DoD INSTRUCTION 5000.97

DIGITAL ENGINEERING

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	December 21, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	Department of Defense Directive 5000.59, "DoD Modeling and Simulation (M&S) Management," August 8, 2007, as amended
Approved by:	Heidi Shyu, Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive 5137.02, this issuance establishes policy, assigns responsibilities, and provides procedures for implementing and using digital engineering in the development and sustainment of defense systems.

TABLE OF CONTENTS

FIGURE

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

a. The DoD will conduct a comprehensive engineering program for defense systems, pursuant to DoD Instruction (DoDI) 5000.88. In support of that effort, the DoD will use digital engineering methodologies, technologies, and practices across the life cycle of defense acquisition programs, systems, and systems of systems to support research, engineering, and management activities.

b. Digital engineering must be addressed in the acquisition strategy, including how and when digital engineering will be used in the system life cycle and expected benefits of its use. In addition, as specified in DoDI 5000.88, certain programs must include a digital engineering implementation plan in the systems engineering plan.

c. Digital engineering requires planning and providing financial and other resources for digital methods (e.g., model-based systems engineering (MBSE), product life-cycle management, computer aided design) in support of program activities to the maximum extent possible.

(1) Programs initiated after the date of this issuance will incorporate digital engineering for the capability in development unless the program's decision authority provides an exception.

(2) Programs initiated before the date of this issuance may incorporate digital engineering when it is practical, beneficial, and affordable, but are not required to do so.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (USD(R&E)).

The USD(R&E):

a. Establishes governing policy, advances practices, and develops workforce skills for digital engineering.

b. Oversees the implementation of digital engineering in the technical activities for which they are responsible, including:

(1) Developmental test and evaluation.

(2) Engineering.

(3) Hardware and software assurance.

(4) Human systems integration.

(5) Reliability and maintainability.

(6) Manufacturing and quality.

(7) Modeling and simulation.

(8) Modular open systems approach.

(9) Resilient systems.

(10) Software development.

(11) System safety.

(12) System security engineering.

c. Coordinates with the DoD Components to plan, implement, and support digital engineering capabilities.

d. Leads and coordinates efforts to define digital engineering data standards.

e. Establishes digital engineering guidance, including guidance published on the Digital Engineering, Modeling, and Simulation Body of Knowledge Website available at https://de-bok.org.

2.2. DIRECTOR, DEPARTMENT OF DEFENSE TEST RESOURCE MANAGEMENT CENTER (TRMC).

Under the authority, direction, and control of the USD(R&E) and in addition to the responsibilities in Paragraph 2.7., the Director, DoD TRMC:

a. Develops and maintains a core DoD-wide digital engineering infrastructure capability, methodologies, and practices to support acquisition programs.

b. Develops and maintains the methodology for distributed developmental testing which may be necessary to support digital engineering capabilities.

2.3. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT.

Pursuant to DoD Directive 5135.02 and DoDI 5010.44, the Under Secretary of Defense for Acquisition and Sustainment:

a. Serves as the senior DoD official overseeing development and implementation of DoD intellectual property policy and guidance for DoD acquisition which is necessary to support digital engineering capabilities.

b. Serves as the lead for the adaptive acquisition framework pathways that govern defense acquisition programs in accordance with DoDI 5000.02.

c. Supports the development of Defense Acquisition University training and education, pursuant to DoDI 5000.57, required to ensure the DoD workforce has the appropriate knowledge, skills, and abilities to understand and conduct digital engineering activities.

2.4. DIRECTOR OF OPERATIONAL TEST AND EVALUATION.

In accordance with Section 139 of Title 10, United States Code, the Director of Operational Test and Evaluation supports the development of practices for the use of digital engineering to achieve operational test and evaluation and live fire test and evaluation objectives (see DoD 5000.89 for more information on operational test and evaluation and live fire test and evaluation).

2.5. DOD CHIEF INFORMATION OFFICER.

Pursuant to DoD Directive 5144.02, the DoD Chief Information Officer:

a. Guides modernization for digital capabilities across the DoD to ensure digital engineering efforts are aligned to DoD modernization efforts.

b. Supports the development and application of practices for the use of digital engineering for information technology-based systems under their purview.

c. Provides risk management framework and process guidance to design engineers in the DoDI 8510.01 to assist them with guiding their customers in attaining systems authorizations such as an authority to operate.

