DoW Instruction 8430.01

Accelerated Mission Software

Originating Component:	Office of the DoW Chief Information Officer
Effective:	September 8, 2026
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Approved 08/31/2026 by:	Kirsten A. Davies, DoW Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02 and DoDD 8000.01, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for software modernization and management within the DoW to maximize lethality in an era of software-defined warfare.
- Promotes reusing software to achieve efficiencies and accelerate capability delivery pursuant to Public Law 118-187.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to:

(1) OSW, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of War, the Defense Agencies, the DoW Field Activities, and all other organizational entities within the DoW (referred to collectively in this issuance as the "DoW Components").

(2) All software throughout its lifecycle, excluding software developed under Budget Activity 1-Basic Research, Budget Activity 2-Applied Research, Budget Activity 3-Advanced Technology Development, or Budget Activity 4-Advanced Component Development and Prototypes funding categories as defined in DoD 7000.14-R. If such excluded software transitions into acquisition or operational use, this issuance applies.

(3) Acquisition and non-acquisition programs containing software, including national security systems within DoW authorities and defense business systems, regardless of dollar value.

(4) Special access program (SAP) information technology (IT), with further guidance provided in the Joint SAP Implementation Guide or successor.

b. Nothing in this issuance alters or supersedes the existing Director of National Intelligence authorities and policies on protecting Intelligence Community information systems in accordance with Executive Order 12333 and other applicable laws and regulations.

1.2. POLICY.

Software is a strategic asset to be managed as an enduring capability throughout its lifecycle, enabling the timely delivery of warfighting capabilities and advanced technologies such as artificial intelligence (AI). The DoW continuously modernizes, manages, and governs software.

a. Modernize.

DoW software development and deployment efforts:

(1) Employ modern, secure, and human-centric software principles and practices, such as those used in Agile and development, security, and operations (DevSecOps), to rapidly translate operational needs into working production software solutions.

(2) Employ software engineering best practices with measurable and testable requirements that are traceable to mission critical functions, including requirements for

cybersecurity, cyber resilience, and zero trust suitability, to ensure continuous alignment with mission objectives and effective performance evaluations throughout the lifecycle.

(3) Incorporate software component analysis, telemetry, observability, and automated monitoring to support proactive maintenance, rapid vulnerability mitigation, software supply chain risk management, responsiveness to user needs, and adaptation to evolving mission and threat environments.

(4) Prioritize using existing software, components, frameworks, and platforms; open-source software; and commercial-off-the-shelf (COTS) and software-as-a-service (SaaS) solutions before developing or acquiring new capabilities to achieve efficiencies and accelerate delivery.

(5) Before software development, examine business processes to improve, reengineer, or rationalize workflows, maximizing the benefits of technology insertion and automation.

b. Manage.

The DoW manages software assets in accordance with DoDD 8115.01; DoD Instructions (DoDIs) 5000.76 and 8115.02 and DoW Instruction (DoWI) 8000.02; and Public Law 118-187 to maintain accountability of software throughout its lifecycle, supporting portfolio management, investment decision making, and cybersecurity.

c. Govern.

The Software Modernization Senior Steering Group, or its successor, guides and facilitates the adoption of modern software development practices as the senior executive decision body for software modernization in accordance with the February 1, 2022 Deputy Secretary of Defense Memorandum.

SECTION 2: RESPONSIBILITIES

2.1. DOW CHIEF INFORMATION OFFICER (CIO).

The DoW CIO:

a. In coordination with the Under Secretary of War for Research and Engineering (USW(R&E)) and the Under Secretary of War for Acquisition and Sustainment (USW(A&S)):

(1) Establishes policies and provides procedures to continuously modernize and manage software within the DoW across its lifecycle.

(2) Establishes and evolves DoW-wide architecture and standards to guide software modernization, incorporating modular delivery, Agile and DevSecOps practices, and interoperability between current and legacy components.

(3) Prescribes reference designs, standards, and data requirements to ensure consistent quality and measurable impact of software and software platforms, factories, and continuous integration/continuous deployment (CI/CD) pipelines.

b. Establishes cybersecurity standards and zero trust acceptance criteria to continuously operate software platforms and factories.

c. Manages requirements for the DoW software asset inventory in accordance with DoDD 8115.01; DoDIs 5000.76 and 8115.02 and DoWI 8000.02; and Public Law 118-187.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA).

Under the authority, direction, and control of the DoW CIO, and in addition to the responsibilities in Paragraph 2.8., the Director, DISA:

a. Provides capabilities to DoW Components that enable software delivery such as DevSecOps platforms, infrastructure-as-code, and cloud management services.

b. Manages the provisional authorization process and issues provisional authorizations for cloud service offerings.

c. Develops and manages repositories for software assets in accordance with DoW CIO requirements and DoDD 8115.01; DoDIs 5000.76 and 8115.02 and DoWI 8000.02; and Public Law 118-187.

2.3. USW(R&E).

The USW(R&E):

a. Establishes policy and provides guidance, procedures, and workforce competency for DoW research, engineering, quality, reliability, human systems integration, system safety, prototyping, experimentation, development test and evaluation (DT&E), and software assurance.

b. Establishes system security engineering and software assurance policy and guidance to protect systems and technologies from adversarial software exploitation and compromise in accordance with DoDI 5000.83.

c. Establishes guidance, standards, mitigations, education, and training for protecting software that provides mission critical functions or is identified as a critical component in accordance with DoDI 5200.44.

d. Advances modern software engineering practices through research, technology development, and engineering pilots.

e. Provides and curates authoritative digital engineering environments for software systems.

f. Establishes methods to validate models against operational data in coordination with the Director of Operational Test and Evaluation (DOT&E), including safety-critical behaviors where applicable.

g. In coordination with the DoW CIO and the USW(A&S), defines and promotes common data and automation standards that enable CI/CD pipelines and continuous authorization in accordance with DoDI 8310.01, ensuring pipeline and authorization artifacts are consumable by risk management processes and United States Cyber Command cyber defense operations.

h. Establishes guidance for AI and machine learning integration in software in accordance with applicable National Institute of Standards and Technology (NIST) guidelines, frameworks, and standards, with attention to assurance, safety, and risk management.

i. In coordination with the USW(A&S), accelerates transitioning software technologies, prototypes, and engineering practices into scalable programs and promotes reuse via authorized DevSecOps platforms and modular open systems.

j. Defines software engineering and system security engineering work roles and validates the knowledge, skills, abilities, and tasks required for the roles in accordance with DoDD 8140.01, DoDI 8140.02, and DoD Manual (DoDM) 8140.03, as applicable.

k. In coordination with the USW(A&S), develops and maintains applicable Warfighting Acquisition University credentials (e.g., software engineering, AI, digital engineering) for continuous learning and professional development.

