DCMA Manual 4401-19

Enterprise Architecture

==========

Office of Primary Responsibility	**Organizational Infrastructure Capability**
Effective:	January 4, 2024
Releasability:	Cleared for public release
New Issuance	
Implements:	DCMA Instruction 4401, "Information Technology Management," January 20, 2020
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://dod365.sharepoint-mil.us/sites/DCMA-BCF-Organizational_Infrastructure/SitePages/4401-19.aspx
Approved by:	Gregory L. Masiello, LtGen, USMC, Director

Purpose: This issuance, in accordance with the authority in DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)":

- Implements DoD Instruction 8330.01, "Interoperability of Information Technology, Including National Security Systems"
- Implements DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)
- Implements policy established in DCMA Instruction 4401

- Implements DCMA's processes and the procedures necessary to effectively, efficiently, and economically define objectives and scope of the Agency's Enterprise Architecture

- Establishes architecture requirements for information technology investments and programs

- Establishes architecture requirements for Capability Development and Management activities to include, Business Process Re-engineering, Continuous Process Improvement, and execution of the DCMA Business Capability Framework

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to all DCMA activities unless higher-level regulations, policy, guidance, or agreements take precedence.

1.2. POLICY. It is DCMA policy to:

a. Develop, implement, and maintain a DCMA Enterprise Architecture (EA) that incorporates and integrates high-level strategic descriptions of DCMA missions, organizations, business processes, data, technology, applications, security, and standards to meet and align with key DoD reference architectures, including the DoD Business Enterprise Architecture (BEA).

b. Leverage the DCMA EA as the common context for analysis and decision-making across the Agency. This includes leveraging architecture to support and document various agency analysis and decision-making processes including but not limited to: capability management, capability needs identification, Continuous Process Improvement, and Business Process Re-engineering (BPR).

c. Develop, implement, and maintain architecture descriptions within the DCMA EA for DCMA Information Technology (IT) programs during each phase of the systems lifecycle.

d. Ensure mandatory metadata is identified and maintained for current and emerging DCMA business systems throughout each phase of the systems lifecycle.

e. Design and implement a structured approach ensuring enterprise and program architecture products are developed and maintained in the Agency's EA repository.

f. Ensure DCMA programs/systems provide EA viewpoints and other artifacts to describe the architecture and descriptions are used to support investment decisions.

g. Execute this Manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DCMA. The Director, DCMA, will:

a. Serve as the Milestone Decision Authority (MDA) for key decision points throughout the Business Capability Acquisition Cycle (BCAC) process in accordance with DoD Instruction (DoDI) 5000.75, "Business Systems Requirements and Acquisition. "

b. Ensure programs designated as a Defense Business System (DBS) are fully documented in the agency EA.

c. Provide adequate funding and personnel to establish and support an effective DCMA EA Program.

d. Require the DCMA Chief Information Officer (CIO) to:

(1) Maintain a list of all DoD Component IT systems using the designated authoritative IT registry.

(2) Oversee the development and use of the DoD Component architectures (enterprise, reference, and solution) that are consistent with the latest version of the DoD Information EA; support development of the architecture data recommended in this instruction.

(3) Advise the Agency Director of alternatives and solutions to identified interoperability issues.

(4) Develop guidance to require and verify that DoD Component IT is interoperable and supportable with other relevant IT, internal and external to DCMA.

(5) Take part in architectural reviews conducted by other DoD Components, as applicable.

2.2. CIO. The CIO will

a. Ensure appropriate EA support is provided for all DCMA business processes and automated capabilities.

b. Ensure that information policy and functional requirements are reflected in architectures and plans across the DCMA enterprise as a means to guarantee information safeguarding, sharing, visibility, trustworthiness, and interoperability.

c. Establish a centralized method to document the architecture of DCMA information systems.

d. Direct that systems and applications designated as DCMA enterprise capabilities are fully documented in the Agency EA.

e. Report effectiveness of DCMA's EA Program to DCMA Director, annually.

2.3 CHIEF DATA OFFICER (CDO). The DCMA CDO will:

a. Implement the appropriate statutory responsibilities of 44 USC §3520.

b. Oversee the development, promulgation, and implementation of data-related strategies, policies, standards, processes, and governance.

c. Exercise judgement and care for the development, deployment, and use of Artificial Intelligence and predictive analytics capabilities.

d. Ensure core Authoritative Data Set responsibilities and expectations are implemented uniformly across the Agency.

e. Ensure Agency data governance roles and assigned responsibilities are executed.

f. Ensure compliance with the DoD Data Strategy, regulations, policies, and standards through measuring and reporting on data maturity and data quality.

g. Ensure review and approval of operational business requirements requesting new data sets or modification to existing data sets.

2.4. CHIEF ENTERPRISE ARCHITECT (CEA). The DCMA CEA will:

a. Provide management and oversight of DCMA's EA Program.

b. Provide direction for EA development and maintenance and ensure its alignment with DoD's BEA, the Unified Architecture Framework (UAF), and other key references.

c. Serve as the senior Enterprise Architect in the Agency responsible for determining scope, framework, tool suite, development strategy, architecture design, socialization, customer outreach, and stakeholder management.

d. Co-Chair the Enterprise Architecture Review (EAR), a DCMA enterprise review body, in conjunction with the business representatives to analyze and evaluate business processes, automated capabilities, and issuance changes to ensure alignment to the DoD guidance, architecture frameworks, and policies.

e. Lead the development of the DCMA Integrated Architecture Framework (DIAF) to establish standardized definitions, viewpoints, and models to further assist the EA team and stakeholders in identifying "fit for purpose" artifacts or models.

f. Lead the development of the DCMA Integrated Enterprise Architecture Design Guide to assist the EA team and stakeholders in the architecture development process.

g. Publish and maintain the EA in a repository.