2.6. CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER.

In accordance with the authority in the December 8, 2021 and February 1, 2022 Deputy Secretary of Defense memorandums, the Chief Digital and Artificial Intelligence Officer:

a. Leads and oversees the DoD's strategy development and policy formulation for data, analytics, and artificial intelligence (AI).

b. Works to break down barriers to data sharing and AI adoption within appropriate DoD institutional processes.

c. Creates digital infrastructure and services that support DoD Component development and deployment of data, analytics, and AI.

2.7. DOD COMPONENT HEADS WITH ACQUISITION AUTHORITY.

The DoD Component heads with acquisition authority:

a. Implement the procedures outlined in this issuance.

b. Support the development of Component policy, practice, and workforce competency for digital engineering.

c. Designate an official or office to serve as the focal point for their respective DoD Component's digital engineering activities.

d. Plan, implement, and support digital engineering capabilities.

e. Through their acquisition executive(s):

(1) Guide their acquisition programs' incorporation of digital engineering practices into their system requirements, cost, business, development, testing, evaluation, production, and sustainment efforts.

(2) Provide guidance and support for program managers (PMs) to develop, validate, and maintain:

(a) Credible and coherent authoritative sources of truth shared with stakeholders.

(b) Digital models that accurately reflect the architecture, attributes, and behaviors of the system they represent.

(3) Approve exceptions to the use of digital engineering for programs for which they are the decision authority.

SECTION 3: DESCRIPTION, IMPLEMENTATION, AND PROCEDURES

3.1. DIGITAL ENGINEERING.

Digital engineering is a means of using and integrating digital models and the underlying data to support the development, test and evaluation, and sustainment of a system. The June 2018 DoD Digital Engineering Strategy describes how the application of digital engineering can modernize how the DoD designs, develops, delivers, operates, and sustains systems. Digital engineering:

a. Is a critical practice necessary to support acquisition and sustainment in an environment of increasing global challenges, complexity, dynamic threats, rapidly evolving technologies, supply instability, and increasing life expectancy of DoD systems currently in operation.

b. Expands on engineering practices to take full advantage of computation, visualization, and collaboration to enable faster, smarter, data-driven decisions throughout the system life cycle. Digital engineering should enable faster, higher-quality decision making in weapon system design, development, testing, fielding, and sustainment. These improved decision operations will enable more rapid delivery of warfighting capabilities to the field.

c. Uses computer systems for the development, verification, validation, use, curation, configuration management, and maintenance of technically accurate digital models in support of system life-cycle activities. These models capture system representations and, together with their underlying data, provide an authoritative source of truth to stakeholders.

d. Moves the primary means of communicating system information from documents to digital models and their underlying data. Digital models become ubiquitous and central to how engineering activities are performed.

3.2. DIGITAL ENGINEERING CAPABILITY.

a. Digital Engineering Capability Requirements.

To help programs successfully implement digital engineering, the DoD will iteratively develop a digital engineering capability that supports the direction provided in Section 231 of Public Law 116-92. This approach will leverage digital engineering capabilities from the DoD, the DoD Components, and program offices. This digital engineering capability will:

(1) Be accessible to, and usable by, individuals and organizations throughout the DoD who have responsibilities relating to requirements, architecture, capability design, development, testing, evaluation, operation, training, production, and sustainment of emerging, new, and existing systems.

(2) Connect the phases of the acquisition life cycle, allowing feedback and flow of information across acquisition activities and processes.

(3) Provide for the development, verification, validation, use, curation, configuration management, and maintenance of technically accurate digital systems and models of systems, subsystems, and their components, at the appropriate level of fidelity to ensure test activities adequately simulate the environment in which a system will be deployed.

(4) Include development, security, and operations (DevSecOps) and test infrastructure, processes, and software to automate testing, data reduction and analysis, and software distribution throughout the system life cycle to support:

(a) The developmental and operational testing community's verification and validation of system, system-of-system, and operational requirements in accordance with DoDI 5000.89.

(b) Automated and non-automated security testing, including vulnerability scanning and penetration testing, as well as threat-based exploitations and assessments that assume advanced data security methods (e.g., zero trust (ZT)) are being used to secure the system being tested.

(c) Distribution and installation of software to the operating environment on a time-bound, repeatable, frequent, and iterative basis.