2.4. USW(A&S).

The USW(A&S):

a. Establishes and evolves software acquisition pathway policies, procedures, and guidance to streamline acquisition and incorporate modern software development practices, cybersecurity, and safety approaches in accordance with cybersecurity and assurance policies for accelerated, secure, and safe delivery of software capabilities to the warfighter.

b. Issues acquisition policy for DoW Components requiring secure software development, safety, and supply chain assurance in accordance with DoDI 5200.44 to enable continuous monitoring.

c. Strengthens continuous software delivery by aligning budget and contracting, facilitating continuous delivery, and by supporting software asset management, enterprise sourcing, and license rationalization.

d. Prepares the acquisition workforce for software by providing resources and lessons learned and by updating Warfighting Acquisition University curricula, credentials, and communities of practice on topics related to software acquisition.

2.5. UNDER SECRETARY OF WAR FOR INTELLIGENCE AND SECURITY (USW(I&S)).

The USW(I&S):

a. In coordination with the DoW CIO, the USW(R&E), and the USW(A&S), establishes policy and provides guidance for applying this issuance to the Defense Intelligence Enterprise, national security systems, SAPs, and other sensitive activities.

b. Ensures software development practices for software activities involving intelligence data or missions are aligned with intelligence oversight, counterintelligence, and DoW security requirements.

c. Directs all-source intelligence and counterintelligence analysis of information and communications technology supply chain threats and ensures methods for sharing threat information are integrated into development processes in accordance with DoDI 5200.44.

2.6. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the USW(I&S); under the authority, direction, and control exercised by the DoW CIO over the activities of the Cybersecurity Directorate of the National Security Agency funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.8., the Director, National Security Agency/Chief, Central Security Service:

a. Advises DoW Components on advanced cybersecurity practices, cryptographic standards, and methods to mitigate software vulnerabilities.

b. Defines technical standards for security test and validation of software intended for use in national security systems.

2.7. DOT&E.

The DOT&E:

a. Establishes policy and provides procedures for conducting operational test and evaluation (OT&E) and oversees designated programs in accordance with Sections 139, 4171, and 4172 of Title 10, United States Code (U.S.C.).

b. Monitors, reviews, and independently reports on all OT&E and live fire test and evaluation activities and resources for DoW systems under DOT&E oversight.

c. In coordination with the USW(R&E), the USW(A&S), the DoW CIO, and the DoW Component heads, evolves test and evaluation (T&E) policies, procedures, and capabilities to accommodate iterative software development and incorporate automation, digital engineering, and software safety assurance in the OT&E and live fire test and evaluation of warfighting capabilities.

d. Requires testers to conduct operational evaluations that are integrated with CI/CD pipelines; plan tests early; observe development; and accept validated automated test artifacts, security scans, performance data, and operational telemetry as test evidence of sufficient operational fidelity.

e. Leverages data generated from continuous monitoring, adversarial testing, and cyber ranges to inform operational evaluations of mission risk and resilience.

f. Ensures that test infrastructure, data standards, and continuous evaluation enable timely sharing of operational test data and findings for continuous improvement while protecting sensitive information.

2.8. DOW COMPONENT HEADS.

The DoW Component heads:

a. Provide direction and resources within their respective Components to implement this issuance, ensuring software is modernized and managed as an enduring capability throughout its lifecycle.

b. Operate secure, automated CI/CD pipelines to continuously integrate, test, secure, and deliver software, treating such pipelines as critical infrastructure that must be authorized, monitored, and protected commensurate with mission impact.

c. Design software using a modular open systems approach (MOSA) to maximize interoperability and portability in accordance with Section 4401 of Title 10, U.S.C.

d. Use government-off-the-shelf (GOTS), COTS, or SaaS solutions before developing new non-commercial software and leverage freely licensed open-source software before buying commercially supported open source or proprietary offerings.

e. Procure software using DoW enterprise agreements, including core enterprise technology agreements, DoW enterprise software agreements, and joint enterprise licensing agreements unless mission or cost dictate otherwise in accordance with DoWI 8000.02.

f. Produce verifiable assurance evidence, including static and dynamic code analysis, fuzz testing, penetration testing, and secure-code reviews, and employ continuous authorization strategies that integrate cybersecurity and test activities from inception through development and deployment.

g. Ensure that:

(1) Software that provides a mission critical function or is a critical component in accordance with DoDI 5200.44, is protected to a level of assurance consistent with system criticality and its function in the system.

(2) Such protections and the generation of assurance evidence are automated to the greatest extent possible.

h. Conduct operational evaluations that are integrated with CI/CD pipelines; plan tests early; observe development; and accept validated automated test artifacts, security scans, performance data, and operational telemetry as test evidence of sufficient operational fidelity.

i. Leverage data generated from continuous monitoring, adversarial testing, and cyber ranges to inform operational evaluations of mission risk and resilience.

j. Ensure test infrastructure, data standards, and continuous evaluation enable timely sharing of operational test data and findings for continuous improvement while protecting sensitive information.

k. Adhere to DoW software supply chain risk management requirements, including generating and maintaining software bills of materials (SBOMs) for custom software and capturing SBOMs for COTS software, tracking provenance and pedigree, and disclosing and remediating vulnerabilities in accordance with DoDIs 5000.82 and 5200.44, and related supply chain risk management policies.

l. Adopt human-centered design and data-informed feedback loops to guide software investments and priorities. Engage representative users regularly (e.g., contextual inquiry, interviews, participatory workshops, usability testing) and instrument products to capture usage and satisfaction telemetry in accordance with applicable law and policy, including DoW privacy policies and DoDI 5200.48. Review value stream metrics and use these inputs in recurring product reviews to align with mission objectives and adapt quickly.

m. Collect quantitative and qualitative performance data for software activities in accordance with DoW standards as defined by the Software Modernization Senior Steering Group, and report to the appropriate Secretary of the Military Department or DoW CIO.

n. Report software asset inventory in accordance with DoDD 8115.01; DoDIs 5000.76 and 8115.02 and DoWI 8000.02; and Public Law 118-187, while abiding by classification and handling caveats.

o. Share custom-developed code across the DoW and with the broader Federal community as appropriate through publicly and privately available repositories to enable reuse pursuant to Public Law 118-187.

p. Manage data and records created or received by software assets and enable the availability of these data and records for a decision advantage in accordance with DoDI 5015.02 and DoDM 8180.01. Continue to manage records throughout and after the software asset's lifespan based on approved records disposition schedules.

q. Recruit, develop, and retain a mission-ready software workforce.

r. Appoint representation at the Software Modernization Senior Steering Group.