2.5. BUSINESS ARCHITECT. The DCMA Business Architect will:

a. Provide input and direction for the design, creation, deployment, and management of the DCMA business architecture to ensure its alignment with DCMA business goals and objectives.

b. Develop a business architecture strategy based on a situational awareness of various business goals and objectives.

c. Apply a structured business architecture approach and methodology for capturing the key views of the enterprise.

d. Ensure strategic enterprise goals, that provide traceability through the organization, are mapped to metrics that provide ongoing governance.

e. Describe through viewpoints the primary business functions of the enterprise and distinguish between customer-facing, supplier-related, business execution and business management functions.

f. Define the set of strategic, core and business support processes that transcend functional and organizational boundaries.

g. Identify and describe external entities such as customers, suppliers, and external systems that interact with the business and describe which performers, resources, and controls are involved in the processes.

h. Define business capabilities, operational activities, and processes across the enterprise to ensure business needs are met effectively, efficiently, and securely.

i. Capture the relationships among roles, capabilities, and business units, the decomposition of those business units into subunits, and the internal or external management of those units.

j. Support EA activities and create deliverables that guide business models, people, process, organizational change and investments.

k. Coordinate and consult on governance and portfolio management activities associated with ensuring compliance with the BEA and DCMA EA.

l. Coordinate and collaborate with stakeholders to define how business process outputs will be stored, consumed, integrated, and managed by various entities, IT systems, and applications.

2.6. DATA ARCHITECT. The DCMA Data Architect will:

a. Provide input and direction for the design, creation, deployment, and management of the DCMA data architecture to ensure its alignment with BEA and other key references.

b. Coordinate and collaborate with stakeholders to define how the data will be stored, consumed, integrated, and managed by different data entities and IT systems, as well as any applications using or processing that data in some way.

c. Ensure logical and physical data assets and management resources are aligned with business, application, and technology capabilities.

d. Oversee and guide the development effort to create, implement, and manage viewpoints required to accurately document the data architecture.

e. Ensure the data architecture is maintained in a repository and aligns to the established DoD framework.

2.7. TECHNOLOGY ARCHITECT. The DCMA Technology Architect will:

a. Determine organization needs and identify system specifications in collaboration with the Program Manager (PM), technical subject matter expert (SME), developers, and functional representatives.

b. Analyze the needs of large internal and external systems by breaking their processing into smaller manageable parts.

c. Participate in the design and document the structure of technology systems and discuss these with the stakeholders during each phase of the lifecycle.

d. Conduct presentations to senior leadership, stakeholders, and technical representatives that explain system requirements, courses of action, and technical capabilities throughout the lifecycle.

e. Work with senior IT personnel to devise plans for future IT requirements of the organization.

2.8. SECURITY ARCHITECT. The DCMA Security Architect will:

a. Develop and integrate cybersecurity architectural designs for systems and networks primarily applicable to government organizations.

b. Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements, and support the execution of secure configuration management processes throughout the acquisition lifecycle.

c. Ensure critical information security functions of acquired or developed system(s) and architecture(s) are developed in collaboration with organizational stakeholders and consistent with cybersecurity architecture guidelines.

d. Perform security reviews, identify gaps in security architecture, and support security risk management planning.

e. Evaluate security architectures and designs to determine the adequacy of proposals provided in response to requirements.

f. Support the determination of protection needs (i.e., security controls) and document how the implementation of a new system or new interfaces between systems impact the security posture of the current environment.

g. Coordinate with systems engineers, system owners, common control providers, and system security officers on the allocation of system-specific, hybrid, or common security controls.

2.9. ENTERPRISE ARCHITECT. The DCMA Enterprise Architect will:

a. Perform the analysis, planning, design, implementation, documentation, assessment, and management of the EA framework to align IT strategy, plans, and systems with the mission, goals, structure, and processes of the organization.

b. Develop reference models of the enterprise and maintain the information in the EA repository.

c. Assist with determining gaps between the current and the target architecture and developing plans for transitioning to the target business, data, security, and technology architecture.

d. Implement the policies and principles to guide technology decisions for the EA.

e. Identify and communicate opportunities to improve enterprise-level systems to support business processes and utilize emerging technologies.

f. Educate customers and stakeholders on the use and value of EA by providing guidance, support, and coordination to customers and IT project teams.

g. Document the EA infrastructure, including the business units and key processes, using modeling techniques that ensure technical integration is achieved across the enterprise.

h. Evaluate the impact of EA products and services on IT investments, business operations, stakeholder satisfaction, and other outcomes.

i. Coordinate and conduct governance and portfolio management activities associated with ensuring compliance with the BEA.

j. Ensure the rigorous application of information security and assurance policies, principles, and practices to all components of the EA.

2.10. CAPABILITY MANAGER. The Capability Manager will:

a. Be the functional proponent for capability development and definition of DCMA business processes and required system capabilities.

b. Support the development and validation of architecture products that define their mission and support areas.

c. Ensure all analysis and documentation pertaining to their capability area leverage EA to support and document all areas of capability analysis and description.

d. Serve as the senior Agency proponent/business owner and validation authority for the segment of the EA addressing their assigned capability area.

e. Appoint Capability Leads as their responsible party to oversee the development and use of the architecture to support their capability and related analysis and efforts.

f. Appoint Product Owners as their responsible party to oversee the development of capabilities to execute business processes that meet Agency requirements.

2.11. CAPABILITY LEAD. The Capability Lead will:

a. Manage and oversee the execution of the capability area on behalf of the capability manager.

b. Serve as the representative responsible for accomplishing the mission of the capability board (CAP BD).

c. Ensure use and development of the supporting EA products as part of capability development related efforts.

d. Oversee and enforce consistency and continuity of the description of the capability and its supporting architecture to avoid perpetual re-definition of the capability and the architecture.

e. Appoint SMEs to coordinate and collaborate with the EA team throughout the development of EA products.

f. Approve EA products prior to submission to Capability Manager for formal validation.

g. Inform and update Capability Managers on the development of the architecture.

2.12. PROCESS MANAGEMENT AND OPTIMIZATION DIVISION (PMOD). The PMOD will:

a. Work closely with Capability Teams and PMs to provide BPR analysis and documentation which impacts the business and Agency solution sets.

b. Use DCMA EA as the authoritative data source for architecture analysis and documentation efforts.

c. Support the development of integrated EA products with assigned architect.

d. Ensure validation and verification of any proposed changes or updates to the architecture with appropriate functional sponsors and DCMA EA team.

