SECRETARY OF THE ARMY
WASHINGTON

11 MAR 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Directive 2024-02 (Enabling Modern Software Development and Acquisition Practices)

1. References. For references, see enclosure 1.

2. Purpose. This directive establishes policy and assigns responsibilities for the Army's adoption of modern software development and acquisition practices. For the purposes of this policy, modern software development practices include, but are not limited to, continuous integration/continuous delivery (CI/CD), agile, lean, and development, security, and operations (DevSecOps). For the definitions applicable to this policy, see enclosure 2.

3. Applicability. The provisions of this directive apply to:

a. Software development efforts executed by the Regular Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve. For the purposes of this directive, a "software development effort" is defined as: (a) development of a custom software solution; (b) customization, integration, or modification of a commercial software solution; and (c) software as a service.

b. Weapons and business software systems and associated training software systems developed and acquired through the formal acquisition processes.

c. Software developed or acquired outside of the formal acquisition process by Army Commands (ACOMs), Army Service Component Commands (ASCCs), Direct Reporting Units (DRUs), or other Army organizations. This includes science & technology software development efforts, funded using Budget Activities 6.1–6.3.

d. Commercial-Off-the-Shelf (COTS) software purchases only when explicitly identified in the policy.

e. Exempted from this directive are low code/no code development activities conducted within Army-authorized data platforms, as identified by the Army Chief Information Officer.

f. Exempted from this directive are cyberspace operations conducted by the U.S. Army Cyber Command.

4. Background. Software is essential to modern military operations. It is a key component in the Army's weapons, business, and training systems and is embedded into the enterprise processes that make the Department function. These systems enable the Army to detect and track adversaries, protect operations from cyber threats, and improve the accuracy and effectiveness of decisions and actions. Software drives improved outcomes and effectiveness in our missions and operations. Consequently, the Army's ability to rapidly develop, deliver, and adapt resilient software is critical to achieving a competitive advantage over adversaries. However, current institutional processes are largely designed for the development of hardware-based capabilities and do not enable the flexibility and agility required by modern software development practices. To further broaden adoption of modern practices, the Army is reforming key institutional processes related to requirements, acquisition, contracting, test and evaluation, cybersecurity, cost estimation, data management, sustainment, and talent management. The Army will modify these processes through the reform initiatives described below. These reforms will enable the Army's adoption of best practices for software development and accelerate the Army's digital transformation to deliver needed capabilities to Soldiers.

5. Reform Initiatives.

a. Initiative 1—Establish a Flexible Requirements Process To Support Agile Development.

(1) Background. Many Army programs and software development efforts are currently based on requirements that are detailed, prescriptive, and infrequently reassessed, which can inhibit iterative development of requirements. Modern software development requires speed and flexibility, accompanied by frequent iteration with users. Requirements processes must be adapted to allow for iterative refinement as software development progresses. The Software Acquisition Pathway – the acquisition pathway designed for agile software development – recommends use of capability needs statements (CNSs) and software initial capabilities documents (SW-ICDs) as these documents allow for requirements to be captured at a high level, prioritized, reassessed over time, and refined based on user input.

(2) Policy.

(a) All software development efforts will plan for software development and deployment as early in the lifecycle as possible, to include in requirements planning and development. All software development efforts will use modern software development practices to the maximum extent practicable. This requirement applies to acquisition programs developing software (regardless of acquisition pathway) and all software development efforts conducted by ACOMs, ASCCs, and DRUs.

(b) In accordance with DoDI 5000.87, acquisition programs executing on the Software Acquisition Pathway will use CNSs or SW-ICDs to document high-level, prioritized requirements or operational need.

(c) Software-intensive acquisition programs that are executing on a pathway other than the Software Acquisition Pathway will capture software requirements in a format consistent with CNSs and SW-ICDs. The software capability requirements can be included as part of, or as an appendix to, the capability requirements document required by any given pathway.