2.9. SECRETARIES OF THE MILITARY DEPARTMENTS.

In addition to the responsibilities in Paragraph 2.8., the Secretaries of the Military Departments manage a portfolio of software-enabling capabilities available across their respective Military Departments, such as DevSecOps platforms, software factories, software repositories, and software development tools and techniques and provide visibility of the portfolio to the DoW CIO for DoW-wide reuse.

2.10. CJCS.

In addition to the responsibilities in Paragraph 2.8., the CJCS:

a. Identifies and prioritizes joint operational problems that depend on software-intensive and digitally interoperable solutions, and publishes guidance that frames software, data, and interoperability expectations tied to those joint operational problems.

b. In coordination with the USW(A&S), tailors the joint force requirements process for software to emphasize outcome-based, flexible requirements aligned to modern software delivery, and to maximize delegated validation processes.

c. Promotes reuse and interoperability by encouraging adoption of authorized DevSecOps platforms, DoW enterprise services, modular open systems, and open interfaces to reduce cycle time for joint fielding and updates.

2.11. COMMANDER, UNITED STATES CYBER COMMAND.

In addition to the responsibilities in Paragraph 2.8., the Commander, United States Cyber Command:

a. Establishes and enforces DoW operational cyber defense directives and requirements for continuous monitoring, threat hunting, incident reporting, and vulnerability management across the DoW in accordance with DoDIs 8530.01, 8530.03, and 8531.01.

b. Specifies the security telemetry, event logging, and automated evidence that DoW Components must provide from cloud services, platforms, and CI/CD pipelines, and ensures integration with continuous monitoring.

c. Leads DoW hunt, adversarial emulation, and cyber range activities against priority systems and disseminates validated tactics, techniques, and procedures, and findings to drive hardening in software factories while preserving the independence of OT&E.

SECTION 3: PROCEDURES

3.1. GENERAL.

a. Software-defined warfare demands rapid adaptability and precise execution. This section:

(1) Outlines procedures to effectively leverage software as a critical element for responding to evolving threats and delivering integrated, innovative capabilities.

(2) Addresses the acquisition, iterative development, T&E, and deployment and maintenance of secure, high-quality software across the spectrum of DoW applications, from embedded systems to low/no-code platforms, SaaS, and commercial software used for DoW missions.

b. The DoW must continuously adopt and adapt the latest software principles and practices, tailoring them to mission-specific requirements. The goal is to empower superior decision-making and accelerated action, informed by performance, risk, and cost considerations, to maintain warfighting dominance.

3.2. MODERN SOFTWARE TENETS.

DoW Components will employ and continuously improve modern software development practices to deliver measurable mission value to the warfighter at the speed of relevance. The following tenets are foundational principles for DoW software development and deployment efforts:

a. Embrace Change through Continuous Feedback.

(1) Treat software as an evolving system that is never done.

(2) Prioritize CI/CD pipelines for rapid feedback loops with operational users and automated data streams, using frequent deployment of working software as the primary mechanism for refining requirements and delivering mission value.

b. Optimize for Flow, Not Phases.

(1) Relentlessly identify and remove friction from the software delivery lifecycle.

(2) Empower small, cross-functional, mission-focused teams with decision authority over technical implementation choices, development workflows, and tooling within DoW architecture boundaries and security baselines, eliminating the bureaucratic silos and handoffs that impede speed when independence improves mission outcomes.

c. Build Security and Quality In, Not On.

(1) Integrate security and quality into every step of the lifecycle, which is the responsibility of the entire team.

(2) Leverage approved reference designs, DoW enterprise platforms and software factories, and provisionally authorized infrastructure-as-code to make the secure path the easy path for development teams.

d. Automate to the Greatest Extent Possible.

(1) Treat testing, security scanning, compliance checks, and deployment as continuous activities, not final gates.

(2) Continuously improve these activities and automate them as much as practical within the CI/CD pipeline to provide immediate, actionable feedback to developers, operational users, program managers, and the T&E community with every code change, in accordance with applicable law and policy.

(3) Ensure automation leveraging AI capabilities complies with the requirements in Paragraph 3.6.

e. Architect for Evolvability and Scale.

(1) Design systems to be loosely coupled and highly cohesive.

(2) Use modular architectures, well-defined application programming interfaces, and packaging technologies such as containerization to enable components to be developed, deployed, and scaled independently, accelerating the pace of change.

(3) Favor simplicity and testability to reduce technical debt.

f. Default to Enterprise Reuse.

(1) Enterprise reuse breaks down programmatic silos, prevents duplicative effort, and maximizes the value of DoW software investments. Treat software and its associated artifacts as enterprise assets, not program-specific property.

(2) Default to making source code, documentation, application programming interfaces, data schemas, algorithms, logic processing, and SBOMs discoverable and reusable across the DoW with unlimited rights, or government purpose rights as a second alternative, as defined in Subpart 227.7203-5 of the Defense Federal Acquisition Regulation Supplement.

(3) Appropriately protect software with military or space application, which is designated as controlled technical information (CTI) at inception in accordance with Subpart 252.204-7012 of the Defense Federal Acquisition Regulation Supplement and Section 130 of Title 10, U.S.C.

g. Align Governance with Speed.

(1) Adapt legacy governance processes including acquisition, cybersecurity, and T&E to support iterative development and continuous delivery.

(2) Delegate decision-making authority to the lowest practical level, trusting teams to move fast while continuously verifying operational capability and compliance through automated evidence generation.

3.3. DATA-DRIVEN DECISION-MAKING FOR CONTINUOUS IMPROVEMENT.

DoW Components will foster a culture of continuous improvement by using empirical data to guide decisions. The goal of measurement is to provide insight, leveraging analytics available by modern software tools and aligning them to meaningful process objectives. Each software activity must deliver value and increase the flow of capability to their mission.

a. Measure Mission Value and User Satisfaction.

To ensure software delivers tangible benefits, DoW software development and deployment efforts will measure the value delivered to stakeholders.

(1) DoW Components will execute and measure human-centered design in accordance with DoDI 5000.95 and industry best practices.

(2) DoW programs using the software acquisition pathway will employ user agreements and contracts to formalize the commitment for continuous and active user involvement throughout the software development process. They will conduct value assessments in accordance with DoDI 5000.87. Non-acquisition programs are encouraged to adopt these practices to assess the impact of software on user productivity, efficiency, and mission success.

(3) DoW software development and deployment efforts will instrument systems to collect direct user feedback, including user satisfaction metrics and usage analytics to understand and improve the user experience, in accordance with applicable law and policy.

b. Measure the End-to-End Flow of Value.

(1) DoW Components will measure their Component's overall effectiveness in delivering software-enabled capabilities to the warfighter. These value stream metrics span the full lifecycle, from funding and contracting to development, validation, deployment, and operational use. The focus is on optimizing the complete value stream, not individual process steps.