2.13. STRATEGIC PLANNING AND ANALYSIS DIVISION. The Strategic Planning and Analysis Division will:

a. Work closely with the CAP BD and functional leaders to facilitate the Agency's Continuous Process Improvement initiatives.

b. Use DCMA EA as the authoritative data source for architecture analysis and documentation efforts.

c. Support the development of integrated EA products with assigned architect.

d. Ensure validation and verification of any proposed changes or updates to the architecture with appropriate functional sponsors and DCMA EA team.

2.14. PM. The PM will:

a. Be the Agency functional sponsor for the IT solutions that enable the execution of business processes.

b. Ensure the acquisition, development, and operation of IT solutions are compliant with DoD Directive (DoDD) 5000.01, "The Defense Acquisition System," DoDI 5000.02, "Operation of the Adaptive Acquisition Framework," DoDI 5000.88, "Engineering of Defense Systems," and DoDI 8330.01, "Interoperability of Information Technology, Including National Security Systems."

c. Shepherd a proposed solution through the Agile Software Development Lifecycle in coordination and collaboration with stakeholders and the Capability Manager.

d. Deliver program-level architecture descriptions of their solutions and how they meet DCMA functional requirements with support from assigned architect.

e. Ensure resources are in place to provide data necessary to develop and maintain required UAF architecture models.

f. Ensure validation and verification of any proposed changes or updates to the architecture with appropriate functional sponsors and DCMA EA team involvement.

SECTION 3: VIEWPOINTS AND MODELS

3.1. UAF. Provides a means to develop an understanding of the complex relationships that exist between organizations, systems, and systems-of-systems that enable the analysis of these capabilities to ensure they meet the expectations of stakeholders. The core concepts in the UAF are based upon the DoD Architecture Framework (DoDAF) 2.0.2 Domain Metamodel and the Ministry of Defence Architecture Framework Ontological Data Exchange Mechanism, Security Views from Canada's Department of National Defense Architecture Framework, and the North Atlantic Treaty Organization Architecture Framework v 4. To assist decision-makers, UAF provides the means of extracting essential information from the underlying complexity and presenting it in a way that maintains coherence and consistency.

3.2. UAF VIEWPOINTS AND MODELS. This framework defines methods of representing EA enabling stakeholders to focus on specific areas of interest in the enterprise while retaining sight of the big picture. The UAF enables modeling of strategic capabilities, operational activities, services, resources, personnel, security, projects, standards, measures and requirements. Summary descriptions of viewpoints are provided below. The terms artifact(s), model(s), and viewpoint(s) may be used interchangeably throughout this document when referring to outcomes or products. Detailed descriptions and examples of viewpoints and models are located on the Resource Page.

a. Summary and Overview Viewpoints. These viewpoints enable the visualization of the Architectural Description definition, which is used to summarize the architecture, the vision it implements, the conditions and locations at which the architecture is intended to be deployed, and the projects that are running or will run to enable the architecture. These viewpoints may also be used to model the architecture of the architecture itself – the Whole Enterprise, its phases, and the Operational Architecture and Resource Architecture of each phase.

b. Architecture Management (Am). Identifies the metadata and views required to develop a suitable architecture that is fit for its purpose.

c. Strategic Viewpoint (St). This domain captures the vision of the organization, the architecture and its phases, the goals of the organization, and the capabilities needed in each phase of the architecture.

d. Operational Viewpoint (Op). This domain includes viewpoints that capture how organizations work, operationally, at a logical, business level.

e. Services Viewpoint (Sv). This enables the development of a business layer to the architecture, and in addition to internal systems and resources the Sv captures service specifications, service interfaces, and who provides those services.

f. Personnel Viewpoint (Ps). Due to the importance of work performed with these views, organizational relationships are utilized to introduce a set of viewpoints enabling effective design of Personnel views.

g. Standards Viewpoint (Sd). Every organization performs activities to certain standards and these views capture those standards and their formats.

h. Resources Viewpoint (Rs). This domain enables the capture of systems in the organization, resources, and supporting documentation. It adds concepts to the metamodel such as software and technology, and also classifies organizations, job titles, and persons as physical resources. The core concepts captured document systems and resources used and the functions they perform.

i. Security Viewpoint (Sc). This domain captures viewpoints of EA to illustrate security assets, security constraints, security controls, security control families and the measures required to address specific security concerns.

j. Projects Viewpoint (Pj). These viewpoints are important to architecture and document ongoing actions to increase the capabilities of the organization, into the future, and the systems or resources they field or change at different milestones of a project. The Agency has many ongoing projects, some of which may be fielding similar capabilities within different systems.

k. Actual Resources Viewpoint (Ar). The purpose of this domain is to illustrate the expected or achieved actual resource configurations and actual relationships between them. This identifies technical, operational, and business standards applicable to the architecture and defines the underlying current and expected standards. These viewpoints document the results of analysis of different alternatives, what-if scenarios, architectural tradeoffs, and the verification and validation of the actual resource configurations.

SECTION 4: APPLYING THE UAF

4.1. ALIGNMENT TO THE JOINT CAPABILITY INTEGRATION AND DEVELOPMENT SYSTEM (JCIDS). In accordance with Chairman of the Joint Chiefs of Staff Instruction 5123.01I, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," architectural views are used to facilitate validation, decision-making, and capability portfolio management. This is accomplished by leveraging the architecture to assess capabilities, and identify, approve, and prioritize gaps in these capabilities, to meet applicable requirements in the National Defense Strategy. UAF is a successor to the DoDAF and will create DoD compliant architecture viewpoints and matrices. In accordance with DoDD 8000.01, EA ensures that information policy and functional requirements are reflected in architectures and plans across the DoD and Component level enterprises as a means to guarantee information safeguarding, sharing, visibility, trustworthiness, and interoperability.