(d) Consistent with paragraph 5.f.(2)(a) of this directive, requirements for software to be developed or procured by ACOMs, ASCCs, and DRUs will be captured in a format consistent with CNSs and SW-ICDs.

(e) Given the rapid and iterative nature of agile software development, requirements should not be overly prescriptive or detailed. Software capability requirements will be written at a high-level, concise, focused on operational issues, and refined iteratively over time based on functional sponsor and user community input during capability development and delivery. Software capability requirements will be assessed routinely over time (annually, at a minimum). This will allow programs and efforts to better respond to the changing needs of the user.

(3) Initiative Leads.

(a) Weapon Systems—Commanding General (CG), U.S. Army Futures Command (AFC) and Deputy Chief of Staff (DCS), G-8.

(b) Defense Business Systems (DBS)—Director, Office of Enterprise Management (OEM).

(c) Systems in the Enterprise Information Environment Mission Area (EIEMA)—Chief Information Officer (CIO) and DCS, G-6.

(d) Support will be provided by the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA (ALT)); DCS, G-3/5/7; and CG, U.S. Army Training and Doctrine Command (TRADOC).

(4) Timeline. Leads will implement processes for this approach and develop CNS and SW-ICD templates no later than four months from the date of this directive.

b. Initiative 2—Ensure Continuous User/Developer Teaming to Deliver Customer Value.

(1) Background. Currently, there is no requirement for user involvement in software development efforts executed outside the Software Acquisition Pathway. Continuous user involvement in the software development process is a recognized software development best-practice as it helps to ensure software solutions are iteratively developed in line with user needs, which may change over time based on evolving technologies and threats.

(2) Policy.

(a) All software development efforts will have a robust and continuous process to solicit and incorporate user feedback. This requirement applies to acquisition programs developing software (regardless of acquisition pathway) and all software development efforts conducted by ACOMs, ASCCs, and DRUs.

(b) Software development programs and efforts will institute User/Developer Teams to ensure users are regularly engaged with developers. User/Developer Teams will be established during requirements development and continue throughout the software development lifecycle. The teams will be codified in a User Agreement.

(c) The User/Developer Team will collaborate to define and prioritize capability requirements and determine tradeoffs of software features and cadence. Users will provide acquirers, developers, and testers with insights into the operational environment; participate in user testing and software demonstrations; and provide assessments of user value.

(d) User/Developer Team composition and size will vary based on the availability of resources, including personnel and funding, and operational requirements. Users should be represented by those that will ultimately use the software solution. Users may be represented by operational users or functional users, based on the capability being acquired. Developers may be represented by program office personnel, vendor personnel, and/or other Army personnel sponsoring the software development.

(e) When operational users are required, the CG, U.S. Army Forces Command (FORSCOM) will seek to meet this need without impacting other requirements. Existing Army enterprise sourcing approaches, such as the Army's Regionally Aligned

Readiness and Modernization Model and the Army Synchronization and Resourcing Conference, will be used.

(3) Initiative Leads.

(a) Weapons systems—CG, AFC.

(b) Defense Business Systems—Director, OEM and the CIO.

(c) Systems in the Enterprise Information Environment Mission Area—CIO and DCS, G-6.

(d) Support will be provided by the ASA(ALT); DCS, G-3/5/7; CG, FORSCOM; and all ACOMs, ASCCs, and DRUs.

(4) Timeline. Leads will implement a process for this approach no later than four months from the date of this directive.

c. Initiative 3—Tailor Processes To Enable Agile Development.

(1) Background. A key tenet of successful software development is the ability to quickly adapt software solutions to respond to emerging threats, opportunities, and needs. However, some acquisition and contracting approaches do not inherently provide the flexibility required by modern software development. The Army must employ approaches that provide the agility and flexibility to be able to rapidly develop and deploy a software solution that can continuously evolve to meet user needs.

(2) Policy.