(2) DoW Components will work with the Office of the USW(A&S) to align on common indicators of technological maturity and capability delivery that reflect mission impact.

c. Optimize Team Performance and Stability.

(1) Improvements in team-level engineering performance metrics are leading indicators for the health of the overall value stream. Development teams will instrument their pipelines and use performance metrics to optimize internal processes.

(2) Industry-recognized metrics for delivery and stability (e.g., DevOps Research and Assessment metrics), as well as management and monitoring are powerful diagnostic tools for teams to enhance their effectiveness. These metrics inform team-level improvement and are not appropriate to compare beyond the team context. DoW enterprise reporting will focus on value stream and mission outcomes as defined by mission and process owners.

d. Ensure Transparency and Access to Data.

(1) Contracts will specify government rights to access all relevant business value, value stream, and team-level metrics and supporting data from contractor and subcontractor environments through the incorporation of appropriate Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, and DoW Component-specific clauses. This ensures full transparency, enables data-driven portfolio management, and facilitates the identification of systemic impediments across the software delivery ecosystem.

(2) Any metrics or telemetry that identify or can reasonably be linked to an individual will be marked and handled in accordance with applicable law and policy, including Section 552a of Title 5, U.S.C., also known and referred to in this issuance as the "Privacy Act of 1974"; DoDIs 5200.48 and 5400.11; DoD 5400.11-R and Volume 2 of DoDM 5400.11; and where applicable, Intelligence Community Policy Memorandum 504 (01). This includes following data-minimization and lawful-processing requirements.

3.4. DOW ENTERPRISE DIGITAL ARSENAL.

a. General.

(1) The DoW enterprise digital arsenal is a federated, curated catalog of authorized DevSecOps platforms, automated CI/CD pipelines, authorized cloud and on-premises services, reference designs/guardrails, and reusable software components (e.g., container image and artifact repositories, infrastructure-as-code, and enterprise cloud contracts) managed by the Software Modernization Senior Steering Group and the Military Departments and DISA as enterprise providers.

(2) The DoW enterprise digital arsenal exists to:

(a) Enable speed through self-service by giving teams on-demand, hardened environments and capabilities.

(b) Produce machine-verifiable compliance evidence (e.g., tests, security checks, SBOMs, provenance) that supports reciprocity and continuous authorization.

(c) Ensure portability across classification levels, including disconnected/tactical environments.

(3) DoW Components will foster and contribute to the DoW enterprise digital arsenal by making capabilities available for DoW-wide use and by leveraging DoW enterprise digital arsenal capabilities to accelerate software delivery.

b. Federated Portfolio and Mandated Use.

DoW Components will:

(1) Enhance and federate their existing capabilities to enable cross-DoW Component discovery, reuse, and reciprocity while abiding by classification and need to know caveats.

(2) Leverage the DoW enterprise digital arsenal to reduce cost and speed time to delivery.

c. Mission Alignment.

Military Departments and DISA, as enterprise providers, will:

(1) Manage their portfolio of DevSecOps platforms, software factories, and cloud services to align with specific mission contexts (e.g., mission critical, training/incubator, and platform/infrastructure), ensuring that the pursuit of efficiency does not overly constrain the ability to choose the most appropriate technical solution.

(2) Provide visibility of their portfolios through the DoW enterprise digital arsenal.

d. Reuse through Shared Evidence.

(1) Software platforms and factories will produce and share machine-readable evidence (e.g., SBOMs, build provenance, security scans, and operational health data) sufficient to support continuous authorization. Authorizing officials will accept this standard evidence to grant reciprocity, avoiding redundant assessments.

(2) Evidence will identify applied protections and residual risks, including identified weaknesses and vulnerabilities, to inform adoption in achieving mission critical functionality or as a critical component.

e. Code and Component Reuse.

Software platforms will provide repository services that enable secure sharing and reuse of source code, software components, and other reusable artifacts such as design and development models across the DoW, in accordance with Paragraph 3.2.f.

f. Adoption through Value.

DoW Components will manage software platforms and factories that are recognized in Military Department and DISA portfolios as customer-driven products, driving adoption through value. Success and adoption will be based on the ability to provide compelling value, security, and speed to customers.

3.5. SECURE SOFTWARE DEVELOPMENT AND SUPPLY CHAIN INTEGRITY.

DoW Components will secure software development and the software supply chain in accordance with Executive Orders 14028, 14144, and 14306 and associated NIST standards.

a. Verifiable Assurance as a Condition for Operation.

(1) All software operated on DoW networks and systems will be supported by machine-readable evidence of its component composition, build integrity, and application security.

(2) The specific standards for evidence formats required to meet these principles will be defined and maintained by the DoW CIO, in coordination with the USW(R&E), on the Cybersecurity Knowledge Service at https://cybersecurityks.osd.mil.

b. Software Component Transparency.

DoW Components will ensure an accurate SBOM is generated and maintained for all covered software in accordance with DoW-approved standards. The SBOM will provide software composition information necessary for supply chain analysis, such as vulnerability and license management.

c. Verifiable Build Integrity, Provenance, and Pedigree.

(1) To manage risk in the software supply chain, DoW Components will produce all covered software using a secure, automated, and observable build process that ensures software originates from trusted sources and is protected from tampering during its creation and distribution. This process will generate machine-readable provenance (a verifiable history of the software's origin and build process) and attestations that provide pedigree (a cryptographically verifiable chain of custody and integrity for the software and its components).

(2) Evidence packages, SBOMs, provenance, and associated telemetry that contain sensitive information will be marked and handled in accordance with applicable law and policy, including the Privacy Act of 1974, DoDI 5200.48, DoDI 5400.11, DoD 5400.11-R, Volume 2 of DoDM 5400.11, and where applicable, Intelligence Community Policy Memorandum 504 (01). DoW Components will minimize collection of personally identifiable information in these artifacts.

d. Integrated and Continuous T&E.

(1) DoW Components will implement an integrated and continuous T&E approach in accordance with DoDI 5000.89, DoDI 5000.98, DoDM 5000.96, and DoDM 5000.103, to provide evidence-based assessments of software operational effectiveness, suitability, survivability, and mission capability. This approach will unify DT&E and OT&E into a seamless continuum of integrated test activities.

(2) DT&E:

(a) Will be conducted as integrated contractor and government DT&E to:

1. Mature software products, verify technical progress, and minimize design risks.

2. Substantiate achievement of contract technical performance requirements, including cybersecurity and cyber resilience requirements.

3. Support certification of readiness for operational testing.

4. Facilitate failure analysis through engineering-type tests using instrumentation, measurements, and controlled environments.

(b) Activities will follow the guidance in DoDI 5000.89 and the DoD Enterprise DevSecOps Activities and Tools Guidebook.