(5) Be operated within an appropriately secure ecosystem that uses policy, standards, and best practices to ensure the confidentiality, integrity, and availability of the digital engineering capability and underlying data.

(a) There are increased risks associated with aggregating information in digital engineering environments and with encouraging sharing of that information, including potential risks to individual privacy.

(b) Ecosystems must be secured with advanced data security methods (e.g., ZT) and comply with applicable privacy requirements, including Section 552a of Title 5, United States Code, also known as the Privacy Act of 1974, as amended, and DoDIs 5400.11 and 5400.16, if the environment will collect, generate, maintain, use, or share personally identifiable information.

(6) Comply with operational security requirements in accordance with DoD Directive 5205.02E.

(7) Support the DoD Data Strategy goal of making data visible, accessible, understandable, linked, trustworthy, interoperable, and secure.

b. Digital Engineering Capability Elements.

The digital engineering capability will consist of integrated elements (see Figure 1). These elements include:

(1) Digital Engineering Ecosystem.

(a) A digital engineering ecosystem includes the infrastructure and architecture necessary to support automated approaches for system development, design, testing, evaluation, production, operation, training, and sustainment throughout the defense acquisition process. The infrastructure consists of the following digital engineering ecosystem assets:

1. Hardware.

2. Software.

3. Networks (including cloud services).

4. Tools.

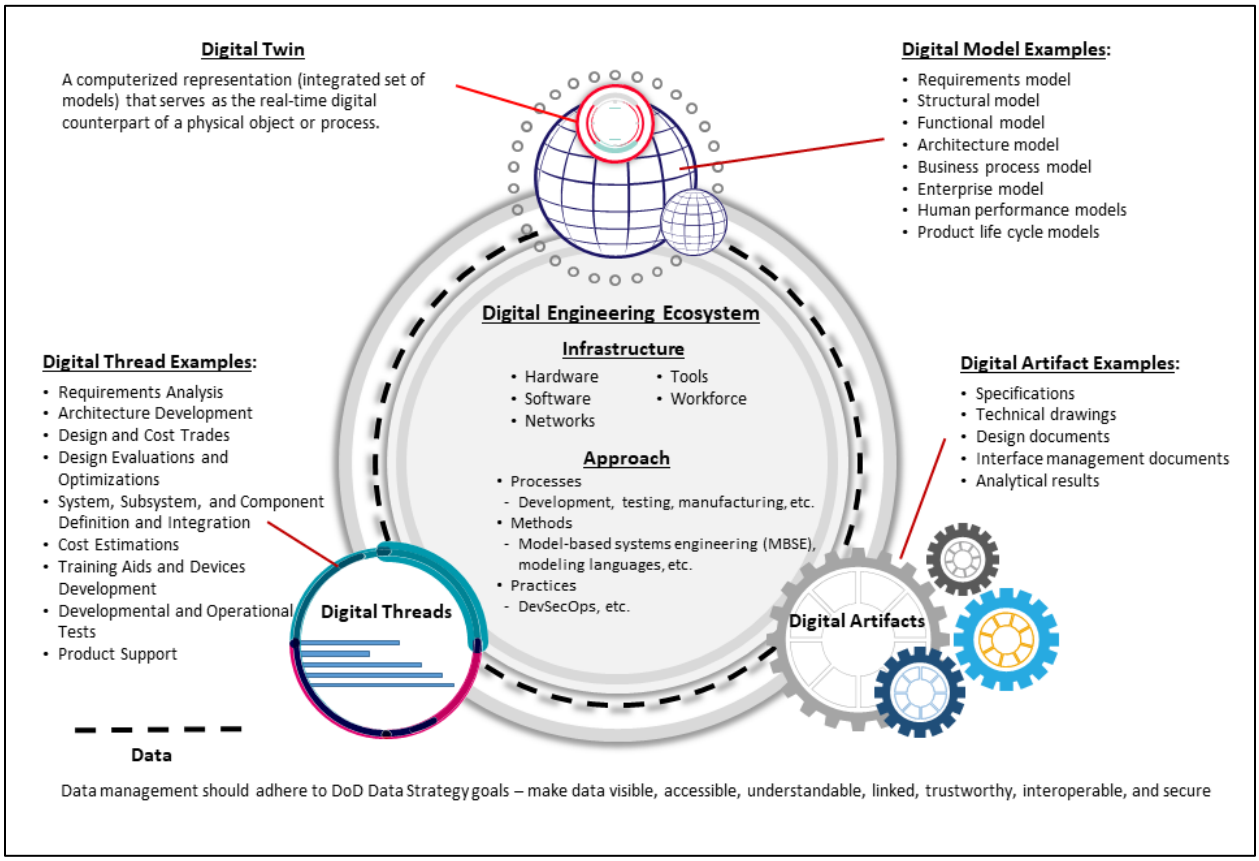
5. Workforce.