4.2. CORE PROCESSES SUPPORTED BY THE UAF. DoD has defined numerous processes supported by architectural descriptions. DCMA must adhere to defined decision support processes mandated by the Department. These processes include, but are not limited to, JCIDS, Joint Interoperability Test Command (JITC), the Adaptive Acquisition Framework (AAF), the Defense Acquisition System (DAS), Systems Engineering (SE), the Planning, Programming, Budgeting, and Execution (PPBE) process, Net-centric Integration, and Portfolio Management (PfM). These key support processes are designed to provide uniform, mandated processes, and standards, in critical decision-making areas tailored to support those decisions-making requirements.

a. JCIDS. The EA Program will provide input, collaborate with stakeholders, and coordinate with business partners to ensure warfighters receive the capabilities required to execute their assigned missions successfully by:

(1) Utilizing joint concepts and integrated Architectural Descriptions to identify prioritized capability gaps.

(2) Integrating joint Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P) approaches (materiel and non-materiel) to resolve those gaps.

(3) Leading collaborative processes to guide development of new capabilities through changes in joint DOTmLPF-P.

(4) Ensuring process owners support architecture requirements through development of specific product sets required in program documentation.

(5) Supporting resource decision-making to include more robust traceability between the missions, requirements, and capability solutions supported by resources.

(6) Modeling architectures for a broad range of complex systems, which may include hardware, software, data, personnel, and facility elements.

(7) Improving the ability to exchange architecture information among related tools that are Systems Modeling Language based.

(8) Modeling consistent architectures for system-of-systems down to lower levels of design and implementation.

b. JITC. Under the oversight and direction of the DoD CIO, JITC serves as the Joint Interoperability Certification (JIC) Authority for all DoD IT and establishes the minimum set of architecture information required in accordance with joint, multinational, and interagency interoperability requirements. JITC uses information from certain architecture viewpoints to test and evaluate DoD IT for interoperability.

(1) All systems with joint interfaces or joint information exchanges with other systems require interoperability certification. A joint interface occurs when any system whose mission is joined through a logical connection with a system(s) or data sources from an external partner for the purpose of exchanging common data, sharing situational awareness, or partnering to perform a single mission.

(2) The architecture viewpoints must be complete, accurate representations of the system, and information in each product should represent the underlying integrated set of architecture data.

(3) "Required" viewpoints represent mandatory architecture information to evaluate the interoperability of a system.

(4) "Conditional" viewpoints are mandatory under certain conditions (i.e., when the conditions described below are met) but are otherwise not necessary for interoperability test and certification. Conditional architecture requirements continue to evolve; many of the conditional viewpoints address IT services/enterprise services. In the following circumstances, conditional information becomes required information.

(5) The Project Management Office/Sponsor must coordinate with the DCMA EA to establish specific architecture viewpoint requirements, and ensure those requirements are sufficiently complete, detailed, measurable, and testable.

(6) The system design and how the architecture is documented will determine what viewpoints are needed making coordination between the Project Management Office/Sponsor and DCMA EA critical.

c. AAF. The DoDI 5000.02, "Operation of the Adaptive Acquisition Framework," establishes policy and prescribes procedures for managing acquisition programs, pursuant to the relevant sections of Title 10, United States Code. It:

(1) Assigns acquisition program management responsibilities in accordance with the authority in DoDD 5135.02, "Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))," DoDI 5000.87, "Operation Of The Software Acquisition Pathway," and DoDD 5000.01.

(2) Describes the responsibilities of principal acquisition officials and the purpose and key characteristics of the acquisition pathways.

(3) Restructures defense acquisition guidance to improve process effectiveness and implement the AAF. As a result of that restructuring, this issuance has been renamed "Operation of the Adaptive Acquisition Framework," to better reflect the current content. The six AAF pathways outlined in the new policy are:

- Urgent Capability Acquisition
- Middle Tier of Acquisition
- Major Capability Acquisition
- Software Acquisition
- DBS Acquisition
- Acquisition of Services

d. DAS. DoD uses the DAS to manage investments in technologies, programs, and product support necessary to achieve the National Security Strategy and support employment and maintenance of the United States Armed Forces. The EA Program uses the requirements in the DAS for coordination, integrated architecture development, and DOTmLPF-P analysis to ensure desired capabilities are supported by affordable systems and other resources.

(1) DoDD 5000.01 provides the policies and principles governing the DAS.

(2) DoDI 5000.02 establishes the management framework for translating mission needs and technology opportunities, based on approved mission needs and requirements, into stable, affordable, and well-managed acquisition programs.

(3) The AAF provides an event-based process where acquisition programs advance through a series of milestones associated with significant program phases.

(4) The Office of the Under Secretary of Defense of Acquisition and Sustainment leads the development of integrated plans or roadmaps using integrated architectures as its base. DCMA uses this roadmap to conduct capability assessments, guide systems development, and define the associated investment plans as the basis for aligning resources and as an input to the Defense Planning Guidance, Program Objective Memorandum development, and Program and Budget Reviews.

e. SE. DoDI 5000.88, "Engineering of Defense Systems," directs the PM to select the appropriate software development approach based on scope, requirements, schedule, and risk.

(1) The PM should consider an iterative software development process using modern agile development and operations methods.

(2) Assign a lead software engineer to manage the software acquisition team, software engineering processes, and delivery of code.

(3) Establish a software factory with multiple pipelines to deliver capability in a series of manageable, minimum viable products, to gain user acceptance and feedback for the next viable product.

(4) The software factory includes trained personnel, culture, architecture, processes, and tools that automate the activities in software development, build, test, and delivery cycles.

(5) The EA Program will support SE efforts by providing a structured approach to document design and development decisions based on established requirements.

f. PPBE. The EA Program will support the PPBE process by identifying touch points between architecture, Capital Planning Investment Control (CPIC), and the PPBE process.

(1) Participates in the identification of the data to be captured within an Architectural Description.

(2) Facilitates informed decision-making, and identify ways of presenting data to various stakeholders/roles in the PPBE decision process.

(3) JCIDS is a key supporting process for PPBE, providing prioritization and affordability advice.

g. PfM. DoDD 7045.20, "Capability Portfolio Management," requires the DoD use of capability portfolio management to advise the Deputy Secretary of Defense and the Heads of the DoD Components on how to optimize capability investments across the defense enterprise (both materiel and non-materiel) and minimize risk in meeting the Department's capability needs in support of strategy. Each portfolio will be managed using the architectural plans, risk management techniques, capability goals and objectives, and performance measures to the greatest extent possible.