(a) Acquisition strategies for software-intensive acquisition programs will enable modern software development approaches. These programs will use the Software Acquisition Pathway as the single pathway or in conjunction with other acquisition pathways to the maximum extent practical. This pathway was designed to enable rapid and iterative delivery of software capability. Programs executing on the Defense Business System pathway should consider leveraging the newly established DBS sub-path within the Software Acquisition Pathway.

(b) Contracting strategies for software development efforts will be flexible and provide the ability to quickly adapt to changes in the software development strategy. This may include employing a multiple-award contract or a modular contracting approach, which uses a series of tightly scoped contracts in place of a single larger contract. This iterative approach allows software development efforts to address changing needs between incremental software releases, enabling them to scale and evolve over their lifecycle.

(c) Software development efforts will use the appropriate contract terms or conditions to allow for refinement of the requirements based on the evolution of the software solution. Cost-reimbursement-type, labor hour, incentive and/or hybrid contract clauses and provisions for the software development activities of an effort should be used to the maximum extent possible. Firm fixed price-type contract clauses and provisions will be minimized for software development activities.

(d) Source selection strategies will be tailored to support software development efforts. Vendor proposals for such efforts will be evaluated based on several factors, including written proposals, oral presentations, and/or solution demonstrations to ensure a comprehensive evaluation of solutions. Past performance on software development efforts should be considered as part of the evaluation; this includes past performance on federal government contracts and commercial contracts.

(e) Contract deliverables for software development efforts will be based on software functionality rather than documentation, whenever possible.

(f) Materiel Release Authority (MRA) will be delegated to Program Executive Officers (PEOs) for software systems for which they oversee development. This includes both Software Materiel Release and Software Release processes. This delegation will better support a rapid and iterative software acquisition approach.

(g) Reference architectures, Modular Open Systems Approach, and design patterns will be used, to the maximum extent practical, when developing custom software solutions. This will enable adding, upgrading, and replacing software components with minimal impact to other components and the system, and increase interoperability with other systems.

(h) Customization to commercial software solutions will be minimized to limit risk to the government. Where appropriate, microservices will be used to add capabilities not present in commercial software solutions. Customization to commercial software should only proceed where potential cost and technical risks are understood and mitigated.

(i) All software-intensive acquisition programs, regardless of acquisition pathway, will consistently track and report established metrics to assess and manage the performance, progress, speed, developmental hours, cybersecurity, and quality of the software development. The ASA(ALT) will develop and publish the required metrics and reporting requirements.

(3) Initiative Lead. The ASA(ALT) is the lead. Support will be provided by the CIO; CG, Army Materiel Command (AMC); and the Assistant Secretary of the Army (Financial Management & Comptroller) (ASA(FM&C)).

(4) Timeline. The ASA(ALT) will issue interim implementing guidance for these requirements no later than five months from directive date.

d. Initiative 4—Establish a Digital Capabilities Contracting Center of Excellence to Improve and Streamline Contracting for Software.

(1) Background. Contracting for software requires specialized expertise to ensure contracting solutions provide the appropriate flexibility, incentivize modern development approaches, and ensure vendor accountability. Currently, however, contract actions for software development efforts are executed by contracting organizations across the Army with varying degrees of software-related expertise. As a result, some software development contracts and agreements in place today do not consistently support modern software development practices.

(2) Policy.

(a) Effective immediately, the Army Contracting Command at Aberdeen Proving Ground (ACC-APG) will be designated as the Contracting Center of Excellence for Digital Capabilities. The Senior Contracting Official (SCO) at ACC-APG will be designated the SCO for all digital procurements to ensure appropriate oversight of digital contract actions.

(b) Select organizations will be required to use the Center of Excellence for software contracts at initial operating capability (IOC) and full operating capability (FOC).

(i) At IOC, the Center of Excellence will be responsible for all new and select existing contracts for software development efforts executed by PEO Enterprise Information Systems; PEO Intelligence, Electronic Warfare & Sensors; PEO Command, Control, and Communications – Tactical; PEO Simulation, Training, and Instrumentation; and select contracts for the ACOMs, ASCCs, and DRUs.

