (ICD).** The PM must ensure that ICDs are CIs under CM, and that ICDs specify interface to establish and maintain compatibility, coordinate control of interface changes, and record and communicate design changes, including physical, functional, and performance interface characteristics of related items (CIs or components).

3.3.6.2. **Interface Control Working Group (ICWG).** A program ICWG may be established and, if established, must be specified by contract to control interface activity. The PM must use the ICWG, if established by contract, to resolve interface problems, document interface agreements, and evaluate ECPs and CRs affecting interfaces among the acquiring activities, supplying activities, or other stakeholder agencies. The ICWG must include members of all entities sharing an interface and be empowered to commit specific interface actions and agreements to create, update, release, and control their ICDs.

3.4. Configuration Change Management. The PM must ensure that a systematic Configuration Change Management process is used to manage change proposals, justification, coordination, disposition, and implementation of all approved changes to baselined configuration documentation. This process must include impact evaluation to all stakeholders, and include cross-program and enterprise interfaces. The formal technical baseline starts when the functional configuration baseline is established for a system or CI, and must include identification of CIs, acceptance criteria captured in specifications, DM, and defined interfaces. All change requests must be configuration controlled and follow the program documented Change Control (CC) and CCB processes, which must be compliant with this SMCI. The PM must ensure that the contractor uses an ECP, or equivalent government approved document, to document all proposed changes using appropriate form/text, such as the Department of Defense Form (DD Form 1692), ECP for describing and managing a change; the contactor's format may be used for Class II changes with Government approval. ECP supporting data must include drawings and all other data (e.g., Logistics Support Analysis (LSA) data, detailed cost proposal data, test data and analyses, quality, packaging, interchangeability factors) required to evaluate all potential impacts including technical, operational, support, schedule and cost, including human engineering, program and technical impacts. The PM must ensure that the Program Office matures technical requirements with the contractor prior to soliciting or presenting an ECP or CR to the CCB to

minimize additional changes, rework, time, and costs. The government must initiate a change with a CR; Government CC process details are covered in the following 3.4. paragraphs.

3.4.1. **Establish Change Criteria** . The PM must ensure that all ECPs, CRs, and deviations (variances, waivers and revisions) are configuration controlled and follow the standard documented CC and CCB processes. CM authority and responsibility lies with the PM, who may create a Configuration Management Office(r) (CMO) and delegate CM activities to the CMO, but may not delegate CM authority or responsibility to the CMO. The PM or designee (LSE or CMO) must oversee contractor CC processes compliance, as documented in the approved program CMP and Software CMP, which must designate levels of control for each identified CI. *(**Note:** the Software CMP may be a separate document, but must be referenced or included in the CMP and remain consistent with the CMP.)* All nonconforming product must be identified and controlled to prevent unintended use or shipment.

3.4.1.1. **Change Classes** . The CCB must review and the PM must approve all proposed Class I changes to the product baseline after CDR. MIL-HDBK-61A, Configuration Management Guidance, defines Class I and II changes as: Class I changes impact the form, fit, function, or interface characteristics of the configuration item; Class II changes are changes to a Government approved technical baseline that do not meet the definition of a Class I change. In classifying a change, consideration must be given to more than the form, fit, function or interface characteristics of the CI itself. All ECP classification factors (Refer to MIL-HDBK 61A Activity Guide: Table 6-2, pages 6-16) must be considered prior to classifying an ECP. In performance- based acquisition, these terms apply only to changes that affect Government-approved (baselined) configurations and their documentation. Class II changes may be approved by the Contractor, but must be reviewed by the Government Program Office for concurrence with classification. If the Defense Contract Management Agency (DCMA) is delegated CM by way of the contract, Letter of Delegation (LOD) or Memorandum of Agreement (MOA), then DCMA will review Class II changes to verify classification of Class II. The contractor implements Class II changes, DCMA does not. Refer to DCMA-INST 217 (IPC-1), *Configuration Change Management,* for additional CM activities that may be delegated to DCMA. All CM delegation must be documented in the program CMP and program CCB OI. If the Government determines that a Class II change is a Class I change, the Government will become the CDCA and must review and approve all Class I changes. The LSE is the authentication authority for approved drawings generated organically, or if tasked by the government to prepare Air Force drawings, the contractor is the authentication authority and must include release control signatures (Reference: AFPAM 63-128).

3.4.1.2. **Modification Types.** Permanent modifications change the configuration for operational effectiveness, suitability, survivability, service life extension, and/or reduced ownership costs of a fielded system or item. The PM must ensure that all sustainment modifications have traceability to existing, validated requirements (CDD, CPD, etc.) and are reviewed by the CCB prior to PM approval. AFI 63-101/20-101, defines two kinds of temporary modifications: Temporary-1 (T-1) and Temporary-2 (T-2). T-1 modifications change the configuration of an item to satisfy short-term operational mission requirements and may be used to satisfy an Urgent Operational Need (UON) that has been validated IAW AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*, and Joint Urgent Operational Needs (JUONs) that have been

validated IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3470.01, *Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS)* in the Year of Execution. T-2 changes used to conduct Test and Evaluation (T&E) must be documented in AF Form 1067, *Modification Proposal*, and when no longer needed, as defined in the AF Form 1067, must be removed and the CI returned to its Technical Baseline permanent configuration. Refer to AFI 10-601 and AFI 63-101/20-101, Attachment 2, *Modification Proposal Process*, for guidance on the use of AF Form 1067 for defining, validating, and approval of modification requirements. Temporary changes do not change the Technical Baseline documents or requirements. The PM must ensure that all permanent and temporary changes are configuration controlled and follow the standard documented CC and CCB processes, including CCB review and PM approval.

3.4.1.3. **Request for Variance (RFV)** . IAW EIA-649-1 3.3.2, if it is necessary to temporarily depart from specified baseline requirements, a request for variance must be identified, classified, documented, coordinated, evaluated and dispositioned. The Program may cite DI-SESS-80640 *Request for Variance (RFV*), for specifying the delivery of the data product to meet this requirement. All critical and major variances must be reviewed by the CCB and approved by the PM. The Supplier must use content in DD Form 1694, *Instructions Request Deviation/Waiver*, for assigning a Critical/Major or Minor classification to an RFV. Minor variances may be approved by the Contractor, or other delegated government agencies such as the DCMA, but must be reviewed by the Government Program Office for concurrence with classification. The Supplier must use content in DD Form 1694 for assigning a Critical/Major or Minor classification to an RFV.