(1) The EA Program will use these architecture plans to support the definition of capability requirements.

(2) PfM uses the Architectural Description to analyze decisions on fielding or analysis of a needed capability.

(3) Architectural support to PfM tends to focus on the investment decision itself (although not exclusively) and assists in justifying investments, evaluating the risk, and providing a capability gap analysis.

h. Operations. The EA Program will capture enterprise routine or repeatable business and mission operations and activities as architectural content. If the process structure is stable and the activity is repeated often, the design will include that process as part of the Architectural Description itself. The EA repository will include templates, checklists, and other artifacts commonly used to support the activity.

(1) The JCIDS, PPBE, and DAS processes establish a knowledge-based approach, which requires PMs to attain the right knowledge at critical junctures to make informed program decisions throughout the acquisition process.

(2) The DoD IT PfM process continues to evolve that approach with emphasis on individual systems and/or services designed to improve overall mission capability.

(3) Consistent with Office of Management and Budget (OMB) CPIC guidance, DCMA will use the four continuous integrated activities to manage its portfolios – analysis, selection, control, and evaluation. The overall process is iterative with results being fed back into the system to guide future decisions.

SECTION 5: EAR

5.1. EAR. Provides an enterprise review body that will analyze and evaluate business processes, automated capabilities, and policy changes to DCMA's existing and proposed operational and business environment to ensure alignment to the DoD and DCMA strategic goals and DOTmLPF-P requirements. The EAR plays a vital role in managing risk and fostering transparency through reviews of and support for DCMA change and acquisition initiatives. The EAR directly assists Agency entities by reviewing proposed capability requirements, advising on solutions, and facilitating change initiatives through management and use of the DCMA EA. By so doing, the EAR reinforces Business Capability Framework (BCF) cross-functional integration and will identify potential trade-offs between CAP BDs.

5.2. ADMINISTRATION. The EAR is co-chaired by the DCMA CEA and Director, PMOD. The co-chairs are assisted in day-to-day operation of the committee duties by Team Leads and scribes, as they may duly designate. The EAR and its members serve as the control point for DCMA capabilities documented in the EA including but not limited to the following areas:

- Business process design and integration
- Data and information architecture
- Policy and performance alignment
- Application architecture
- Technology infrastructure and architecture
- Cybersecurity architecture

5.3. BATTLE RHYTHM. The EAR will meet at least quarterly but is authorized to convene meetings as needed to review initiatives approved by CAP BDs and the Data Management Committee. The meeting procedures:

a. The EAR will meet not more than bi-weekly or as needed for emergencies.

b. Each meeting will have an agenda and relevant read-ahead materials communicated at least 5 business days before the meeting.

c. Members are required to attend scheduled meetings or provide a designated alternate authorized to act on behalf of the member.

d. The EAR will review and, if necessary, amend established EAR processes, procedures, and templates annually.

e. Members may invite task team leads/representatives or SMEs to offer information to aid in decision-making and development of EA products.

f. The EAR will provide a report of accomplishments to the DCMA War Room/Senior Leadership Team annually.

g. The CEA will report on progress of completed and ongoing EAR activities and priorities during each meeting.

h. The Director, PMOD, will report on progress of completed and ongoing BPR activities and priorities during each meeting.

5.4. CHARTER. The EAR charter, signed by the Director and managed by the Corporate Governance (CG) CAP BD, delineates the membership, goals, and responsibilities. The signed EAR Charter is located on the Resource Page.

5.5. DOCUMENTATION. To support the CG decision-making process, the EAR reviews capability requirements, conducts applicable impact analysis, and provides recommendations to CAP BDs, the War Room, Senior Leadership Team, and Agency Director on solution sets. The EA team actively monitors the Agency Intake system for situational awareness in order to provide assistance to CAP BDs through the EAR as they assess the merits of various Intake items. EAR meetings will be documented with meeting minutes. A Problem Statement Worksheet will be completed and posted for transparency, as appropriate.

SECTION 6: THE BUSINESS ARCHITECTURE

6.1. OVERVIEW. The Business Architect (in collaboration and coordination with stakeholders) will provide input and direction for the design, creation, deployment, and management of the business architecture to ensure its alignment with DCMA business goals and objectives. The Business Architect will develop a business architecture strategy based on a situational awareness of various business goals and objectives. The business architecture describes through viewpoints and models the primary business functions of the enterprise and distinguishes between customer-facing, supplier-related, business execution and business management functions.

6.2. BUSINESS VIEWPOINTS AND MODELS. The Business Architecture will be documented using a variety of artifacts, viewpoints, and models that define the primary business functions of the enterprise. The Business Architect leads the effort to identify and describe internal and external entities such as customers, suppliers, and systems enabling execution of business mission requirements and describe which performers, resources and controls are involved in the processes. These artifacts will capture the relationships among roles, capabilities and business units, the decomposition of those business units into subunits, and the internal or external management of those units. The business architecture description will include, but is not limited to the following viewpoints and models:

- Summary & Overview (Sm-Ov)
- Architecture Information: Dictionary (Am-If)
- Actual Resources Connectivity (Ar-Cn)
- Actual Resources Structure (Ar-Sr)
- Personnel Taxonomy (Ps-Tx)
- Operational Connectivity (Op-Cn)
- Operational Processes (Op-Pr)
- Operational Structure (Op-St(r))
- Operational Sequences (Op-Sq)
- Operational Traceability (Op-Tr)
- Operational Taxonomy (Op-Tx)
- Strategic Structure (St-Sr)

- Strategic Taxonomy (St-Tx)

- Strategic Traceability (St-Tr)

6.3. BUSINESS ARCHITECTURE INPUT TO DIAF. The Business Architect will design, lead the creation, deployment, and management of the DCMA business architecture domain within the DIAF. The Business Architect will ensure the domain aligns with the data, technology, cybersecurity, and application architecture domains, the BEA, and other key references.