(ii) Within three months of the date of this directive, the CG, AMC will submit to the Undersecretary of the Army a plan for reaching FOC and the proposed scope of contracts to be executed by the Center of Excellence at FOC. This plan will identify contracts across the PEOs, ACOMs, ASCCs, and DRUs that the Center of Excellence will execute, based on input from these organizations.

(c) The Center of Excellence will ensure its contracting personnel are trained in industry best practices related to procurement of software, including cybersecurity considerations, and can develop and execute Requests for Information (RFIs), Requests for Proposals (RFPs), contracts, and agreements in line with modern software best practices. This centralized expertise will enable streamlined and expedited timelines for contract development and award.

(d) For software contracts under its purview, the Center of Excellence, in coordination with the mission partner and cognizant contracting personnel, will assist in the development of contracting strategies, RFIs, RFPs, and source selection criteria, and will execute contracts and agreements.

(e) The Center of Excellence will be responsible for training other contracting centers on software procurement best practices. The Center of Excellence will provide guidance and support, as appropriate, to other Army contracting organizations. AMC will ensure the other contracting centers, once trained, implement the appropriate methods to enable modern software practices and ensure vendor accountability.

(f) The Center of Excellence will collaborate with industry in creative ways to ensure Army contracts support the objectives of this directive.

(3) Initiative Lead. The CG, AMC is the lead. Support will be provided by the ASA(ALT).

(4) Timeline. The Contracting Center of Excellence for Digital Capabilities will reach IOC no later than three months from the date of this directive and reach FOC no later than nine months from the date of this directive. Within three months of the date of this directive, the CG, AMC will submit to the Undersecretary of the Army a plan for reaching FOC and the proposed scope of contracts to be executed by the Center of Excellence at FOC.

e. Initiative 5—Establish the Software Management and Response Team (SMART) to Assist Army Commands & Organizations.

(1) Background. Successful execution of Army software development efforts requires input and review from personnel with expertise and experience in modern software development practices. While this type of expertise exists in various

organizations across the Army, it is not accessible at scale to support the many software development efforts underway across the Department. It is critical that the appropriate support is provided to organizations undertaking such efforts.

(2) Policy.

(a) The SMART will be established within the Office of the CIO to provide distributed support to and conduct advisory peer reviews of all software development efforts conducted by ACOMs, ASCCs, DRUs, and other Army organizations.

(b) The SMART will be staffed with software developers with a deep understanding of modem software development practices, including CI/CD, agile, lean, and DevSecOps, and cybersecurity considerations. Personnel in the SMART will have experience and familiarity with recurring challenges in Army software requirements, requests for proposals and information, contracts, and acquisition approaches that contribute to software development challenges.

(c) The SMART will perform the following primary functions: (1) assist with the development and deployment of software; (2) perform technical assessments of software development efforts; (3) evaluate progress of software development efforts; (4) review software architectures; (5) review RFIs and RFPs before release; and (6) review contracts and agreements before execution.

(d) When reviewing RFIs, RFPs, contracts, and agreements, the SMART will coordinate with and operate under guidance provided by the Contracting Center of Excellence for Digital Capabilities at ACC-APG.

(3) Initiative Lead. The CIO is the lead.

(4) Timeline. The CIO will establish a charter codifying the roles and responsibilities of the SMART and will issue guidance to the ACOMs, ASCCs, and DRUs for complying with the requirements of the SMART no later than three months from the date of this directive.

f. Initiative 6—Manage Software Development Efforts Not Subject to Formal Acquisition Oversight.

(1) Background. Currently, software development is conducted by many organizations across the Army, including ACOMs, ASCCs, and DRUs. As efforts executed by these organizations are conducted outside of the formal acquisition system, they are subject to less robust oversight and coordination processes. This can

lead to duplication of efforts, integration and interoperability challenges, and systems that are not maintained through a CI/CD model. Software development must be synchronized across the Army to ensure an appropriate return on investment and ensure users' needs are being met. To that end, the requirements identified at paragraph 5.f.(2) of this directive apply to ACOMs, ASCCs, and DRUs, and other Army organizations executing software development efforts outside of the formal acquisition system.