3.4.2. **Establish Review & Control Organizations.** The PM must establish a CCB composed of technical, functional, and administrative representatives and stakeholders to assess the necessity of proposed changes, alternatives considered, benefits, and impacts (cost, schedule, and performance) to the functional, allocated, and product baselines, including enterprise or cross program impacts. The CCB must include any cross-program and enterprise level interface stakeholders. The PM must ensure that the CCB structure including any related CCBs, technical review boards, Engineering Review Boards (ERBs), Sustainment Modification Review Boards (SMRBs), etc., their membership, roles and responsibilities, processes, metrics, chairperson, secretariat, signature authority, and internal/external organizational representatives are documented in a program CCB OI. Conducting an ERB, or equivalent technical review board, as part of this pre-CCB process is required. All changes approved by these Boards must be reviewed by the Program CCB. Mandatory CCB members must include Systems Engineering, Program Control, Contracts, Operations, Cybersecurity, Systems Safety Engineering, and Logistics/Life Cycle Sustainment (may be PSM). The PM may specify additional required members from other functional area representatives and stakeholders. CCBs may be conducted at several levels in addition to the program level such as the segment, field, prime contractor, Directorate, and Enterprise levels. A program may act on a change recommendation of a related CCB such as a cross-program or Directorate CCB, but the program PM must approve the change for the program and ensure that it is documented IAW the program CCB OI. Some CCB items may be elevated to the Headquarter Air Force (HAF)-level Configuration Steering Board (CSB) for AFPEO/SP action based on CSB established criteria, including requirements and

significant technical configuration changes that have potential to impact cost and schedule. The Cybersecurity Manager must be a fully participating member of the CCB for all systems that have any impact (low, moderate, high) to loss of information system integrity. The SMC CCB OI Template v 2.0 is located at **https://insidesmc.losangeles.af.mil/u?q=3Ci**.

3.4.3. **Establish Change Control Procedures.** The PM must ensure that the CCB OI defines a tailorable change control process to ensure full technical review of all proposed changes, including a Cybersecurity review of all proposed DoD information system changes to include interconnections to other DoD information systems. The CCB must review and recommend approval or disapproval of all proposed ECs, CRs, or variances to a CI's current approved and baselined configuration documentation. The CCB is not a voting body. The CCB Chairperson is the single decision authority in consultation with the CCB members. The PM is the CCB Chair unless the PM has delegated the CCB Chair authority in the program CCB OI, such as to the LSE, or other role. The LSE is responsible for technical evaluation of changes. The PM must make the final decision regardless of who chairs the CCB. CCBs must publish minutes documenting alternatives considered and decision results. Each CCB decision must be documented on a Configuration Control Board Directive (CCBD) document or equivalent, such as an Engineering Change Directive (ECD), signed by the CCB Chairperson. The Program CO must use the change decision documentation to take appropriate actions to implement the approved change through a formal contract modification. All information systems Cybersecurity CM must be under the control of the Program CC. Artifacts that demonstrate adherence to Cybersecurity and Risk Management Framework (RMF) for DoD Information Technology (IT) requirements include a CMP, CCB OI, and CCB minutes in accordance with the baseline configuration controls and configuration change controls as described in Committee on National Security Systems Instruction (CNSSI) 1253, and National Institute of Standards and Technology (NIST).

3.4.4. **Configuration Control Documentation.** The PM must ensure that the change control documentation includes control of revisions to architectures, specifications, designs, drawings, and data applied to hardware and software CIs and their interfaces (ICDs). This includes control of all technical baseline and other required documentation under CM control in all media including Model-Based System Engineering (MBSE) and other modeling and automated tools (i.e., test script generation, test data generation, etc.), which must also be under CM. System, solution or enterprise configuration changes, such as changes to the CONOPS, may require review and potential updates to various program documents. Examples include solution or enterprise architecture documentation (e.g., DoD Architecture Framework (DoDAF) views, system, solution, or enterprise models, SEP, Test & Evaluation Master Plan (TEMP), LCSP, Programmatic Environment, Safety and Occupational Health Evaluation (PESHE), and the Space Debris Assessment Report (SDAR)). Product preservation (e.g., handling, packaging, storage, and protection) documentation, processes and specifications must be baselined and under CC. The SMC PM or designee must monitor the execution and compliance to the contractor CMP, including the Software CMP. *(**Note**: There may be a separate Software CMP document; however, it must be referenced or included in the CMP and remain consistent with the CMP. For Agile software development, the Software CMP must define at what levels formal change control and CCB review will be implemented.)* Table 3.2, a synopsis of MIL-HDBK 61A (SE) Table 5-9, *Software Documentation and Configuration Control*, is an example of Software CC for a program.

Table 3.2. Software Documentation and Configuration Control (Excerpt from MIL-HDBK-61A (SE) Configuration Management Guidance Table 5-9).

DOCUMENT Acronym		CM Relationship
OCD	*Operational Concept Document (OCD)* - Proposed system; user needs	Not configuration documentation. Data Control Only (i.e., Baseline internal to developer for document, document representation and file management purposes only)
SDP	*Software Development Plan (SDP)* - Development effort; process, methods, schedules, organization, resources. (Includes or refers to Software Configuration Management (SCM) & Software Quality Assurance (SQA) plans)	
STP	*Software Test Plan (STP)* - Qualification testing; Software (SW) item; SW system; environment, tests, schedules	
SIP	*Software Installation Plan (SIP)* - Installing SW; user sites; preparations; training; conversion	
STrP	*Software Transition Plan (STrP)* - Transitioning to maintenance organization; Hardware (HW); SW; resources; life cycle support	
SSS	*System/Subsystem Specification (SSS)* - Specifies system or subsystem requirements; requirement verification methods. May be supplemented with system level Interface Requirements Specification (IRS)	Functional or Allocated Baseline
SSDD	*System/Subsystem Design Description (SSDD)* - System/subsystem-wide design; architectural design; basis for system development. May be supplemented with Interface Design Description (IDD), Data Base Design Description (DBDD)	Design release
SRS	*Software Requirements Specification (SRS)* - Specifies SW requirements; verification methods. May be supplemented with *Interface Requirements Specification (IRS)* - Specifies interface requirements for one or more systems, subsystems, HW items, SW items, operations or other system components; any number of interfaces (Can supplement SSS, SSDD, SRS)	(Government or Contractor) Allocated Baseline for CSCI
IRS		

SDD	*Software Design Description (SDD)* - SW item-wide design decisions; SW item architectural design; detailed design, basis for implementing; information for maintenance (May be supplemented by IDD, DBDD)	All are Config Doc Design release
IDD	*Interface Design Description (IDD)* - Interface characteristics; one or more systems, subsystems, HW items, SW items, operations or other system components; any number of interfaces; detail companion to IRS; communicate and control interface design decisions (Can supplement SSDD, SDD)	
DBDD	*Data Base Design Description (DBDD)* - Data base design; related data, files, SW/data base management system for access, basis for implementation and maintenance	
SPS	*Software Product Specification (SPS)* - Contains or references executable SW, source files; SW maintenance information; "as-built" design information, compilation, build, modification procedures; primary SW maintenance document.	Product baseline; either Government or Contractor
SVD	*Software Version Description (SVD)* - Identifies and describes a SW version; used to release, track and control each version.	Not baselined. Status Accounting record for released
VDD	*Version Description Document (VDD)* - For software items, the content of a CSCI Version Description Document (VDD) reflects the documentation required to operate and support the software and is the equivalent of a release record for hardware.	Is a CSCI, part of PCA

3.4.5. **Life Cycle Configuration Management.** The PM must ensure that the program Life Cycle CM process documents all the technical activities/events throughout the system life cycle, as required in the SEP, Acquisition Strategy Document (ASD), TEMP, Program Protection Plan (PPP), LCSP, RFPs, source selection evaluation criteria, contractor proposal evaluations, contract awards, system design, development, and testing activities. CM must be applied to all technical reviews and audits (e.g., PDRs, CDRs, SVRs, Test Readiness Reviews (TRRs), Production Readiness Reviews (PRRs), FCAs, and PCAs) to capture results and any approved configuration changes. Refer to DoDI 5000.02 for required technical reviews; these and typical additional SMC reviews and audits are in Figure 3.4. Audits must be used to verify the configuration. Inputs to Configuration Verification and Audit (the Functional and Physical Configuration Audits) must include schedule information (from CSA), CI configuration documentation, product test results, and the physical hardware or software. The PPP must be compliant with RMF, which defines Cybersecurity (formerly Information Assurance) requirements, must be under CM and remain compliant with RMF throughout the system life cycle.