(c) Cyber activities will be informed by iterative mission-based cyber risk assessments and conducted in accordance with DoDM 5000.103.

(d) Software development efforts will conduct continuous or periodic adversarial security testing in accordance with DoDM 5000.103. The scope of this testing will include automated CI/CD pipelines, infrastructure-as-code scripts, source code repositories, and running applications.

(e) Findings from testing activities will be formally documented, prioritized in the software development effort's backlog, and tracked to remediation to ensure a continuous cycle of security improvement and validation.

(3) OT&E:

(a) Will enable evaluations of the operational effectiveness, suitability, and survivability of software in realistic mission environments.

(b) Will leverage evidence generated during DT&E, including automated testing, security scanning, and user assessments, to inform and enable operational evaluations, but will not replace DT&E.

(c) Activities will follow the guidance in DoDI 5000.98 and DoDM 5000.96.

(4) DoW Components will establish an integrated T&E function embedded within software development and deployment efforts. This function will:

(a) Collaboratively develop and maintain a T&E strategy in accordance with DoDI 5000.89 and DoDI 5000.98.

(b) Align DT&E and OT&E activities to ensure a unified continuum of test activities.

(c) Leverage evidence from all sources, including contractor-led and government-led testing, to provide a comprehensive evaluation of mission capability.

(5) DoW Components will conduct continuous assessments to:

(a) Provide ongoing evaluations of mission capability, including cybersecurity and cyber resilience.

(b) Generate formal evidence to support risk-based fielding decisions.

(6) DoW Components will ensure that DT&E and OT&E are integrated throughout the software lifecycle to rigorously test software products, ensure resilience, and meet mission demands in dynamic operational environments. Integrated testing means using test events to gather data, which is separately evaluated for DT&E and OT&E objectives.

(7) While automation provides a portion of the required continuous evidence, software development efforts will still plan for and conduct periodic, independent government cyber DT&E events to validate findings, explore attack paths, and provide objective assessments of cyber resilience.

e. Security Baseline for DoW Enterprise Digital Arsenal Components.

(1) Software factories and services within the DoW enterprise digital arsenal that store, process, or develop DoW software or associated artifacts will be hardened, monitored, and authorized at a minimum of moderate confidentiality and moderate integrity. For cloud hosting, the minimum impact level (IL) is IL2 or higher as defined in the Cloud Service Provider Security Requirements Guide.

(2) Software and associated technical artifacts (e.g., source code, build scripts, SBOMs, test vectors, design documents) with a specific military or space application are CTI under the DoD Controlled Unclassified Information Program per DoDI 5200.48 and must be protected at a minimum of moderate confidentiality and moderate integrity.

(3) DoW software development and deployment efforts will be protected by applying operations security in accordance with DoDD 5205.02E.

f. Verifiable Application Security, Resilience, and Safety.

To ensure software is designed, implemented, and maintained to withstand known and emerging threats, DoW Components will develop, test, and validate all covered software against

a common set of verifiable and measurable security and resilience requirements. These requirements will be validated through automated tooling where feasible and produce verifiable evidence suitable for risk-based authorization decisions and, at a minimum, address:

(1) Secure architecture and design, including least privilege, defense-in-depth, and modularization.

(2) Authentication and authorization.

(3) Input validation, output encoding, and injection prevention.

(4) Cryptography, covering encryption of data at rest and in transit using Federal Information Processing Standards-validated algorithms.

(5) Error handling and logging, ensuring no leakage of sensitive information.

(6) Software safety, especially for operational technology and mission-critical systems.

(7) Operational resilience, including runtime protection, fault tolerance, and rollback/recovery mechanisms.

(8) Continuous vulnerability management, including static/dynamic analysis and dependency scanning integrated into pipelines.

g. Evidence for Assessment and Continuous Monitoring.

Evidence demonstrating conformance with Paragraph 3.5. will be required input to risk management processes. This evidence will be used to inform and validate the assessment of security controls consistent with the Assess Only Construct on the Cybersecurity Knowledge Service at https://cybersecurityks.osd.mil/.

h. Continuous Supply Chain Monitoring and Disclosure.

(1) DoW Components will continuously monitor software (e.g., COTS, custom-developed) deployed on DoW networks for vulnerabilities and supply chain risks in alignment with supply chain risk management policies.

(2) DoW Components will require vendors and developers to report any discovery of critical or actively exploited vulnerabilities to the designated authority within a timeframe specified by the DoW CIO as a condition for deployment or continued use.

i. Risk Management Considerations for Third-Party and Open-Source Software.

(1) DoW Components will conduct market research when assessing and selecting software components in accordance with Section 3306 of Title 41, U.S.C.; Part 10.001 of the Federal Acquisition Regulation; and Part 210.001 of the Defense Federal Acquisition Regulation Supplement.

(2) When determining suitability of any third-party software components, including open-source software, the following risk factors will be addressed:

(a) Sustainment.

The stability, activity level, and availability of technical support for the component.

(b) Source Trustworthiness.

The integrity of the distribution source and the provenance of the software.

(c) Dependencies.

The security and license obligations of all sub-components.

(d) Security Posture.

Verifiable evidence of the developer's security practices, including vulnerability management and timely remediation.

(e) Integrity Protections.

The availability of strong integrity validation mechanisms, such as cryptographic signatures for releases and support for reproducible builds.

(f) Foreign Influence Risks.

The potential for adversarial ownership, investment, contribution, or control over the project or vendor.

(3) While open-source software is a critical DoW resource, it presents unique governance and community-related risks that require specific analysis beyond that for commercial products. In addition to the factors in Paragraph 3.5.i.(2), the assessment of any non-trivial open-source software component will include a detailed review of the following aspects of a software project:

(a) Governance and Control Model.

This includes the structure of the project's leadership and commit authority. Analysis must differentiate between projects managed by established foundations (e.g., Apache, Cloud Native Computing Foundation) and those controlled by individuals or small, unaudited groups.

(b) Community Health and Security Practices.

This includes the level of community activity, the rigor of its contribution and pull-request review process, its public security disclosure policy, and the track record of its core maintainers.

(c) License Compliance and Legal Risk.

This includes an understanding of legal obligations, license compatibility issues, copyleft requirements, and usage scenarios that may trigger undesirable conditions (e.g., disclosure of source code). License risk must be evaluated alongside security and operational risk and documented as part of the software risk assessment process to ensure that the inclusion or use of open source components does not violate the terms of their licenses and to enable the management of overall risk.

(4) All third-party software components, including open-source software, COTS products, and their transitive dependencies, must be included in the SBOM for the system in which they are integrated in accordance with Paragraph 3.5.b.