(2) Policy.

(a) Requirements for software development efforts executed by ACOMs, ASCCs, or DRUs will be reviewed by the appropriate functional domain lead and prioritized by the appropriate mission area lead before the effort can progress. Requirements will be captured in a format consistent with CNSs and SW-ICDs. Mission area and functional domain leads are identified at enclosure 3.

(b) For COTS software procurements, the appropriate functional domain lead will work with the Army CIO to ensure appropriate contract vehicles are being used to mitigate risk of duplicative solutions across the Army.

(c) ACOMs, ASCCs, and DRUs must implement User/Developer Teams for software development efforts, as required by paragraph 5.b. of this directive; organizations will submit biannual reports to the CIO illustrating compliance with this requirement.

(d) Effective six months from the date of this directive, ACOMs, ASCCs, and DRUs may not issue RFIs, RFPs, or award contracts or agreements that are primarily for software development efforts until the documents have been reviewed and assessed by the SMART, as established at paragraph 5.e. of this directive.

(e) ACOMs, ASCCs, and DRUs must work through one of the six contracting centers within the ACC when developing RFIs and RFPs, or to award contracts and agreements that are primarily for software development efforts. The centers include ACC-APG; ACC-New Jersey; ACC-Orlando; ACC-Redstone Arsenal; ACC-Rock Island; and ACC-Detroit Arsenal. This does not preclude organizations from leveraging non-Army contracting vehicles; in accordance with the requirements in AFARS 5117.502-1, these organizations must obtain approval from a SCO at one of the six contracting centers to leverage such vehicles.

(i) The Mission and Installation Contracting Command will not execute contracts or agreements that are primarily for software development efforts.

(ii) The United States Army Corps of Engineers, Army National Guard Bureau, and the United States Army Medical Command may continue to execute contracts through their respective contracting organizations; these contracting organizations will be subject to the guidance issued by the Contracting Center of Excellence for Digital Capabilities at ACC-APG.

(f) ACOMs, ASCCs, and DRUs executing software development efforts must submit a biannual report of software development efforts to the CIO. The CIO will issue guidance identifying the reporting requirements within three months of the date of this directive; reporting requirements will include total projected cost, development timeline, user base, and projected lifecycle.

(3) Initiative Leads. The CIO and ASA(ALT) are the leads. Support will be provided by the Director, OEM and CG, AMC.

(4) Timeline. The CIO will issue interim guidance implementing these requirements within three months of the date of this directive.

g. Initiative 7—Streamline Software Test Requirements.

(1) Background. Software is required to go through extensive Test and Evaluation (T&E) activities at various points throughout the lifecycle before it can be deployed. These processes are rigid in nature, and do not enable the speed or flexibility required by modern software development approaches. T&E processes must be modernized and streamlined to support modern software development practices.

(2) Policy.

(a) T&E representatives will be included throughout the lifecycle of the software development effort, to include the requirements development process to ensure requirements are testable and measurable, and the development of test plans and strategies.

(b) Test data reciprocity will be employed to the greatest extent possible to reduce or eliminate duplicative testing. The relevant Army operational test agency will leverage all available test data, including data from vendor testing and testing performed at a System Integration Laboratory, to inform operational assessments. Dedicated government testing will only be required when sufficient credible data from other sources is not available.

(i) RFIs and RFPs for software efforts will solicit vendor test plans and vendor specific data tools to be used (e.g., Modeling and Simulation (M&S), automated test tools, and digital twins). The relevant operational test agency will assist in reviewing responses to RFIs and RFPs to determine what test data can be used to inform operational assessments.

(ii) Contracts will require vendors to provide test plans for review. The relevant Army operational test agency will assess the test plans and provide recommendations to ensure the resulting data can be used for operational assessments.