3.5. Configuration Status Accounting (CSA). The PM must ensure that CSA is performed to capture, store, and provide access to configuration information required to manage systems and their CIs effectively, and that the contractor CSA system provides government access to all product configuration information, which includes but is not limited to product definition information (information that defines the product's requirements, documents the product attributes, and is the authoritative source for CM of the product) and product operational information (information developed from product definition information used to test, train, operate, maintain, retire, and dispose of a product).

3.5.1. **CSA Records** . CSA records must include product description, current version/revision/release of each entity, a record of changes to the entity, status of problem/change reports affecting the entity, and configuration verification records including audit schedules, status, and results. The PM or designee must, at a minimum, perform CSA as part of each technical baseline release. All audit and baseline review results must be captured and documented, as defined in the program CMP. The Government must ensure that the Contractor prepares and maintains records of the configuration status of all CIs (Hardware Configuration Items (HWCIs) and CSCIs)) under any level of configuration control above the individual author/developer level. These records must be maintained for the life of the contract. The Government may require DI-SESS-81253 *Configuration Status Accounting Information*, and DI-SESS-81245 *Installation Completion Notification*, for specifying the delivery of CSA data. The Government must ensure integrity of the technical baseline, and may use the contractor's CSA system to validate the content of the program technical baseline, but must not depend on the contractor's CM team to ensure integrity of the technical baseline. IAW with AFI 33-322, *Communications and Information Records Management Program*, the PM must ensure that the AF Records Information Management System (AFRIMS) is used as the data source for metrics associated with program management, i.e., file plan approval rates, staff visits (visited/not visited), training, and staging. The PM must ensure that all records created as a result of processes prescribed in this publication are maintained IAW AFMAN 33-363, *Management of Records*, and disposed of IAW the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**.

3.5.2. **Government data access rights** . The Government must ensure data access rights to any CSA data under the Contractor's control pertinent to the any system under research, development or sustainment contract. The PM must ensure that the contractor CSA system is in compliance with DoD Cybersecurity requirements for the purpose of interoperating with the Government's CSA system in an integrated digital environment; and has close linkage to the product configuration and product operational information through either an integrated Product Data Management (PDM) system or integrated individual IT tools.

3.5.3. **CC Metrics.** The PM must ensure that audit CC metrics are derived from CSA reports and collected, analyzed, reported, and acted upon to measure and ensure program CM effectiveness. CM metrics must be defined in the program CMP or CM OI to enable CM continuous process improvement; representative metrics include number of audit action items generated per audit and how long to closure of action items.

3.6. Configuration Verification and Audit. The PM must use configuration verification and audit to ensure that: (1) Configuration documentation used as the basis for CC and for support and sustainment of the product throughout its life cycle is complete and accurate, (2) the physical product and documentation configurations remain synchronized, (3) other configuration management functions are being performed satisfactorily, (4) configuration changes are not allowed to occur outside the approved change control process, and (5) product design meets documented contractual requirements. Configuration verification and audit must consist of: (1) verification and audit planning, (2) a continuous configuration verification process, and (3) periodic verification audits, each consisting of pre-audit preparation, audit conduct, and post-audit reporting and follow-up. Verification of proposed configuration changes requires testing before implementation in the operational environment to provide assurance that the product/system meets requirements and that the CM process is working properly. Rigorous CM processes and verification and audit must be used to help to ensure that Cybersecurity vulnerabilities and all other specialty issues are identified and addressed before implementation. The PM must ensure that the program's configuration verification processes, relationships, and interaction between Contractors' and Government configuration verification processes, responsibilities, planned configuration audits, and metrics are documented.

3.6.1. **Configuration Verification.** Configuration verification applies to systems engineering, design engineering, manufacturing, quality assurance, and contracting throughout the lifecycle. The PM must ensure that configuration planning, execution, and reporting from these other functional disciplines is adequate to support the program's overall CM processes and goals. The PM must ensure that the configuration verification process ensures the following: (1) that the initial baseline definition of each CI is accurate and complete, (2) that approved changes to the baseline are incorporated into both the CI itself and its documentation, and (3) that variances are documented and worked to resolution.

3.6.2. **Configuration Audits** . Program configuration audits for CIs (HWCIs and CSCIs) provide the framework and detailed requirements for verifying that the contractor's development effort has successfully achieved requirements specified in the configuration baselines. The PM must ensure that all action items are identified, resolved, and closed before the design activity and technical reviews are considered complete. These audits must ensure that all approved changes at the time of the audit are incorporated and no other changes are included. The PM must ensure that Configuration Audits are conducted periodically throughout a program's life cycle to evaluate the accuracy of the configuration verification process, and must be conducted at initial baseline, milestones, and technical reviews. Planned audits must be documented in each program's CMP. Two specific types of audits (i.e., FCA and PCA) are described in SMC-S-021, *Technical Reviews and Audits for Systems, Equipment, and Computer Software*, Appendices G and H. SMC-021 has been replaced with IEEE 15288.2 IEEE *Standard for Technical Reviews and Audits on Defense Programs*. The PM must ensure that SMC-S-021 for existing, or IEEE 15288.2 for new program contracts is a contractual compliancy document, tailored to the program's acquisition and lifecycle support strategies, and coordinated with SMC/EN. Audits that require contractor participation must be planned, conducted, and followed-up in accordance with the tailored documents under contract.