3.6. AI IN SOFTWARE DEVELOPMENT.

The DoW recognizes that AI-assisted software development is a significant force multiplier for the delivery of speed and quality. The requirements in this paragraph establish the security, accountability, and transparency baseline that enables teams to confidently adopt AI in mission-critical software development contexts while managing associated risks.

a. Principle of Human Responsibility and Accountability.

(1) Developers and development teams remain fully accountable for the security, functionality, and integrity of any code generated or modified using AI.

(2) DoW Components will implement a risk-based review that, at a minimum, requires human review and approval for AI-generated changes to security- or safety-critical functionality. AI-generated code will be considered unverified input, and its use does not absolve the developer or the government of responsibility for the resulting work product.

b. Protection of Government Data.

(1) Non-public DoW information, including code, configuration scripts, infrastructure definitions, schematics, or documentation, may not be entered into or processed by generative AI applications or services unless those applications or services reside on DoW information systems and are approved for use by DoW personnel in accordance with DoDI 8500.01 and DoDI 8582.01.

(2) When approved AI applications or services process information about individuals, DoW Components will comply with applicable law and policy, including the Privacy Act of 1974, DoDI 5400.11, DoD 5400.11-R, Volume 2 of DoDM 5400.11, DoDD 3115.18, and where applicable, Intelligence Community Policy Memorandum 504 (01). This includes applying appropriate data minimization and access controls.

c. Security Validation of AI-Generated Code.

(1) All code suggested or generated by AI, including software code, scripts, and automated tests, will be subject to the same or similar rigorous code review and security testing processes as manually written code, in accordance with Paragraph 3.5.

(2) Code must be explicitly reviewed for security vulnerabilities, safety implications, logical errors, subtle bugs, potential intellectual property infringement, license obligations, and proper implementation of security controls before being integrated into a codebase.

d. Approved AI Applications or Services and Environments.

DoW Components will only use AI applications or services for DoW proprietary software development that were developed with AI cybersecurity requirements as defined in the DoW AI Cybersecurity Risk Management Tailoring Guide and are explicitly authorized through formal DoW cybersecurity approval processes and guidance on the Cybersecurity Knowledge Service at https://cybersecurityks.osd.mil/. Approved applications or services must, at a minimum:

(1) Provide contractual guarantees that government data and user prompts are not shared or used for training any public or DoW-external models.

(2) Allow for auditing and monitoring of their use by designated authorities.

e. Reliable AI.

(1) For each AI-enabled capability, DoW Components will:

(a) Determine the use case-specific risk and mitigation requirements.

(b) Define measurable performance benchmarks in accordance with DoW AI policy and guidance and aligned to applicable NIST or other appropriate industry standards on AI.

(c) Verify performance benchmarks and risk remediation efforts are satisfactory before deployment.

(d) Ensure that performance benchmarks are continuously monitored while the AI-enabled capability is in operation.

(2) DoW Components will ensure that AI is designed and deployed to minimize unintended bias across relevant statistical, computational, human, and systemic contexts in alignment with DoW standards.

(3) Software using AI will implement techniques to detect and monitor for unintended bias and will notify appropriate stakeholders of any detected model bias. Bias considerations will be addressed as part of existing risk management processes.

f. AI Component Transparency.

To ensure transparency when using AI, software efforts will maintain a record of models, versions, and significant datasets used to generate or test software. This information will be included as part of the comprehensive software evidence package, analogous to the SBOM, to enable risk assessment and traceability of AI-driven components.

g. AI Training.

DoW Components will ensure that appropriate members of development teams receive training on the principles outlined in Paragraph 3.6. This includes awareness of common AI-generated vulnerability patterns, best practices for prompt engineering to elicit secure code, and understanding the risks of intellectual property and license contamination.

h. Design and Implementation with AI.

(1) DoW Components should leverage AI technologies to modernize software systems, enhance operational efficiency, and accelerate capability delivery.

(2) DoW Components can apply AI to automate software development processes, optimize system integration, and improve resilience and security.

(3) DoW Components will design and implement software systems with AI in accordance with DoDIs 5000.87 and 5000.97.

3.7. SOFTWARE ASSET MANAGEMENT.

a. Custom-Developed Code.

DoW Components will report custom-developed code (i.e., GOTS) unless security requirements dictate otherwise, in accordance with DoDI 8115.02 and Public Law 118-187.

(1) DoW Components will report unclassified systems in the DoW IT Portfolio Repository and classified systems, up to SECRET//NOFORN, in the SIPRNet IT Registry to enable portfolio management and rationalization.

(2) DoW Components will share custom-developed code in a publicly or privately available repository to enable DoW enterprise-wide reuse. Before any release, DoW Components will remove personally identifiable information and other sensitive data from code, documentation, issues, and commit history, and mark shared artifacts in accordance with DoDI 5200.48 where applicable.

(a) Custom-developed code for which the existence of the code is classified, the source code developed is primarily for use in national security systems, or the source code developed is used by an agency, or part of an agency, that is an element of the intelligence community are exempt from the requirements of Public Law 118-187.

(b) Custom-developed code with military or space application, along with its associated documentation and binaries, is designated as CTI at its inception. Pursuant to Public Law 118-187, this code will be shared for discovery and reuse across the DoW using an InnerSource model.

(c) The public release of GOTS as open-source software is encouraged to drive innovation and maximize value. As determined by the program manager or authorizing official, software without specific military or space application, or other sensitivities (e.g., intellectual property, export controls, sensitive operational capabilities (tactics, techniques, procedures)) will be developed using an open source, collaborative approach that maximizes value through reuse and minimizes maintenance and integration costs. DoW Components will use MOSA to separate CTI components from potentially releasable components.

(d) Custom-developed code released as open-source software will use permissive, widely recognized licenses that allow unrestricted use, modification, and distribution. These licenses must ensure compatibility and ease of reuse and be approved by the Military Departments or the DoW CIO. Software development and deployment efforts will not develop custom or unique licenses unless explicitly approved by the appropriate Military Department or the DoW CIO.

b. Proprietary Licenses and SaaS Subscriptions.

DoW Components will manage commercial software licenses and SaaS subscriptions to minimize cost, reduce risk, and ensure compliance with DoW policy, and will track them in accordance with the January 28, 2021, DoD CIO Memorandum and associated guidance.

(1) Inventory and Discovery.

DoW Components will maintain an authoritative, automated inventory of all commercial software entitlements and SaaS subscriptions, including license data, entitlements, deployments/usage, versions, end-of-support dates, costs, and contract identifiers in accordance with DoDI 5000.76 and DoWI 8000.02. Inventories will integrate with Comply-to-Connect and Information Security Continuous Monitoring tools to detect and remediate unauthorized software and shadow IT.

(2) Sourcing and Acquisition.