(b) Digital engineering ecosystem assets may be provided by the DoD, the DoD Components, or program offices.

(c) A digital engineering ecosystem includes stakeholder approaches to digital engineering. These approaches include the processes, methods, and practices necessary to conduct digital engineering. The approaches are the basis for accomplishing engineering activities and generating knowledge through digital threads and in the form of digital artifacts by extracting information from digital models. These digital engineering approaches and the larger digital engineering ecosystem provide a feedback mechanism for stakeholders and contributors to the authoritative source of truth.

(d) A digital engineering ecosystem may include, but is not limited to, government-to-government, contractor-to-government, and contractor-to-supplier digital collaboration. These collaborative digital environments are key to involving all stakeholders in developing models, executing simulations, and performing analysis and optimizations for the digital models or digital twins. In some instances, customers, regulators, contractors, suppliers, or operators must be integrated into the digital engineering ecosystem to complete the digital thread.

Figure 1. Digital Engineering Framework



(2) Digital Models (Including Digital Twins).

(a) Modeling is essential to understanding complex systems and system interdependencies and to communicate among team members and stakeholders. Simulations and analysis provide a means to explore concepts, system characteristics, and alternatives; facilitate informed decisions; and assess overall system performance. Modeling and simulation that integrates all relevant real-world data is the basis for the authoritative source of truth.

(b) Configuration control must be maintained on digital models and digital twins. Digital models, including their information and data, should be traceable from operational capabilities through requirements, design constructs, production, test, training, and sustainment. The use of this data should be considered during the program planning and the acquisition and contracting phases of the system's life cycle to ensure the appropriate data rights are obtained and the system will remain functional, sustainable, upgradable, and affordable. Programs should verify and validate the baseline(s) of digital model(s) before technical milestones. Digital model types include, but are not limited to:

1. Requirements models.

2. Structural models.

3. Functional models.

4. Business process models.

5. Architecture models.

6. Enterprise models.

7. Physics-based models.

8. Human performance models.

9. Threat models.

10. Product life cycle models.

(c) A digital twin is a virtual representation of a product, system, or process that uses the best available models, sensor information, data collected from the physical system, and input data to mirror and predict system activities and performance over the life of its corresponding physical twin and inform system design changes over time. There can be multiple digital twins of a system, but all digital twins should be based on authoritative sources of information and have clearly defined uses and scopes. Digital twins may vary in fidelity, based on the use case.

(3) Digital Threads.

(a) A digital thread should be an extensible and configurable analytical framework. The digital thread should seamlessly advance the controlled interplay of technical data, software, information, and knowledge in the digital engineering ecosystem. Digital threads are used to connect authoritative data and orchestrate digital models and information across a system's life cycle. The digital thread informs decision makers throughout a system's life cycle by providing the capability to access, integrate, and transform data into actionable information. The digital thread should also support the feedback loop over the life cycle.

(b) The digital thread allows different audiences with different perspectives to extract data from and adjust usage of models to carry out different activities, including, but not limited to:

1. Requirements analysis.

2. Architecture development.

3. Design evaluation and optimization.

4. System, subsystem, and component definition and integration.

5. Cost estimating.

6. Training aids and devices development.

7. Developmental and operational tests.

8. Product support and sustainment through disposal.

9. Air worthiness.

10. Nuclear certification.

(4) Digital Artifacts.

Digital artifacts are the digital products and views that can be dynamically generated directly from digital models. These artifacts are created from the standards, rules, tools, and infrastructure within a digital engineering ecosystem. Some common examples of digital artifacts include, but are not limited to:

(a) Design specifications.

(b) Technical drawings (e.g., authorization boundaries, data flows).

(c) Design documents.