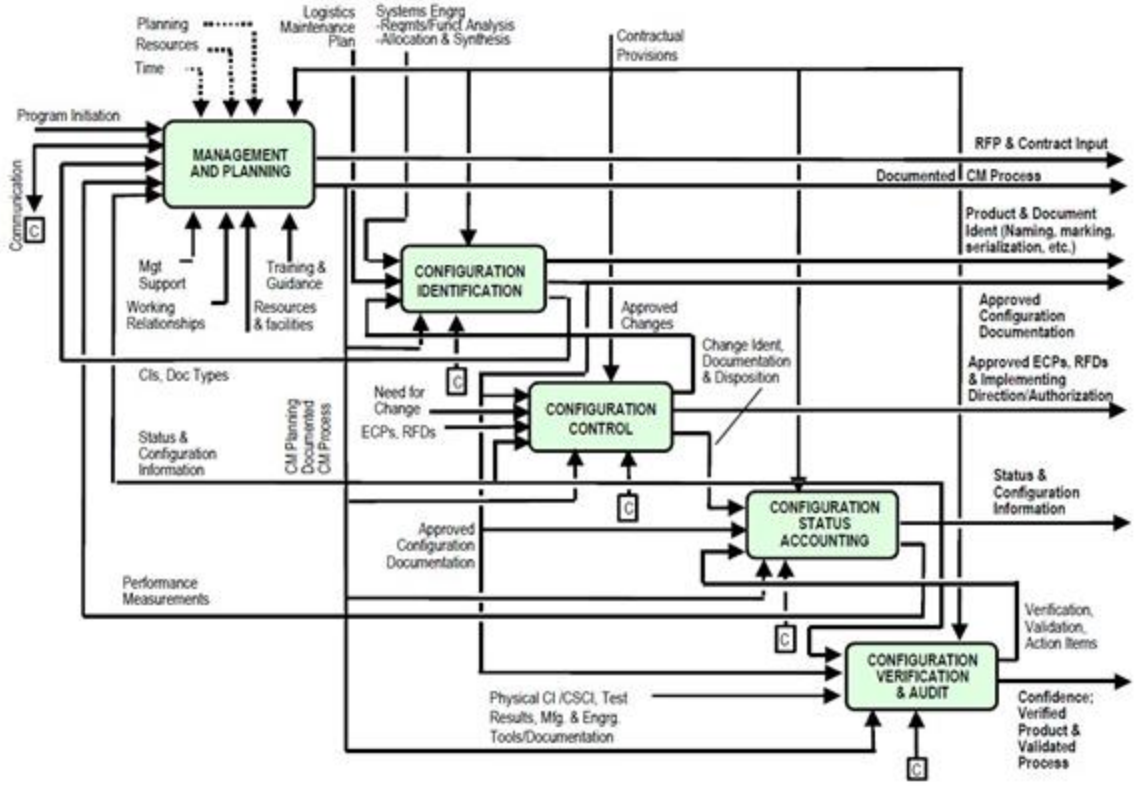
3.6.2.1. **Functional Configuration Audit (FCA).** The PM must ensure that a FCA is performed to verify and certify that actual system and lower CI performance, as reflected in test results documentation, meet requirements stated in its performance specification. A minimum of one FCA is required for each CI or system; however, a number of FCA-like activities may be conducted during the life cycle. An FCA must be conducted after changes, specifically for incorporation of new CIs into the system via a modification. Refer to MIL-HDBK-61A for additional details. The Government must ensure that the contractor provides a requirements/test matrix or test verification matrix to include identification and traceability for all requirements; a cross reference to the test plans, test procedures, test programs with automatic/automated test equipment (when applicable), test reports (results of demonstrations, inspections and analyses for each requirement) and any known deficiencies supported by applicable deficiency report numbers.

3.6.2.2. **Physical Configuration Audit (PCA).** The PM must ensure that a PCA is performed to formally examine the "as-built" configuration of a CI against its technical documentation to verify that the physical product matches its baseline documentation. Additional or incremental PCAs may be conducted during the CI life cycle. As an example, ground systems will have periodic audits performed during the O&S phase to ensure the system accuracy. The PM must ensure resolution of any discrepancies between the production-representative item that has successfully passed Operational Test and Evaluation (OT&E) and the associated documentation currently under configuration control. At the conclusion of the PCA, the product baseline is established and all subsequent changes are processed by formal engineering change action. Refer to IEEE 15288.2, Technical Reviews and Audits, for tailoring PCA entry and exit criteria which are determined by the acceptance of the contractor Systems Engineering Management Plan (SEMP).

3.6.2.3. **Audit Documentation.** The Government may require DI-SESS-81646, *Configuration Audit Pla*n*; Data Item – Administrative Data* – 81249 (DI-ADMN-81249), *Conference Agenda*; DI-ADMN-81250 *Conference Minutes*; and DI-SESS-81022 *Configuration Audit Summary Report*, for specifying the delivery of FCA and PCA results and data. The DoD requires DD Form 250, *Material Inspection and Receiving Report (MIRR)* to document inspection, acceptance, receipt, and delivery of services or product, often based on the final PCA and FCA results.

3.7. Top Level CM Process Flow . Figure 3.6. illustrates top-level CM process relationships among the required five integrated SMC CM functions.

Figure 3.6. Top Level CM Process Flow (Reference MIL-HDBK-61A).



SAMUEL GREAVES, LT GEN, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems (CNSSI-1253) January 2013

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3470.01, Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) in the Year of Execution, 10 January 2012.

DoDD 5000.01, *The Defense Acquisition System*, 12 May 2003

Department of Defense Instruction (DoDI) 5000.02 *Operation of the Defense Acquisition System*, 07 January 2015, Incorporating Change 2, Effective February 2, 2017

DoDI 8320.04, *Item Unique Identification (IUID) Standards for Tangible Personal Property*, 03 September 2015

DoD Product Support Manager (PSM) Guidebook, April 2016 869

DoDI 8500.01, *Cybersecurity*, March 14, 2014

DoDI 8510.01, *Risk Management Framework for DoD IT*, 12 March 2014, Incorporating Change 1, Effective May 24, 2016

DCMA-INST 217 (IPC-1), *Configuration Change Management*, 8 August 2015

AFI 10-601, *Operational Capability Requirement Development*, 6 November 2013

AFI 16-401, *Designing and Naming Defense Military Aerospace Vehicles*, 16 May 2014

AFI 63-101/20-101 *Integrated Life Cycle Management*, 09 May, 2017

AFI 37-138, *Information Management, Records Disposition – Procedures and Responsibilities*, 31 March 1994

AFSPCI 10-605, *Operational Acceptance Process*, 20 June 2016

SMCI 63-104, SMC Operating Instruction (SMCI) – *SMC Software Acquisition Instruction*, 28 April 2011

SMCI 63-106, *SMC Specifications and Standards (S&S)*, June 2012

SMC/CC GM, SMC/CC Guidance Memorandum (GM) - Product (As-Built) Baseline and Final As-Built Configuration for SMC, 3 February 2011

SMC Enterprise Systems Integration, SMC/CC Memo 02 February 2016

TO 00-35D-54 (AFD-091021-009), Technical Order (TO) 00-35D-54 TECHNICAL MANUAL USAF *Deficiency Reporting, Investigation, and Resolution*, 01 August 2015

AFI 63-510, *Deficiency Reporting, Investigation and Resolution*, 27 March 2013

SMC-S-002, SMC Standard (SMC-S)-002, *Configuration Management*, 13 June 2008

SMC-S-012, *Software Development for Space Systems*, 13 June 2008

SMC-S-021, *Technical Reviews and Audits for Systems, Equipment, and Computer Software*, 15 September 2009 (replaced by IEEE 15288.2, *IEEE Standard for Technical Reviews and Audits on Defense Programs*, 2014

SMC-T-007, *SMC Tailoring of EIA-649-1: Definition of Major (Class I) ECP*, 15 May 2015

SMC-S-024, SMC Standard, *Test Reqts for Ground Systems*, 30 September 2013 TO 00-5-16, *Methods and Procedures Software Managers and Users Model for the United States Air Force (USAF) Automated Computer Program Identification Number System (ACPINS),* 01 January 2009

DFARS, *Defense Federal Acquisition Regulation Supplement*

DFARS §§ 227.7202-1(a), *Defense Federal Acquisition Regulation Supplement (DFARS) – Rights in Computer Software and Computer Software Documentation*

DFARS §§ 252.227-7014, *Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation*