DoW Components will first consider DoW Enterprise Software Initiative agreements and other enterprise vehicles, and comply with Subpart 208.74 of the Defense Federal Acquisition Regulation Supplement when acquiring software or SaaS. DoW Components will coordinate with Military Departments or the DoW CIO to avoid duplicative buys and enable portfolio rationalization. DoW Enterprise Software Initiative agreements and other enterprise vehicles are available at https://www.esi.mil.

(3) License Compliance and Optimization.

DoW Components will meter usage, reconcile entitlements to deployments, remediate over- and under-licensing, plan and fund true-ups, reharvest unused licenses, and rationalize duplicative products to optimize total cost of ownership.

(4) SaaS Security, Authorization, and Data Safeguards.

SaaS offerings must meet Federal Risk and Authorization Management Program, also known as FedRAMP, authorization appropriate to the information IL and comply with the Cloud Service Provider Security Requirements Guide. Authorizing officials will issue and maintain an Authorization to Operate in accordance with risk management processes. In accordance with applicable policy, SaaS contracts should include government data rights, data portability/export in non-proprietary formats, incident reporting, continuous monitoring, and termination/exit assistance, including timely return and destruction of data. Additional guidance will be provided on the Cybersecurity Knowledge Service at https://cybersecurityks.osd.mil.

(5) Terms and Conditions.

DoW Components will ensure license and subscription terms comply with Section 1653 of Public Law 114-328 and DoW CIO guidance prohibiting unapproved click-through, end-user license agreements; and address audit rights, usage metrics, privacy, records management, and Section 508 of Public Law 93–112, also known as "the Rehabilitation Act of 1973," as amended, accessibility requirements.

3.8. ACQUISITION AND CONTRACTING.

Acquisition strategies and contracting vehicles are critical enablers for modern software delivery and must be aligned with the principles of speed, iteration, and flexibility.

a. Utilize the Software Acquisition Pathway.

(1) The software acquisition pathway, established in DoDI 5000.87, is the DoW's preferred process for the rapid and iterative delivery of software capabilities. Acquisition programs will use the software acquisition pathway as the preferred pathway for all DoW software acquisition.

(2) Commercial Solutions Openings and Other Transactions are the default solicitation approaches for this pathway. Sufficient intellectual property and data rights are required to enable long-term operation, maintenance, modification, and cybersecurity of DoW software capabilities.

b. Leverage Commercial Best Practices.

Acquisition programs will use the software acquisition pathway to leverage its tailored policies and commercial best practices for planning, funding, contracting, and executing, all of which are designed to support the tenets of this issuance.

c. Ensure a Trained Acquisition Workforce.

Government program teams, including program management, engineering, and contracting personnel, will pursue training in modern software principles and the software acquisition pathway to ensure that they can effectively plan and deliver software capabilities as well as design, award, and manage Agile software contracts.

3.9. SOFTWARE WORKFORCE.

The dynamic nature of war requires a highly skilled workforce that can quickly analyze and leverage emerging technologies to perform accelerated software operations for mission dominance.

a. Develop an Adaptable, Skilled Software Workforce.

DoW Components will build and sustain a workforce with the skills required to execute software operations needed for ever-changing mission parameters.

(1) DoW Components will use the DoW Cyber Workforce Framework to identify and define positions with relevant work roles that comprise the knowledge, skills, and abilities needed for high-performing software development, security, and operations teams.

(2) DoW Components will leverage the DoW Software Cadre, Warfighting Acquisition University, and other DoW education and training resources (e.g., DoW, government, academia, industry) to close skill gaps (e.g., upskilling, reskilling, cross-skilling) and to provide pathways for continuous learning and professional development.

(3) DoW Components will ensure that software workforce personnel obtain "Foundational" and "Residential" qualifications, as applicable, in accordance with DoDD 8140.01, DoDI 8140.02, and DoDM 8140.03.

b. Implement a Continuous Improvement Tempo.

DoW Components will foster a continuous learning environment and remove barriers, so teams are empowered to learn and adapt skills rapidly.

c. Create Performance-Oriented Assessments.

DoW Components will link skills to performance and mission outcomes. Regular assessments are integral to the mission to determine if performance standards are met. Problems and failures are critical opportunities for learning and systemic improvement. Performance assessments inform and enable teams to innovate, adapt, and solve problems in a purposeful manner with targeted feedback and clear metrics.

3.10. EXCEPTION TO POLICY (E2P).

a. DoW Components requesting an exception to this issuance will submit an E2P for alternate approach. DoW Components will submit their E2P request on the E2P Portal at https://rmfks.osd.mil/dode2p/Pages/default.aspx.

b. DoW Components may review submission requirements under the resources section of the E2P Portal and review the document titled, "E2P SOP."

c. Information regarding the process for exceptions will be included on the E2P Portal.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AI	artificial intelligence
CI/CD	continuous integration/continuous deployment
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
COTS	commercial-off-the-shelf
CTI	controlled technical information
DevSecOps	development, security, and operations
DISA	Defense Information Systems Agency
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DOT&E	Director of Operational Test and Evaluation
DoW	Department of War
DoWI	DoW instruction
DT&E	development test and evaluation
E2P	exception to policy
GOTS	government-off-the-shelf
IL	impact level
IT	information technology
MOSA	modular open systems approach
NIST	National Institute of Standards and Technology
OSW	Office of the Secretary of War
OT&E	operational test and evaluation
SaaS	software-as-a-service
SAP	special access program
SBOM	software bill of materials
T&E	test and evaluation
U.S.C.	United States Code
USW(A&S)	Under Secretary of War for Acquisition and Sustainment
USW(I&S)	Under Secretary of War for Intelligence and Security
USW(R&E)	Under Secretary of War for Research and Engineering

G.2. DEFINITIONS.

These terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
Agile	Defined as "Agile software development" in DoDM 5000.96.
CI/CD pipeline	The process workflows and associated tools to achieve the continuous integration and continuous deployment of software with maximum use of automation.
covered software	Any software, including firmware, operating systems, applications, and cloud-based services that are developed, acquired, integrated, or operated by or on behalf of the DoW.
DevSecOps	A combination of software engineering methodologies, practices, and tools that unifies software development (Dev), security (Sec), and operations (Ops). It emphasizes collaboration across these disciplines, along with automation and continuous monitoring to support the delivery of secure, high-quality software. Integrates security tools and practices into the development pipeline, emphasizes the automation of processes, and fosters a culture of shared responsibility for performance, security, and operational integrity throughout the entire software lifecycle, from development to deployment and beyond.
DevSecOps platform	A group of resources and capabilities that form a base upon which other capabilities or services are built and operated within the same technical framework. Use of a DevSecOps platform is encouraged to accelerate development, delivery, and cybersecurity accreditation.
DoW enterprise digital arsenal	A discoverable, federated, curated catalog of authorized DevSecOps platforms, CI/CD pipelines, cloud and on-premises services, reference designs, reusable software components, and enterprise catalogs that provide self-service, on-demand environments for building, testing, deploying, and operating software across classification levels and environments. The DoW enterprise digital arsenal exists to accelerate secure delivery, generate continuous authorization evidence, and enable reciprocity and reuse across DoW Components.