(d) Interface management documents.

(e) Analytical results.

(f) Bills of material.

(g) Software source code.

(h) Work breakdown structure.

(i) Production or machining instructions.

(j) Test planning and cases.

(k) Schedules.

(l) Product support strategy.

(m) Data flow diagrams.

3.3. DIGITAL ENGINEERING TRAINING AND GUIDANCE.

a. As part of an ongoing effort with the Defense Acquisition University, the DoD workforce will have access to training and education to use digital engineering concepts. The DoD workforce training will include an understanding of digital engineering principles (e.g., MBSE, modeling languages), awareness of the available digital engineering capabilities, and the use of the digital engineering capabilities.

b. DoD Components may provide digital engineering training as appropriate. This training may be developed organically within a DoD Component or supplied by external sources.

c. PMs, systems engineers, life-cycle logisticians, acquisition intelligence analysts, and testers may use the Digital Engineering, Modeling, and Simulation Body of Knowledge Website as a guide when implementing digital engineering procedures within their programs.

d. The USD(R&E) will periodically reevaluate training, policy, and guidance to better integrate digital engineering across the entire acquisition life cycle and the associated policies.

3.4. IMPLEMENTATION OF DIGITAL ENGINEERING.

a. The PM must implement digital engineering procedures as early in program planning as possible and across the system life cycle.

(1) Major Capability Acquisition.

At each milestone defined in DoDI 5000.85, the PM will present the digital engineering approach for the program.

(2) Middle Tier of Acquisition.

For programs utilizing the middle tier of acquisition pathway pursuant to DoDI 5000.80, the PM will implement a digital engineering approach to the maximum extent possible. Middle tier of acquisition programs may need to address digital engineering use in preparation for transition to the major capability acquisition pathway or another appropriate adaptive acquisition framework pathway.

(3) Software Acquisition.

During the planning phase defined in DoDI 5000.87, the PM will develop plans for the use of digital engineering procedures. During the execution phase, the PM will implement the planned digital engineering approach to the maximum extent possible.

(4) Defense Business Systems Acquisition.

At each authority-to-proceed decision point defined in DoDI 5000.75, the PM will report on the status of the implementation of digital engineering procedures to the program decision authority.

(5) Urgent Capability Acquisition.

For programs utilizing the urgent capability acquisition pathway pursuant to DoDI 5000.81, the PM will assess whether tailored digital engineering procedures in design, testing, and acceptance best meet the urgent need or reduce acquisition risk.

(6) Acquisition of Services.

For programs utilizing the acquisition of services pathway pursuant to DoDI 5000.74, the PM will implement digital engineering procedures to the maximum extent possible. Programs using acquisition of services may need to identify digital models and the data output from those models during execution of contracted services.

b. The PM will identify and require digital models, artifacts, and data sets as deliverables in the contract through contract data requirements lists and data item descriptions. The PM will ensure contracts provide the DoD with intellectual property rights in the digital models and artifacts that are in accordance with the program's intellectual property strategy (see DoDI 5010.44 for more information on the intellectual property strategy) and intellectual property management plan for product support (see DoDI 5000.91 for more information on product support) to ensure the system(s) will remain functional, sustainable, upgradable, and affordable throughout the system life cycle.

c. The PM will consider implementing the following key elements (see Paragraph 3.2.b. for additional details) as appropriate and document the use (or non-applicability) of each in the acquisition strategy and, where appropriate, in the systems engineering plan:

(1) Digital engineering ecosystem (e.g., architectures, data infrastructures, computing capabilities, and use of available DoD shared resources).

(2) Digital models, including digital twins.

(3) Digital threads.

(4) Digital artifacts.

d. The DoD is making major investments in developing an infrastructure to support digital engineering capabilities. PMs should use existing DoD or Military Service-level digital engineering resources to the maximum extent possible before investing in new digital engineering capabilities.

(1) The DoD TRMC is investing in the Joint Mission Environment Test Capability, which provides core digital engineering infrastructure components for PMs to use in their digital engineering ecosystems. The Joint Mission Environment Test Capability includes DevSecOps capabilities, integration services, and enterprise network connectivity at any classification level built on top of the Defense Research and Engineering Network.