DFARS 227.7102-4(b), *Rights in Technical Data*

DFARS 227.7103-6(a), *Government Rights*

DFARS 212.7003(b)(1), *Solicitation Provision*

MIL-STD-196E, *Military Standard -196E Department of Defense Standard Practice Joint Electronics Type Designation System*, 17 February 1998

MIL-STD-31000A, *Technical Data Packages*, Revision A, 26 February 2013 941

MIL-STD-130, *Identification Marking of U.S. Military Property*, 16 November 2012

MIL-STD-1285, *Department of Defense Standard Practice: Marking of Electrical and Electronic Parts*, 10 November 2010

MIL-STD-13231, *Department of Defense Standard Practice: Marking of Electronic Items*, 18 November 2013

MIL-STD-961 *Defense and Program-Unique Specifications Format and Content*, 09 January 2014, with change 3, 27 October, 2015

Air Force Manual (AFMAN) 33-363, *Management of Records*, 21 June 2016

AFPAM 63-113, Air Force Pamphlet (AFPAM) 63-113 - *Program Protection Planning*, 17 October 2013

AFPAM 63-128, *Guide to Acquisition and Sustainment Life Cycle Management*, 10 July 2014

SMC-G-1201, SMC Guide - *Assurance of Operational Safety, Suitability & Effectiveness (OSS&E) for Space and Missiles Systems*, 7 October 2009

MIL-HDBK-61A (SE) Military Handbook (MIL-HDBK) *61A Systems Engineering (SE) - Configuration Management Guidance*, 7 February 2001

MIL-HDBK-505 *Definitions of Item Levels, Item Exchangeability, Models, and Related Terms,* 12 February 1998

MIL-STD-973, Military Standard (MIL-STD) -973 *Configuration Management*, 17 April 1992 (Rescinded 3 September 2000) (Use for reference only)

SMC CCB OI Template, *SMC Configuration Control Board (CCB) Operating Instruction (OI) Template* v2.0, 24 November, 2015; **https://insidesmc.losangeles.af.mil/u?q=3Ci**

SMC CMP OI Template, *SMC Configuration Management Plan OI Template v2.0*, 24 November, 2015; **https://insidesmc.losangeles.af.mil/u?q=3Cj**

DoD *Open Systems Architecture (OSA) Contract Guidebook for Program Managers*, v.1.1, June 2013

DoD *Defense Acquisition Guidebook* (DAG) 2016

National Institute of Standards and Technology (NIST) Special Publication (800 Series) NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*, September 2012

Non-Government Standards (NGS) Documents:

American National Standards Institute/Electronic Industries Alliance National (ANSI/EIA)-649-1, *Configuration Management Requirements For Defense Contracts, 20 November,* 2014

American Society of Mechanical Engineers (ASME) Y14.24, *Types and Applications of Engineering Drawings*, 2012

ASME Y14.35, *Revision of Engineering Drawings*, 2014

IEEE STD 828-2012 Institute of Electrical and Electronics Engineers (IEEE) *Software Configuration Management Plans* (Application for copies should be addressed to the IEEE Service Center, P. O. Box 1331, 445 Hoes Lane, Piscataway, NJ 08855-1331), 2012

IEEE 15288.2, *IEEE Standard for Technical Reviews and Audits on Defense Programs,*

2014

ISO/IEC 15288:2015 International Standards Organization or International Organization for Standardization (ISO) *Systems and software engineering -- System life cycle processes*, 2015

ISO 10007:2003, ISO *Systems Quality Management Systems -- Guidelines for Configuration Management* (Application for copies should be addressed to the American National Standards Institute, 11 West 42nd St., New York, NY 10036), 2003

Society of Automotive Engineers (SAE) International GEIA859, Rev A, *Data Management*, April 2012

DoDI 5230.24 *Distribution Statements on Technical Documents*, 08 August 2012

MIL-STD-881 *Work Breakdown Structures for Defense Materiel Items*, 03 October 2011

MIL-HDBK-502 *DoD Handbook Product Support Analysis*, 03 May, 1997

MIL-STD-882 *System Safety*, 11 May 2012

MIL-STD-962 *Defense Standards Format and Content*, 1 August 2003

Adopted Forms

AF Form 1067, *Modification Proposal*, 01 January 1999

AF IMT 847, *Air Force Information Management Tool Recommendation for Change of Publication*

AF673 Form, *Air Force Publication/Form Action Request*

DD Form 250 *Material Inspection and Receiving Report (MIRR)*

DD Form 1692, *Engineering Change Proposal*

DD Form 1694, *Request for Deviation/Waiver (RFD/RFW)*

DI-SESS-81646, *Data Item (DI) Systems Engineering Specifications and Standards (SESS) Configuration Audit Plan*, 10 January 2014

DI-SESS-80640, *Request for Variance (RFV),* 7 April 2015

DI-ADMN-81249, *DI Administrative Data (ADMIN), Conference Agenda,* 01 October 1993

DI-ADMN-81250, *Conference Minutes*, 01 October 1993

DI-CMAN-81022C, *Configuration Audit Summary Report,* 30 September 2000

DI-SESS-81887, *Configuration Audit Summary Report and Certification* (MIL- STD-3046), 28 February 2013

DI-SESS-80858, *Supplier's Configuration Management Plan*, 07 April, 2014

DI-MISC-80508, *Technical Report–Study/Services*, 14 November, 2006

DI-CMAN-80858B, *Contractor's Configuration Management Plan*, 30 September 2000

DI-MISC-80508, *Technical Report–Study/Services*, 14 November 2006

DI-SESS-81880, *Engineering Change Proposal* (ECP) (MIL-STD-3046), 28 February 2013

DI-CMAN-81253A, *Configuration Status Accounting Information*, 30 September 2000

DI-SESS-81884, *Configuration Status Accounting Information* (MIL-STD-3046), 28 February 2013

DI-CMAN-81245A, *Installation Completion Notification (ICN),* 30 September 2000

Acronyms and Abbreviations

AAI—Audit Action Item

ABL—Allocated Baseline

ACAT—Acquisition Category

ACD—Allocated Configuration Documentation

ACPINS—Automated Computer Program Identification Number System

ADMIN—Administrative Data

AF IMT—Air Force Information Management Tool

AF—Air Force

AFD—Air Force Directive

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPAM—Air Force Pamphlet

AFPEO/SP—Air Force Program Executive Officer for Space

AFRIMS—AF Records Information Management System

AFSPC—Air Force Space Command

AML—Acquisition Master List

ANSI—American National Standards Institute

APB—Acquisition Program Baseline

AS—Acquisition Strategy

ASD—Acquisition Strategy Document

ASR—Alternative Systems Review

CARD—Cost Analysis Requirements Description

CC—Configuration Control (also Center Commander)

CCB—Configuration Control Board

CCBD—Configuration Control Board Directive

CDCA—Current Document Control Authority

CDD—Capability Development Document

CDR—Critical Design Review

CDRL—Contract Data Requirement List

CI—Configuration Item

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CM—Configuration Management

CMAN—Configuration Management

CMO—Configuration Management Office(r)

CMP—Configuration Management Plan

CO—Contracting Office(r)