SECTION 7: THE DATA ARCHITECTURE

7.1. OVERVIEW. The Data Architect (in collaboration and coordination with stakeholders) will define how data is stored, consumed, integrated, and managed by different data entities and IT systems, as well as any applications using or processing data. The Data Architecture provides a description of where data exists and how it travels throughout the organization and its systems. The data architecture provides the information and tools the Data Governance Team needs to properly make decisions about data policies and standards.

7.2. DATA VIEWPOINTS AND MODELS. The Data Architecture will be documented using a variety of artifacts, viewpoints, and models that define services and systems and how they interact with data objects, the attributes of those objects, the relationship among the objects, as well as the flow of data (e.g., data exchanges). The Data Architect will lead the design, creation, deployment, and management of the DCMA data architecture domain to ensure its alignment with the BEA and other key references. The data architecture description will include, but is not limited to the following viewpoints and models:

- Summary & Overview (Sm-Ov)
- Architecture Information: Dictionary (Am-If)
- Strategic Information (St-If)
- Operational Information (Op-If)
- Resources Information (Rs-If)
- Operational Connectivity (Op-Cn)
- Services Connectivity (Sv-Cn)
- Services Processes (Sv-Pr)
- Personnel Processes (Ps-Pr)

7.3. DATA ARCHITECTURE INPUT TO DIAF. The Data Architect will design, lead the creation, deployment, and management of the DCMA data architecture domain within the DIAF. The Data Architect will ensure the domain aligns with the business, technology, and application architecture domains, BEA, and other key references.

SECTION 8: THE TECHNOLOGY ARCHITECTURE

8.1. OVERVIEW. The Technology Architect (in collaboration and coordination with stakeholders) will provide input and direction for the design, development, deployment, and management of the architecture to ensure its alignment with DCMA technical goals and objectives. The Technology Architect will develop a technology architecture strategy based on current situation awareness of asset inventories information for all internal and external enterprise systems, hardware, virtualization, and associated software specifications. This includes all end-to-end resource interface connections, their configuration, and exchanges of information. The Technology Architect creates, modifies and maintains viewpoint models and matrices of system and network infrastructures and their related purpose and functions.

8.2. TECHNOLOGY VIEWPOINTS AND MODELS. The Technology Architecture will be documented using a variety of artifacts, viewpoints, models and matrices that define the primary technical capabilities of the enterprise. The Technology Architect leads the effort to identify and describe systems enabling execution of business mission requirements and describes which resource interfaces and exchanges are involved in each end-to-end process. The technology architecture description will include, but is not limited to the following viewpoints and models:

- Summary & Overview (Sm-Ov)
- Architecture Information: Dictionary (Am-If)
- Operational Processes (Op-Pr)
- Resource Connectivity (Rs-Cn)
- Resource Structure (Rs-Sr)
- Strategic Taxonomy (St-Tx)

8.3. TECHNOLOGY ARCHITECTURE INPUT TO DIAF. The Technology Architect will design, lead the creation, development, and management of the DCMA technology architecture domain within the DIAF. The Technology Architect will ensure the domain aligns with the data, business, cybersecurity, and application architecture domains, BEA, and other key references.

SECTION 9: THE SECURITY ARCHITECTURE

9.1. OVERVIEW. The Security Architect (in collaboration and coordination with stakeholders) will provide input and direction for the design, creation, implementation, management, and changes to the security architecture that ensure its alignment with DCMA goals and objectives. The security architecture describes how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. The Security Architect creates strategy, performs security reviews, identifies gaps in security architecture, and supports security risk management planning. The Security Architect will modify and maintain viewpoint models and matrices of system and network infrastructures, cybersecurity appliances, tools, products and services and their related purpose and functions.

9.2. SECURITY VIEWPOINTS AND MODELS. The Security Architecture will be documented using a variety of artifacts, viewpoints, models, and matrices that define the Agency's information security, cybersecurity protection needs (i.e., security controls), systems security engineering requirements, and support the execution of secure configuration management processes throughout the acquisition lifecycle. The security architecture description will include, but is not limited to the following viewpoints and models:

- Summary & Overview (Sm-Ov)
- Architecture Information: Dictionary (Am-If)
- Security Controls (Sc-Mv)
- Security Taxonomy (Sc-Tx)
- Security Structure (Sc-Sr)
- Security Connectivity (Sc-Cn)
- Security Processes (Sc-Pr)
- Security Constraints (Sc-Ct)
- Security Traceability (Sc-Tr)

9.3. SECURITY ARCHITECTURE INPUT TO DIAF. The Security Architect will design, lead the creation, development, and management of the DCMA security architecture domain within the DIAF. The Security Architect will ensure the domain aligns with the business, data, technology, and application architecture domains, BEA, and other key references.

SECTION 10: THE EA

10.1. OVERVIEW. The Enterprise Architect (in collaboration and coordination with stakeholders) will provide input and direction for the design, creation, deployment, and management of the architecture to ensure its alignment with DCMA goals and objectives. The application of the architecture describes how the capability integrates with the infrastructure, uses data, supports the business units, executes key processes, and incorporates data, business, and technology at the lowest level.

10.2. APPLICATION VIEWPOINTS AND MODELS. Application of the architecture will be documented using a variety of artifacts, viewpoints, and models that define the primary application capabilities. The Enterprise Architect will lead the effort to identify and describe internal and external systems that interact with the enterprise and how the resources and controls are involved in the processes. This will include, but is not limited to the following viewpoints:

- Summary & Overview (Sm-Ov)
- Architecture Information: Dictionary (Am-If)
- Operational Connectivity (Op-Cn)
- Operational Processes (Op-Pr)
- Operational Processes (Op-Pr)
- Operational Sequences (Op-Sq)
- Operational Sequences (Op-Sq)
- Personnel Processes (Pr-Pr)
- Resources Processes (Rs-Pr)
- Resources Structure (Rs-Sr)

10.3. EA INPUT TO DIAF. The Enterprise Architect will design, lead the creation, deployment, and management of the DCMA application architecture domain within the DIAF. The Enterprise Architect will ensure the architecture aligns with the business, data, security, and technology architecture domains, BEA, and other key references.