TERM	DEFINITION
human-centered design	An approach to design products focused on the human limitations and capabilities of those who will operate, maintain, and support the system, including the services and processes associated with the system and across domains that align with human performance needs.
human systems integration	Defined as "HSI" in DoDI 5000.95.
infrastructure-as-code	The management of infrastructure (e.g., networks, virtual machines, load balancers, and connection topology) in a descriptive model, using the same versioning that the DevSecOps team uses for source code. Infrastructure-as-code evolved to solve the problem of environment drift in the release pipeline.

TERM	DEFINITION
InnerSource	The application of open-source software development principles and practices within the boundaries of an organization. It encourages transparency, cross-team collaboration, and the reuse of software components to break down programmatic silos and accelerate development. InnerSource includes: Open Collaboration: Contributions are made through a transparent process, such as pull requests or code reviews. Transparency: Code, documentation, and project discussions are accessible to all personnel across the DoW. This openness encourages knowledge sharing and reduces silos. Voluntary Participation: Personnel can voluntarily contribute to projects outside their immediate responsibilities, often driven by interest or expertise. Shared Ownership: Code is not "owned" by a single team but is treated as shared assets of the DoW. Contributions from multiple teams are welcomed and encouraged. Governance: Code typically has maintainers or core teams responsible for reviewing contributions, setting priorities, and ensuring quality. Governance structures for software projects are often lightweight and modeled after open source community practices. Reuse and Standardization: The InnerSource model encourages the reuse of code and components across teams, reducing duplication and improving efficiency. It promotes the creation of standardized tools, libraries, and frameworks.
modern software development practices	Defined in DoDI 5000.87.
MOSA	Defined in Section 4401 of Title 10, U.S.C.
open-source software	Software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by users of such software.

TERM	DEFINITION
SBOM	A formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships. These inventories should be comprehensive or should explicitly state where they could not be. SBOMs may include open source or proprietary software and can be widely available or access-restricted.
software	Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled. Includes custom-developed software, COTS software, GOTS software, SaaS, and open-source software.
software factory	A collection of people, tools, and processes that enables teams to continuously deliver value by deploying software to meet the needs of a specific community of end users. It leverages automation to replace manual processes.
value stream metrics	Performance indicators that assess how effectively a capability is delivered to the warfighter across the entire development and delivery lifecycle. Value stream metrics track progress across funding, acquisition, engineering, compliance, deployment, and operational use. They aim to optimize the full system rather than isolated stages, enabling better decision-making and continuous improvement across the DoW software enterprise.

REFERENCES

Deputy Secretary of Defense Memorandum, "Department of Defense Software Modernization," February 1, 2022

Defense Federal Acquisition Regulation Supplement, current edition

Defense Information Systems Agency, "Cloud Service Provider Security Requirements Guide, Version 1, Release 6," December 10, 2025

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD 7000.14-R, "Department of Defense Financial Management Regulation (DoD FMR)," current edition

DoD Chief Information Officer, "DoD Enterprise DevSecOps Activities & Tools Guidebook," April 2025

DoD Chief Information Officer, "DoD Artificial Intelligence Cybersecurity Risk Management Tailoring Guide," July 14, 2025

DoD Chief Information Officer Memorandum, "DOD CIO Update: National Defense Authorization Act, Fiscal Year 2017, Section 1653 Compliance, Information Security Continuous Monitoring, Implementing Comply-to-Connect Policy, and Limitations on Software Licensing," January 28, 2021[1]

DoD Directive 3115.18, "DoD Access to and Use of Publicly Available Information (PAI)," August 20, 2020, as amended

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 Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005

DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020

DoD Instruction 5000.76, "Accountability and Management of Internal Use Software (IUS)," March 2, 2017, as amended

DoD Instruction 5000.82, "Requirements for the Acquisition of Digital Capabilities," June 1, 2023

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

DoD Instruction 5000.87, "Operation of the Software Acquisition Pathway," October 2, 2020

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020

DoD Instruction 5000.95, "Human Systems Integration in Defense Acquisition," April 1, 2022

DoD Instruction 5000.97, "Digital Engineering," December 21, 2023

DoD Instruction 5000.98, "Operational Test and Evaluation and Live Fire Test and Evaluation," December 9, 2024

[1] This memorandum is available by emailing a request to osd.mc-alex.dod-cio.mbx.devsecops@mail.mil.

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," February 16, 2024

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

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

DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006

DoD Instruction 8140.02, "Identification, Tracking, and Reporting of Cyberspace Workforce Requirements," December 21, 2021

DoD Instruction 8310.01, "Information Technology Standards in the DoD," April 7, 2023

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Instruction 8530.03, "Cyber Incident Response," August 9, 2023

DoD Instruction 8531.01, "DoD Vulnerability Management," September 15, 2020

DoD Instruction 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019

DoD Manual 5000.96, "Operational and Live Fire Test and Evaluation of Software," December 9, 2024

DoD Manual 5000.103, "Cyber Developmental Test and Evaluation," February 25, 2026

DoD Manual 5400.11, Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021, as amended

DoD Manual 8140.03, "Cyberspace Workforce Qualification and Management Program," February 15, 2023

DoD Manual 8180.01, "Information Technology Planning for Electronic Records Management," August 4, 2023

DoD SAP Chief Information Officer, "Joint Special Access Program (SAP) Implementation Guide with Errata," October 5, 2018

DoW Instruction 8000.02, "Information Technology Category Management," July 29, 2026

Executive Order 12333, "United States Intelligence Activities," December 4, 1981

Executive Order 14028, "Improving the Nation's Cybersecurity," May 17, 2021

Executive Order 14144, "Strengthening and Promoting Innovation in the Nation's Cybersecurity," January 16, 2025

Executive Order 14306, "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144," June 6, 2025

Federal Acquisition Regulation, current edition

Intelligence Community Policy Memorandum 504 (01), "Intelligence Community Policy Framework for Commercially Available Information," February 6, 2025

Public Law 93–112, "the Rehabilitation Act of 1973," September 26, 1973, as amended

Public Law 114-328, "National Defense Authorization Act for Fiscal Year 2017," December 23, 2016

Public Law 117-81, "National Defense Authorization Act for Fiscal Year 2022," December 27, 2021

Public Law 118-187, "Source Code Harmonization and Reuse in Information Technology Act," December 23, 2024

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

United States Code, Title 10

United States Code, Title 41, Section 3306