CONOPS—Concept of Operations

COTS—Commercial Off The Shelf

CPD—Capability Production Document

CPI—Critical Program Information

CNSSI—Committee on National Security Systems Instruction

CR—Change Request

CSA—Configuration Status Accounting

CSB—Configuration Steering Board

CSCI—Computer Software Configuration Item

CSI—Critical Safety Item

CTE—Critical Technology Element

DAL—Data Accession List

DAG—Defense Acquisition Guidebook

DBDD—Data Base Design Description

DCMA—Defense Contract Management Agency

DD—Department of Defense Form

DFARS—Defense Federal Acquisition Regulation Supplement

DI—Data Item

DM—Data Management

DoD—Department of Defense

DoDAF—DoD Architecture Framework

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DR—Deficiency Report

DRI&R—Deficiency Reporting, Investigation & Resolution

DT—Developmental Test

DTL—Detail Specification

EC—Engineering Change

ECD—Engineering Change Directive

ECO—Engineering Change Order

ECP—Engineering Change Proposal

ECR—Engineering Change Release or Request

EIA—Electronics Industry Alliance

EMD—Engineering and Manufacturing Development

EN—Engineering (refers to SMC Engineering Directorate in this document)

ERB—Engineering Review Board

EVM—Earned Value Management

FABC-Final (As—Built) Configuration

FBL—Functional Baseline

FCA—Functional Configuration Audit

FCD—Functional Configuration Documentation

FRR—Flight Readiness Review

FY—Fiscal Year

GFP—Government Furnished Property

GM—Guidance Memorandum

GS(s)—Ground Segment (s) or Ground System

GSU(s)—Geographically Separate Units

HAF—Headquarter Air Force

HDBK—Handbook

HHQ—Higher Headquarters

HW—Hardware

HWCI—Hardware Configuration Item

IA—Information Assurance - the current appropriate term is Cybersecurity

IAW—In Accordance With

IBR—Integrated Baseline Review

ICD-Initial Capabilities Document **(Note:**—ICD is not used for Initial Capabilities Document in this SMCI except in Figure 3.5.)

ICD—Interface Control Document; ICD is for Interface Control Document in this SMCI text

ICWG—Interface Control Working Group

IDD—Interface Design Description

IEC—International Electrotechnical Commission

IEEE—Institute of Electrical and Electronics Engineers

IM—Interface Management

IMP—Integrated Master Plan

IMS—Integrated Master Schedule

IMT—Information Management Tool

IOC—Initial Operational Capability

IP—Intellectual Property

IPPD—Integrated Product and Process Development

IPT—Integrated Product or Process Team or Integrated Product Development Team

IRS—Interface Requirements Specification

ISO—International Standards Organization or International Organization for Standardization

ISR—Intelligence, Surveillance, and Reconnaissance

IT—Information Technology

IUID—Item Unique Identification

JCIDS—Joint Capability Integration Development System

JDRS—Joint Deficiency Reporting System

JETDS—Joint Electronics Type Designation System

JUON—Joint Urgent Operational Needs

KPP(s)—Key Performance Parameters

KSA(s)—Key System Attributes

Ktr—Contractor

LCCE—Life Cycle Cost Estimate

LCCM—Life Cycle Configuration Management

LCSP—Life Cycle Sustainment Plan

LOD—Letter of Delegation

LR—Launch Range (s)

LS (s)—Launch Services

LSA—Logistics Support Analysis

LSE—Lead (Program) Systems Engineer

LV(s)—Launch Vehicles

MAC—Mission Assurance Category

MAIS—Major Acquisition Information Systems

MAJCOM—Major Command

MBSE—Model Based Systems Engineering

MDA—Milestone Decision Authority

MDAPS—Mandatory Procedures for Major Defense Acquisition Programs

MFP—Material Fielding Plan

MIL—Military

MIPRB—Materiel Improvement Project Review Board

MIRR—Material Inspection and Receiving Report

MFR—Memo for Record

MS—Milestone

MOA—Memorandum of Agreement

NAF—Numbered Air Force

NGS-Non—Government Standard(s)

NIST—National Institute of Standards and Technology

NOR—Notice of Revision

O&S—Operations & Sustainment

OCD—Operational Concept Document

OI—Operating Instruction

OPR—Office of Primary Responsibility

ORR—Operational Readiness Review

OSA—Open Systems Architecture

OSD—Office of the Under Secretary of Defense

OSS&E—Operational Safety, Suitability, and Effectiveness

OT—Operational Test

OT&E—Operational Test & Evaluation

PBL-Product (As-Built) Baseline

PBM—Performance Measurement Baseline

PCA—Physical Configuration Audit

PCD—Product Configuration Documentation

PDM—Product Data Management

PDR—Preliminary Design Review

PESHE—Programmatic Environment, Safety and Occupational Health Evaluation

PEWG—Army Product Data and Engineering Working Group

PM—Program Manager

PPP—Program Protection Plan

PRR—Production Readiness Review

RAM-C—Reliability, Availability, Maintainability - Cost

RDS—Air Force Records Disposition Schedule

RFD—Request for Deviation

RFP—Requests for Proposal

RMF—Risk Management Framework

RMP—Risk Management Plan

PSM—Product Support Manager

PSR—Program Support Review

PWS—Performance Work Statement

(RFD/RFW)—Request for Deviation/Waiver

RFV—Request for Variance

S/N—Serial Number

SAR—Software Requirement and Architectural Review

SCM—Software Configuration Management

SCN—Specification Change Notice

SDAR—Space Debris Assessment Report

SDD—Software Design Description (Note: also System Development and Demonstration)

SDD—System Development and Demonstration

SDR—System Design Review

SDP—Software Development Plan

SE—Systems Engineering

SEP—Systems Engineering Plan

SEMP—Systems Engineering Management Plan

SESS—Systems Engineering Specifications and Standards

SFR—System Functional Review

SIB—Safety Investigation Board

SIP—Software Installation Plan

SMC—Space and Missile Systems Center

SMC/CC—Space and Missile Systems Center Center Commander

SMC/EN—Space and Missile Systems Center Engineering Directorate

SMC/JA—Space and Missile Systems Center Judge Advocate

SMC-S—Space and Missile Systems Center Standard

SMC-T—Space and Missile Systems Center Tailoring Standard

SMCI—Space and Missile Systems Center Instruction

SME—Subject Matter Expert

SOW—Statement of Work

SPD(s)—System Program Director(s)

SPEC—Specification

SPM—System Program Manager

SPO—System Program Office

SPS—Software Product Specification

SRR—Systems Requirements Review

SRS—Software Requirements Specification

SSDD—System/Subsystem Design Description

SSR—Software Specification Review

SSS—System/Subsystem Specification

STD—Standard

STP—Software Test Plan

STrP—Software Transition Plan

SV(s)—Space Vehicle(s)

SVD—Software Version Description

SVR—System Verification Review

S/W or SW—Software

TBS—To Be Supplied

TDP—Technical Data Package

TDL—Technical Data List/Sheet

TEMP—Test Evaluation Master Plan

TMRR—Technology Maturation and Risk Reduction

TO—Technical Order

TOR—Technical Operating Report

TRD—Technical Requirements Document

TRR—Test Readiness Review

UON—Urgent Operational Need

USAF—United States Air Force

VDD—Version Description Document

VER—Version

Attachment 2

COMMON CONFIGURATION MANAGEMENT TERMINOLOGY DEFINITIONS

Table A2.1. Common Configuration Management Terminology Definitions.