SECTION 11: APPLYING THE DIAF

11.1. INTRODUCTION. The DCMA DIAF combines the Business, Data, Security, and Technology architectures while aligning to the UAF. The DIAF was developed for the internal use by architects, analysts, and modelers to establish a standardized set of architecture products. The DIAF serves as a guide to describe the methods, rules, and conventions to be used in development of diagrams and models that comprise the DCMA Enterprise Architecture (DEA). The terms model(s), diagrams(s), view(s), viewpoint(s), and matrices may be used interchangeably when referring to outcomes or products. Although the DIAF is aligned to architectural models included in the DEA, it also provides guidance and descriptions for other DoD requirements and their relationships. The primary information sources used to develop, revise, and update the DIAF are the UAF and Business Process Modeling Notation v2.0.

11.2. PURPOSE AND SCOPE. The DIAF is intended for an audience that understands, documents, and develops solutions to key mission requirements. The framework provides a baseline set of views used by modelers and analysts to describe how we define, create, update, and interpret requirements within the DEA. The DIAF defines how DCMA documents lines of effort, objectives, capabilities, and the combination of systems, exchanges, operational performers, and initiatives that enable them. It describes key concepts required to develop the set of baseline DEA viewpoints in support of Agency mission requirements to include the following:

- JCIDS
- JITC
- BEA
- AAF
- ICAM
- Zero Trust (ZT)
- Comply to Connect (C2C)

11.3. DIAF CONFORMANCE. DCMA has defined numerous processes supported by architectural descriptions. The architecture must also adhere to defined decision support processes mandated by the Agency, these processes include, but are not limited to, the DCMA BCF, CG, SE, the PPBE process, and IT PfM. These key support processes are designed to provide uniform, mandated, processes in critical decision-making areas and tailored to support those decisions-making requirements.

11.4. DIAF OBJECTIVE. The principal objective of the framework is to establish a standardized approach to present information that is understandable to stakeholder communities involved in developing, delivering, and sustaining capabilities in support of DCMA's mission.

The framework achieves this by segmenting the problem space into manageable views as defined by the DEA and DIAF baseline.

11.5. DCMA PROCESSES SUPPORTED BY THE FRAMEWORK. DCMA has defined numerous processes supported by architectural descriptions that must adhere to decision support processes mandated by the Agency. These processes include but are not limited to the DCMA BCF, SE, PPBE, and IT PfM. These key processes are intended to ensure compliance and support of critical decision-making.

a. **BCF.** DCMA's business capability framework is a set of contract management functions that support the Agency's strategic plan by capturing the results of daily, multi-functional activities that provide actionable insight into the Defense Acquisition Enterprise. The EA Program will provide input, collaborate with stakeholders, and coordinate with business partners to ensure architecture enhances the capabilities required to execute their assigned missions through:

- Negotiation Intelligence & Cost Evaluation (NICE)
- Product Acceptance & Proper Payment (PAPP)
- Contract Maintenance
- Contractor Effectiveness (CE)
- Acquisition Insight
- CG
- Organizational Infrastructure

b. **SE.** DoDI 5000.88 directs the PM to select the appropriate software development approach based on scope, requirements, schedule, and risk.

(1) The PM should consider an iterative software development process using modern agile development and operations methods.

(2) Assign a lead software engineer to manage the software acquisition team, software engineering processes, and delivery of code.

(3) The EA Program will support SE efforts by providing a structured approach to document design and development decisions based on established requirements.

c. **PPBE.** The EA Program will support DCMA's PPBE process by identifying the touch points between architecture, CPIC, and the PPBE process.

(1) Participates in the identification of the data to be captured within an Architectural Description.

(2) Facilitates informed decision-making and identify ways of presenting data to various stakeholders/roles in the PPBE decision process.

d. **IT PfM**. Each portfolio will be managed using the architectural plans, risk management techniques, capability goals and objectives, and performance measures to the greatest extent possible.

(1) The EA Program will use these architecture plans to support the definition of capability requirements.

(2) IT PfM uses the Architectural Description to analyze decisions on deployment or analysis of a needed capability.

(3) Architectural support to IT PfM tends to focus on the investment decision itself, and assists in justifying investments, evaluating the risk, and providing a capability gap analysis.

(4) The CPIC team continues to evolve the PfM approach with emphasis on individual systems and/or services designed to improve overall mission capability. The Agency's IT budget and management submissions are executed in three components. The Agency IT Portfolio Summary collects information on all Investments within the IT portfolio.

(5) Consistent with OMB CPIC guidance, DCMA will use the four continuous integrated activities to manage its portfolios – analysis, selection, control, and evaluation. The overall process is iterative with results being fed back into the system to guide future decisions.

e. **OPERATIONS.** The EA Program will capture enterprise routine, repeatable business and mission operations, and activities as architectural content. If an activity's structure is stable and repeated often, the design will include that structure as part of the Architectural Description. The EA repository will include templates, checklists, and other artifacts commonly used to support operational activities. The BCF, SE, PPBE, and IT PfM processes establish a knowledge-based approach, which requires PMs to attain the right knowledge at critical junctures to make informed program decisions throughout the acquisition process.

GLOSSARY

G.1. DEFINITIONS.

AAF. The AAF supports the DAS with the objective of delivering effective, suitable, survivable, sustainable, and affordable solutions to the end user in a timely manner. To achieve those objectives, MDAs, other Decision Authorities, and PMs have broad authority to plan and manage their programs consistent with sound business practice. The AAF acquisition pathways provide opportunities to develop acquisition strategies and employ acquisition processes that match the characteristics of the capability being acquired.

BCAC. This process seeks to develop and implement business/acquisition processes to acquire systems more efficiently. The process facilitates changes in the process through DOTmLPF-P to drive performance improvements, efficiencies, and effectiveness. The BCAC aligns commercial best practices and minimizes the need for customization of commercial products to the maximum extent possible. The BCAC is part of the DoDI 5000.75 and the DoDI 5000.02.

BCF. The official framework that comprises the senior level decision-making bodies in the Agency, and the approved venues for the proposal and review of initiatives, processes, programs, and policies that have agency-wide impact.