(2) The DoD TRMC is investing in the National Cyber Range Complex (NCRC), which provides a high-fidelity, realistic cyber environment in which to conduct sophisticated cyber activities during all phases of the system life cycle. The NCRC can support:

(a) Security testing that includes vulnerability scanning and penetration testing, including threat-based red team exploitations and assessments that assume advanced data security methods (e.g., ZT) are being used to secure the system being tested.

(b) Red team testing. Use of the NCRC does **not** meet the need for adversarial assessments unless a National Security Agency-certified red team is employed.

(3) When selecting and maintaining an infrastructure, PMs should consult with their DoD Component and consider enterprise solutions. PMs should consider the need and resources required for:

(a) A secure high-speed network with efficient and automated network configuration and management capabilities to support multilevel classification environments.

(b) Common tools that provide an understanding of activities occurring within the digital engineering ecosystem.

(c) Interoperability and ease of integrating components together within the digital engineering ecosystem.

(d) Knowledge management, analysis, and evaluation capabilities that leverage the latest industry tools and techniques and promote sharing data across organizations and system life-cycle activities.

(e) Access to advanced digital technologies (including DevSecOps infrastructure), software licenses, and applications.

(f) Test and evaluation across system-of-systems interfaces with emulated communications or actual interoperability across those interfaces.

(g) Protection of information and technology in accordance with DoDIs 5000.83, 8500.01, and 8510.01. Due to the aggregation of program information in digital engineering environments, PMs must work with their DoD Components to identify and implement advanced security methodologies (e.g., ZT).

3.5. PROCEDURES FOR MAINTAINING DIGITAL MODELS AND AUTHORITATIVE DATA SOURCES.

a. Digital Models.

(1) Programs will identify and maintain model-centric baselines, approaches, and applications in a digital form that integrates the technical data and associated digital artifacts that stakeholders generate throughout the system life cycle. The program should develop digital model(s) using standard and best practice model representations, methods, and underlying data structures to maximize interoperability.

(2) Programs should establish a standard approach for developing each type of digital model. Programs should consider the use of existing modeling standards and approaches to improve integration of models across the DoD. Programs must evaluate all digital models to ensure they are accurate, complete, trusted, and reusable. Programs will develop digital models in accordance with applicable DoD policies, guidance, and standards. Programs should

reference the Acquisition Streamlining and Standardization Information System (available at https://assist.dla.mil/online/start/) and DoD Information Technology Standards Registry repositories as government-adopted authoritative sources of truth for standards.

(3) Programs will update and maintain the digital model(s) throughout the system life cycle and maintain configuration management (i.e., version control). These updates, conducted within the digital models, will provide program stakeholders, including digital model developers, simulation users, testers, and other engineering and program management personnel, with the ability to extract and analyze consistent and up-to-date system information. Digital models and simulations must be updated using all relevant real-world data throughout the system life cycle since they will be used to make decisions, inform manufacturing, generate software code, etc.

(4) Programs will ensure digital models, simulations, and associated data are verified, validated, and accredited for their intended use, in accordance with DoDI 5000.61.

b. Authoritative Data.

Programs should develop and implement plans to establish current, consistent, enduring, and authoritative sources of truth for digital models and data. See the DoD Data Strategy for additional information on data attributes, including achieving visible, accessible, understandable, linked, trustworthy, interoperable, and secure goals.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AI	artificial intelligence
DevSecOps	development, security, and operations
DoDI	DoD instruction
MBSE	model-based systems engineering
NCRC	National Cyber Range Complex
PM	program manager
TRMC	Test Resource Management Center
USD(R&E)	Under Secretary of Defense for Research and Engineering
ZT	zero trust

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
analytical framework	A structured and logical approach that serves as a foundation and starting point for conducting data analysis.
authoritative source of truth	The reference point for models and data across the system life cycle. The authoritative source of truth provides traceability as the system evolves, capturing historical knowledge and connecting configuration controlled versions of models and data.
configuration management	Defined in the Defense Acquisition University Glossary.
data attributes	The quantitative or qualitative characteristics of a data element.