Common Configuration Management Terms Terminology Definitions	
TERMINOLOGY	**DEFINITION**
Audit Action Item (AAI) Form	A form used by audit team members while conducting FCA/PCA to write-up deficiencies and/or discrepancies for a resolution by the contractor.
Advance Change Study Notice (ACSN)	A document which may be used, instead of a preliminary Engineering Change Proposal (DD Form 1692), to identify an idea or problem in order to obtain authorization to submit a formal routine Engineering Change Proposal.
Approval	The agreement that an item is complete and suitable for intended use.
Allocated Baseline (ABL)	The initial approved documentation describing an item's functional, interoperability, and interface characteristics that are allocated from those of system or a higher-level configuration item, interface requirements with interfacing configuration items, additional design constraints, and the verification required to demonstrate the achievement of those specified characteristics.
Allocated Configuration Documentation (ACD)	The approved allocated baseline plus approved changes.
Change Request (CR)	Information describing the justification to request a change submitted to a Configuration Approval Authority for disposition (i.e., approval/disapproval/deferral). Information, by which a change is proposed, described, justified, and submitted to the approver.
Configuration	The performance, functional, and physical attributes of an existing or planned product, or a combination of products.
Configuration Audit	Review of processes, product definition information, documented verification of compliance with requirements and an inspection of products to confirm that products have achieved their required attributes and conform to released product configuration definition information. (Source: EIA-649-1) See also "Functional Configuration Audit" and "Physical Configuration Audit".
Configuration Baseline	(1) An agreed-to-description of the attributes of a product, at a point in time, which serves as a basis for defining change. (2) 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. (3) The currently approved and released configuration documentation, (4) A released set of files comprising a software version and associated configuration documentation. See: Allocated Baseline (ABL), Functional Baseline (FBL), and Product Baseline (PBL)

Configuration Control (CC)	(1) A systematic process that ensures that changes to released configuration documentation are properly identified, documented, evaluated for impact, approved by appropriate level of authority, incorporated, and verified. (2) The configuration management activity concerning: the systematic proposal, justification, evaluation, coordination, and disposition of proposed changes; and the implementation of all approved and released changes into (a) the applicable configurations of a product, (b) associated product information, and (c) supporting and interfacing products and their associated product information.
Configuration Control Board (CCB)	A board composed of technical and administrative representatives who recommend approval or disapproval of a proposed engineering changes to, and proposed deviations from, a CI's current approved configuration documentation.
Configuration Control Board Directive (CCBD)	The document that records the Engineering Change proposal (ECP) approval (or disapproval) decision of the CCB and that provides the directions to the contracting activity either to incorporate the ECP into the contract for performing activity implementation or to communicate the disapproval to the performing activity.
Configuration Documentation	Technical documentation, the primary purpose of which is to identify and define a product's performance, functional, and physical attributes (e.g., specifications and drawings). See also: Allocated Configuration Documentation (ACD), Functional Configuration Documentation (FCD), and Product Configuration Documentation (PCD)
Configuration Identification	(1) The systematic process of selecting the product attributes, organizing associated information about the attributes, and stating the attributes, (2) Unique identifiers for a product and its configuration documents, (3) The configuration management 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; and the establishment of configuration baselines for CIs.
Critical Variance	Variance classification when it is a departure from requirements affecting one or more of the following: safety human health environment, and security (local program or national).
Current Document Change Authority (CDCA)	The authority currently responsible for the content of a drawing, specification, or other document and which is the sole authority for approval of changes to that document.
Configuration Item (CI)	A Configuration Item is any hardware, software, or combination of both that satisfies an end use function and is designated for separate configuration management. Configuration items are typically referred to

	by an alphanumeric identifier which also serves as the unchanging base for the assignment of serial numbers to uniquely individual units of the CI.
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 Management Plan (CMP)	The document defining how configuration management will be implemented (including policies and procedures) for a particular acquisition or program.
Configuration Status Accounting (CSA)	The configuration management activity concerning capture and storage of, and access to, configuration information needed to manage products and product information effectively.
Concept of operations (CONOPS, CONOPs, or ConOps)	A concept of operations (abbreviated CONOPS, CONOPs or ConOps) is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. It is used to communicate the quantitative and qualitative system characteristics to all stakeholders. CONOPS are widely used in the military, governmental services and other fields.
Deficiencies	Deficiencies consist of two types: 1) Conditions or characteristics in any item which are not in accordance with the item's current approved configuration documentation; or 2) 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. A deficiency is any result from a Government test (Developmental Test (DT) or Operational Test (OT) affecting system operational capability and is required to be reported, tracked, investigated and resolved.
Deviation	A specific written authorization to depart from a particular requirement(s) of an item's current approved configuration documentation for a specific number of units or a specified period of time, and to accept an item which is found to depart from specified requirements, but nevertheless is considered suitable for us "as is" or after repair by an approved method. (A deviation differs from an engineering change in that an approved engineering change requires corresponding revision of the item's current approved configuration documentation, whereas a deviation does not).
Deficiency (test)	A functional or structural anomaly or failure which indicates a possible deviation from specification requirements for the test item. A test Deficiency may be a momentary, nonrepeatable, or permanent failure to respond in the predicted manner to a specified combination of test environment and functional test stimuli. Test deficiencies may be due to a failure of the test item or to some other cause, such as the test setup, test instrumentation, supplied power, or test procedures.
Deficiency Report (DR).	Description of the discrepant behavior and effect on the system component being tested. Report may also include information for

	managing and analyzing defects and testing, such as proposed correction, due date, assignee, completion date, source (requirements, design, implementation, etc.) or cause of the Deficiency. Also called problem report and other similar terms.
Effectivity	A designation, defining the product range e.g., serial numbers, block numbers, batch numbers, lot numbers, model, dates or event, at which a specific product configuration applies, a change is to be or has been affected, or to which a variance applies. (Source: EIA-649-1)
Engineering Change (EC)	(1) A change to the current approved configuration documentation of a configuration item. (2) 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 Priority	The priority (emergency, urgent, routine) assigned to an Engineering Change Proposal (ECP) to indicate the urgency with which the ECP is to be reviewed, evaluated and, if approved, ordered and implemented. (Source: EIA-649-1)
Engineering Change Proposal (ECP)	The documentation by which a proposed engineering change is described, justified, and submitted to (a) the current document change authority for approval or disapproval of the design change in the documentation and (b) to the procuring activity for approval or disapproval of implementing the design change in units to be delivered or retrofit into assets already delivered.
Engineering Release	An action whereby configuration documentation or an item is officially made available for its intended use. (Source: EIA-649-1)
Engineering Release Record (ERR)	Information (in a document or data base) that indicates or authorizes an engineering release. 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. (Source: EIA-649-1)
Firmware	The combination of a hardware device and computer instructions or computer data that reside as read only software on the hardware device.
Fit	The ability of an item to physically interface or interconnect with or become an integral part of another item.
Form	The shape, size, dimension, 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 configuration documentation.