BEA. This is the Enterprise Architecture for the DoD Business Mission Area (BMA). The BEA guides and constrains implementation of interoperable DBS solutions as required by Title 10, Section 2222 of the United States Code (U.S.C.) by guiding system alignment to end-to-end processes. It also guides IT investment management to align with strategic business capabilities as required by the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 (3)), and supporting the OMB and the Government Accountability Office policies.

BPR. This is the practice of rethinking and redesigning the way work is done to achieve improvements in critical measures of performance – such as cost, quality and service – to better support an organization's mission. BPR enables organizations to shape a leaner, more integrated and simplified business environment that rapidly innovate and adapt to seamlessly address the needs of the Department.

C2C. A framework of tools and technologies operating throughout the network infrastructure to discover, identify, characterize, and report all devices connecting to the network. The C2C capability will orchestrate multiple tools to prevent non-compliant and unauthorized devices and personnel from connecting to the network, thus maintaining the secure configuration of the network and protecting the information in accordance with established standards and configurations.

DBS. An information system that is operated by, for or on behalf of the DoD, including a financial system, a financial data feeder system, a contracting system, a logistics system, a planning and budgeting system, an installations management system, a human resources management system or a training and readiness system.

DoD IE. The DoD information resources, assets, and processes required to achieve an information advantage and to share information across DoD and with mission partners.

ICAM. A set of security tools, policies, and systems that helps organizations manage, monitor, and secure access to their IT infrastructure. ICAM represents the combination of digital identities, credentials, and access controls into a single comprehensive approach. ICAM reduces the risk of cyber attacks to your organization by preventing unauthorized access to your networks, systems, and data.

JCIDS. The formal DoD process which defines acquisition requirements and evaluation criteria for future defense programs. JCIDS was created to replace the previous service-specific requirements generation system that allowed redundancies in capabilities and failed to meet the combined needs of all US military services. In order to correct these problems, JCIDS is intended to guide the development of requirements for future acquisition systems to reflect the needs of all four services by focusing the requirements generation process on needed capabilities as requested or defined by one of the US combatant commanders.

JIC. The primary sources for approved joint interoperability requirements are typically the Information Support Plan (ISP) and Capability Production Document (CPD), and, in some cases, the Capability Development Document (CDD). These documents, when approved, should contain the information needed to support a Joint Interoperability Certification (i.e., a certified NR KPP and the required architecture viewpoints).

JITC. The wing of the DoD that tests and certifies IT products for military use.

MDA. The MDA, with respect to a major defense acquisition program, means the official within the DoD designated with the overall responsibility and authority for acquisition decisions for the program, including authority to approve entry of the program into the next phase of the acquisition process.

UAF. Provides a means to develop an understanding of the complex relationships that exist between organizations, systems, and systems-of-systems that enable the analysis of these capabilities to ensure they meet the expectations of stakeholders.

ZT. A network security philosophy that states no one inside or outside the network should be trusted unless their identification has been thoroughly checked. ZT operates on the assumption that threats both outside and inside the network are an omnipresent factor, and also assumes that every attempt to access the network or an application is a threat. These assumptions inform the thinking of network administrators, compelling them to design stringent, trustless security measures.

GLOSSARY

G.2. ACRONYMS.

AAF	Adaptive Acquisition Framework
AR	Actual Resources Viewpoint
BCAC	Business Capability Acquisition Cycle
BCF	Business Capability Framework
BEA	Business Enterprise Architecture
BPR	Business Process Re-engineering
CAP BD	Capability Board
CEA	Chief Enterprise Architect
CG	Corporate Governance
CIO	Chief Information Officer
C2C	Comply to Connect
CPIC	Capital Planning Investment Control
DAS	Defense Acquisition System
DBS	Defense Business System
DEA	DCMA Enterprise Architecture
DIAF	DCMA Integrated Architecture Framework
DoDD	Department of Defense Directive
DoDAF	DoD Architecture Framework
DoDI	Department of Defense Instruction
DOTmLPF-P	Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, and Facilities and Policy
EA	Enterprise Architecture
EAR	Enterprise Architecture Review
IT	Information Technology
JCIDS	Joint Capability Integration and Development System
JIC	Joint Interopearbility Certification
JITC	Joint Interoperability Testing Command
MDA	Milestone Decision Authority
NICE	Negotiation Intelligence & Cost Evaluation
OMB	Office of Management and Budget
PfM	Portfolio Management
PM	Program Manager

PMOD	Process Management and Optimization Division
PPBE	Planning, Programming, Budgeting, and Execution
SE	Systems Engineering
SME	Subject Matter Expert
UAF	Unified Architecture Framework
ZT	Zero Trust

REFERENCES

Chairsman of the Joint Chiefd of Staff Instructions (CJCSI) 5123.01I, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," October 30, 2021
Clinger-Cohen Act of 1996 (40 U.S.C. 1401 (3))
DCMA Instruction 4401, "Information Technology Management," January 20, 2020
DCMA Manual 4401-16, "Capital Planning Investment Control," September 11, 2023
DCMA Instruction 4501, "Administration," February 23, 2019
DCMA Manual 4502-01, "Corporate Governance Structure and Procedures," July 22, 2019
DoD Directive 5000.01, "The Defense Acquisition System," September 9, 2020
DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013, as amended
DoD Directive 5135.02, "Under Secretary of Defense for USD(A&S)," July 17, 2020
DoD Directive 7045.20, "Capability Portfolio Management," June 21, 2019, as amended
DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020, as amended
DoD Instruction 5000.75, "Business Systems Requirements and Acquisition," February 2, 2017, as amended
DoD Instruction 5000.87, "Operation of the Software Acquisition Pathway," October 2, 2020
DoD Instruction 5000.88, "Engineering of Defense Systems," November 18, 2020
DoD Instruction 8330.01, "Interoperability of Information Technology, Including National Security Systems," September 27, 2022
Joint Capability Integration and Development System (JCIDS) Manual, "Manual for the Operation of the Joint Capabilities Integration and Development System," October 30, 2021
United States Code, Title 10