(iii) The relevant Army operational test agency may conduct oversight of vendor testing to ensure data is suitable.

(c) The relevant Army operational test agency will leverage industry standards and data from vendor specific tools to the maximum extent possible to inform operational assessments (e.g., M&S, automated test tools, and digital twins).

(d) The relevant Army operational test agency will tailor test requirements based on a capability-based risk assessment of new capabilities and/or features to reduce test requirements when possible. The ASA(ALT), in partnership with the CG, Army Test & Evaluation Command (ATEC), will develop and publish guidance on how to perform a capability-based risk assessment of new capabilities and features.

(e) Automated testing and test methods will be used to the maximum extent practical.

(3) Initiative Lead. The ASA(ALT) is the lead to develop and issue policy implementing the above processes; the Army operational test agencies are responsible for executing the above processes. Support will be provided by the CIO.

(4) Timeline. The ASA(ALT) will publish interim guidance implementing the above processes no later than four months from the date of this directive.

h. Initiative 8—Modernize Cybersecurity Approaches To Enable Real-time Cyber Monitoring.

(1) Background. As the Army's reliance on software solutions grow, it becomes ever-more important to understand the risks systems can introduce to the network and to mitigate those risks to the greatest extent possible. The Risk Management Framework (RMF) establishes the continuous management of cybersecurity risk within the DoD. Current RMF implementation focuses on obtaining an Authority to Operate

(ATO), a status which approves an IT system for use on an Army network. The current ATO process is a manual, time consuming effort that can form the costliest step in developing and deploying software. Moreover, the static ATO process does not allow for real-time monitoring of cybersecurity risks.

(2) Policy.

(a) In accordance with reference 1.v., the Army has established and recognizes ATO reciprocity across Army organizations to reduce test requirements, documentation, and the associated costs in time and resources. This reciprocity will allow systems with an ATO from one Army organization to be readily accepted by other Army organizations.

(b) The Army will seek ATO reciprocity from the other Services and the Office of the Secretary of Defense (OSD) components.

(c) The Army will work with the Defense Information Systems Agency to automate RMF processes, to the maximum extent practicable, to decrease the time and workload required by the traditional ATO process.

(d) The Army will align Directive Authority for Cyberspace Operations and the ATO process to accelerate deployment and feedback based on threat intelligence.

(e) The Army will transition from the traditional ATO to a continuous ATO (cATO) process to enable real-time cybersecurity monitoring.

(i) No later than the second quarter of FY24, all software development conducted within Army authorized DevSecOps platforms will transition to a cATO delivery model for authorization by the Army Chief Information Security Officer.

(ii) The Army will identify additional DevSecOps platforms and toolsets that qualify for cATO delivery authorization for non-traditional software packages.

(iii) The Army will establish a continuous monitoring program with a defined set of prerequisites that must be in place before a system can transition from a traditional ATO to a cATO. This will enable other software development efforts to transition to cATO, as appropriate.

(f) Automated software assurance tools will be leveraged to ensure newly developed code meets a minimum threshold of quality and does not introduce weaknesses or vulnerabilities into the system.

(g) Cyber penetration testing will be iteratively performed to identify system vulnerabilities.

(3) Initiative Lead. The CIO is the lead. Support will be provided by the ASA(ALT); DCS, G-6; CG, AMC; and CG, ARCYBER.

(4) Timeline. The CIO will issue interim revised policy and guidance and update processes to implement the above requirements no later than four months from directive date.

i. Initiative 9—Modernize Approach to Software Cost Estimating.

(1) Background. The Army's adoption of modern software development and acquisition practices may create challenges in estimating near-term and life-cycle software development costs, which could result in inaccurate and non-comprehensive estimates for programs utilizing agile software development and CI/CD. Insufficient cost, effort, and technical data on historical agile software development projects, coupled with lack of detailed extended requirements planning, amplifies the challenges of modern software development cost estimating.

(2) Policy.

(a) The Army will investigate and employ new software cost estimating methods that support modern software development approaches.