Functional Configuration Audit (FCA)	The formal examination of functional characteristics of a configuration item, or system to verify that the item has achieved the requirements specified in its functional and/or allocated configuration documentation.
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 (HWCI)	See Configuration Item (CI).
Interchangeable Item	An item which (1) possesses comparable functional and physical characteristics as to be equivalent in performance, reliability and maintainability to another item of similar or identical purposes and (2) is capable of being exchanged for the other item without selection for fit or performance, alteration of the items themselves, or adjoining items, except for adjustments. (Also known as an Alternate Item) (Source: EIA-649-1; Adapted from MIL-HDBK-505)
Interface	The performance, functional, and physical characteristics required to exist at a common boundary
Interface Control	The process of identifying, documenting, and controlling all performances, functional and physical attributes relevant to the interfacing of two or more products provided by one or more organizations.
Interface Control Document (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, configuration item, or a computer software configuration item 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 non-specific term used to denote any product, including systems, material, parts, subassemblies, sets, accessories, etc.
Major variance	Variance classification when it is a departure from requirements affecting one or more of the following: (1) performance or operational limits, (2) interchangeability, reliability, survivability, maintainability, or durability of the item or its repair parts, structural strength, effective use or operation,

	weight, moment, center of gravity appearance, limits on product use or operation, temporary use of alternate items, or when the configuration documentation defining the requirements for the item classifies the departure from the requirement as major.
Materiel	A generic term for complete systems, equipment, stores, supplies and spares, including related documentation, manuals, computer hardware, firmware and software. (Source: EIA-649-1)
Modification Directive	The documentation that indicates the approval of, and direction to implement, a modification request.
Modification Request	The documentation by which a proposed modification of an asset is described, justified, and submitted to the asset owner (who is not the Current Document Change Authority (CDCA) for the asset design documentation) for approval or disapproval of implementing the modification in one or more units. A modification request may result in modification or installation drawings being created to describe the new configuration, but does not result in a revision of the existing design documentation for which an Engineering Change Proposal would be required.
Nomenclature	(1) 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 and/or lot numbers. (2) Names assigned to kinds and groups of products. (3) Formal designations assigned to products by customer or supplier (such as model number, or model type, design differentiation, specific design series or configuration).
Notice of Revision (NOR)	A document used to define revisions to configuration documentation which require revision after Engineering Change Proposal approval. (See also Engineering Change Proposal (ECP).
Performance Specification	A specification that states requirements in terms of the required results with criteria for verifying compliance but without stating the methods for achieving the required results. A performance specification defines the functional requirements for the item, the environment in which it must operate, and interface and interchangeability characteristics. Both defense specifications and program-unique specifications may be designated as performance specification. (Source: EIA-649-1; Adapted from MIL- STD-961)
Physical Configuration Audit (PCA)	The formal examination of the “as built” configuration of a configuration item against its technical documentation to establish or verify the configuration item’s product baseline.
Product Baseline (PBL)	The approved product configuration documentation.

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.
Program Manager (PM)	The Program Manager (PM) is the designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs. The PM shall be accountable for credible cost, schedule, and performance reporting to the MDA. (Reference: DoDD 5000.01, para.3.5)
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.
Repair	A procedure which reduces but does not completely eliminate a nonconformance from a CI and which has been reviewed, concurred, and approved for use by the Acquirer. The purpose of repair is to reduce the effect of the 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. Unique configuration identification must be applied to repaired items. (Source: EIA-649-1)
Retrofit	The incorporation of new design or software code, resulting from an approved engineering change, to a product's current approved configuration documentation and into products already delivered to and accepted by customers.
Revision	An attribute that distinguishes a change to a design or document in order to differentiate one closely related design or document iteration from another. A revision represents a change to a document's contents or a modification to a part such that it remains interchangeable with its previous iterations. See also version. (Source: EIA-649-1; Adapted from ASME Y14.35)
Rework	A procedure applied to a nonconformance that will completely eliminate it and result in a product that conforms completely to the drawings, specifications, or contract requirements. The supplier must disclose that the rework occurred when outside the normal process to manufacture the part. (Source: EIA-649-1)
Serial Number	An identifying number consisting of alpha and numeric characters which is assigned sequentially in the order of manufacturer or final test and which, in conjunction with a manufacturer's identifying CAGE code, uniquely identifies a single item which a group of similar items identified by a common product-tracking base-identifier.
Software	Computer programs and computer databases.

Source Control Drawing	A drawing that provides an engineering description, qualification requirements and acceptance criteria for commercial items or vendor-developed items procurable from a specialized segment of industry that provide the performance, installation, interchangeability or other characteristics required for critical applications. The drawing provides a list of approved sources of supply and the sub-vendor's item identification for the item(s) that have been qualified and approved for use in the critical application(s). The source control drawing establishes the source control item identification. (Source: EIA-649-1, Adapted from ASME Y14.24)
Specification	A document that explicitly states essential technical attributes and/or requirements for a product and procedures to determine that the product's performance meets its requirements and/or attributes.
Specification Change Notice (SCN)	See Engineering Change Proposal (ECP).
Substitute Item	An item which possesses such functional and physical characteristics as to be capable of being exchanged for another only under specified conditions or in particular applications and without alteration of the items themselves or of adjoining items. (Source: EIA-649-1; Adapted from MIL-HDBK-505)
System	A self-sufficient unit in its intended operational environment, which includes all equipment, related facilities, material, software, services, and personnel required for its operation and support.
System Elements	Members of a set of elements that constitute a system. Also referred to as configuration items, subsystems, segments, components, assemblies, or parts. (Source: EIA-649-1; Adapted from ISO/ICE/IEEE 15288 and Defense Acquisition Guidebook (DAG))
Technical Baseline	All technical information needed to support a product throughout its life cycle, including product requirements, design, and manufacturing information required to produce, test, accept, package, store, distribute, operate, maintain, modify, and dispose of the product. Examples include: (1) customer/user - program direction, preferences, needs, requirements; (2) configuration baselines (allocated, functional, product), including: requirements, architecture, interfaces, drawings, models, code, data, commercial-off-the-shelf (COTS), open source software (OSS); (3) program specific - performance reports, deficiency reports, aging trends, certification; (4) Supply - vendors, spare parts, DMS; (5) production/maintenance: facilities, training/certification. The Product Configuration Documentation (PCD) documents the PBL and includes detailed design including necessary physical (form, fit, and function) characteristics and selected functional characteristics designated for production, acceptance testing and production test requirements, verifications necessary for accepting product deliveries (first article and

	acceptance instructions). The PCD must also contain any special tooling, software, equipment and facilities required to manufacture, operate, maintain, calibrate, or inspect items contained in the design, any special packaging parts required to package the CI, any quality assurance provisions required to accept deliveries of the CI (first article or acceptance inspection), any unique process specifications required to manufacture, operate, maintain, or calibrate items contained in the design, and technical data which provides instructions for the installation, operation, maintenance, training, and support of a system or equipment.
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 configuration item and its documentation have a high probability of meeting contract requirements.
Value Engineering Change Proposal (VECP)	A proposal submitted by the Supplier to propose a change that, if accepted and implemented, provides an eventual, overall cost savings to the Government. A subcategory of ECP which proposes to reduce cost to manufacture, test, inspect, maintain, or operate the item. The purpose of the VECP is to provide an incentive to propose engineering changes which reduce cost without reducing product performance. Savings resulting from approved VECPs are shared between the supplying and acquiring activities as stipulated by the contract. (Source: EIA-649-1)
Version	(1) One of several sequentially created configuration of a data product. (2) 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).