TERM	DEFINITION
digital artifact	A product or output, in computer (i.e., digital) format, created within or generated from the digital engineering ecosystem. Digital artifacts provide data for alternative views to visualize, communicate, and deliver data, information, and knowledge to stakeholders.
digital engineering	Defined in the Defense Acquisition University Glossary.
digital engineering capability	The ability to develop, validate, use, curate, and maintain technically accurate digital systems and models of systems, subsystems, and their components, at the appropriate level of fidelity to ensure test activities adequately simulate the environment in which a system will be deployed.
digital engineering ecosystem	Defined in the Defense Acquisition University Glossary.
digital model	A digital (i.e., in an electronic form, able to be read and manipulated by computer) representation of an object, phenomenon, process, or system. The representation can include form, attributes, and functions and may be depicted visually or described via mathematical or logical expressions.
digital thread	An extensible and configurable analytical framework that seamlessly expedites the controlled interplay of technical data, software, information, and knowledge in the digital engineering ecosystem, based on the established requirements, architectures, formats, and rules for building digital models. It is used to inform decision makers throughout a system's life cycle by providing the capability to access, integrate, and transform data into actionable information.
digital twin	A computerized representation (integrated set of models) that serves as the real-time digital counterpart of a physical object or process.
extensible	Capable of being extended, particularly to add new capabilities and functionality.
logical expressions	A statement that evaluates to true or false.
MBSE	The formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout development and later system life-cycle phases.

TERM	DEFINITION
model	Defined in the Defense Acquisition University Glossary.
modeling language	A set of rule-based graphical or text expressions used to communicate the form, attributes, and functions of an object, process, phenomenon, or system.
modular open systems approach	An acquisition and design strategy consisting of a technical architecture that uses system interfaces compliant with widely supported and consensus-based standards (if available and suitable). The strategy supports a modular, loosely coupled and highly cohesive system structure that allows severable system components at the appropriate level to be incrementally added, removed, or replaced throughout the life cycle of a system platform to afford opportunities for enhanced competition and innovation.
penetration testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system, in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 5.
personally identifiable information	Defined in Office of Management and Budget Circular No. A-130.
red team	An ad-hoc organizational element that provides an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others.
simulation	Defined in the Defense Acquisition University Glossary.
user	The human(s) who operates, maintains, trains, and supports the equipment, system, or facility. Includes the definition of "end user" in DoDI 5000.87.
ZT	Defined in the Defense Acquisition University Glossary.

REFERENCES

aDefense Acquisition University Glossary

Deputy Secretary of Defense Memorandum, "Establishment of the Chief Digital and Artificial Intelligence Officer," December 8, 2021

Deputy Secretary of Defense Memorandum, "Initial Operating Capability of the Chief Digital and Artificial Intelligence Officer," February 1, 2022

Digital Engineering, Modeling, and Simulation Body of Knowledge Website, https://de-bok.org

Department of Defense, "Data Strategy," October 2020

DoD Digital Engineering Strategy, June 2018

DoD Directive 5135.02, "Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))," July 15, 2020

DoD Directive 5137.02, "Under Secretary of Defense for Research and Engineering (USD(R&E))," July 15, 2020

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended

DoD Information Technology Standards Registry Website, https://gtg.csd.disa.mil/disr/dashboard.html[1]

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020, as amended

DoD Instruction 5000.57, "Defense Acquisition University (DAU)," December 18, 2013, as amended

DoD Instruction 5000.61, "DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)," December 9, 2009, as amended

DoD Instruction 5000.74, "Defense Acquisition of Services," January 10, 2020, as amended

DoD Instruction 5000.75, "Business Systems Requirements and Acquisition," February 2, 2017, as amended

DoD Instruction 5000.80, "Operation of the Middle Tier of Acquisition (MTA)," December 30, 2019

DoD Instruction 5000.81, "Urgent Capability Acquisition" December 31, 2019

DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020, as amended

DoD Instruction 5000.85, "Major Capability Acquisition", August 6, 2020, 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 5000.89, "Test and Evaluation," November 19, 2020

[1] Available to individuals with common access cards.

DoD Instruction 5000.91, "Product Support Management for the Adaptive Acquisition Framework," November 4, 2021

DoD Instruction 5010.44, "Intellectual Property (IP) Acquisition and Licensing," October 16, 2019

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

National Institute of Standards and Technology Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020

Office of Management and Budget Circular No. A-130, "Managing Information as a Strategic Resource", July 28, 2016

Public Law 116-92, Section 231, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019

United States Code, Title 5, Section 552a (also known as the "Privacy Act of 1974"), as amended

United States Code, Title 10, Section 139