(b) To enable this, the ASA(FM&C) will conduct research on methods used by industry and the other Services when developing software cost estimates; provide recommendations to Army senior leadership on which methods and supporting data metrics and inputs are most appropriate to enable valid approaches to cost estimating; and assess and validate the application of such data and methods to Army software costing.

(c) Requirements owners, program managers, and contracting personnel will work with ASA(FM&C) to help assess the most appropriate cost estimating method.

(3) Initiative Lead. The ASA(FM&C) is the lead. Support will be provided by the CG, AFC; CG, AMC; and ASA(ALT).

(4) Timeline. The ASA(FM&C) will publish interim guidance on implementing the above processes no later than six months from directive date. The ASA(FM&C) will reassess and validate the guidance every two years based on changing best practices.

j. Initiative 10—End Traditional Software Sustainment.

(1) Background. Software is no longer developed, tested, procured, operated, and sustained sequentially. Modern software development requires adoption of a CI/CD model where software is continuously and iteratively developed and upgraded throughout the development lifecycle. However, current processes do not support this model. Current fiscal rules dictate that systems that have transitioned to sustainment are limited to Operations and Maintenance, Army (O&MA) funding, which can only be used for minor software modifications. This construct prevents software from being iteratively developed throughout its lifecycle. To that end, the Army must change the way software is supported.

(2) Policy.

(a) Historic approaches and procedures for software sustainment in acquisition programs will transition to enable a CI/CD model. Software support activities for acquisition programs scheduled to transition in FY24 or later will no longer be funded by a central sustainment fund; instead, funding will be allocated directly to program offices. Materiel developers will identify software support funding requirements through the annual Program Objective Memorandum process.

(b) For systems employing a CI/CD model or planning for future software capability development, this may require Research, Development, Test & Evaluation funding. For systems that do not anticipate future capability development, this may require O&MA funding. The DCS, G-8 will establish the appropriate funding line(s) to enable the PEOs and Project Managers to resource support activities for the programs.

(c) Systems that have already transitioned to sustainment will continue to be supported by AMC using O&MA funding. By exception, these systems may identify if they require funding other than O&MA to support future capability development.

(d) Materiel Developers are responsible for full lifecycle support of software system/components. As part of the acquisition strategy, Materiel Developers will consider leveraging existing and organic Army software expertise to execute software support activities, maximize software development effectiveness, and meet statutory core software requirements.

(3) Initiative Lead. The DCS, G-8 is the lead. Support will be provided by the ASA(ALT); CG, AMC; ASA(FM&C), and DCS, G-4.

(4) Timeline. The DCS, G-8 will publish interim guidance on implementing the above processes no later than four months from the date of this directive.

k. Initiative 11—Enable Data Centric Interoperability.

(1) Background. Currently, the Army has a complicated data environment, where data is stovepiped across various communities and systems. The Army must shift emphasis from network and system-centric approaches to data centric policies and approaches. This will allow the Army to effectively generate, organize, prioritize, and use data products across the business and warfighting enterprise and enable data-informed decisions.

(2) Policy.

(a) The Army will update the Army Data Plan and related policies to align with the following data mesh principles to enable data centric interoperability in and between enterprise and tactical environments:

(i) Decentralized domain-oriented data ownership and architecture.

(ii) Data-as-a-Product designed to meet decision makers' information needs at echelon.

(iii) Self-serve data infrastructure for data product production, discovery, and consumption.

(iv) Federated governance with automated enforcement through robust metadata.

(b) No later than three months from the date of this directive, the Army will define a data reference architecture which provides data mesh technical architecture implementation guidance for all Army programs with data centric capabilities.

(c) The Army will develop a plan for incrementally implementing the revised Army Data Plan, updated policy guidance, and reference architecture for applicable Army programs with the goals of advancing data interoperability with agile software development and providing enterprise data services to facilitate multiple programs. As needed, the Army will update contractual requirements in RFPs.

(d) Data Stewards and Functional Data Managers will identify the data products needed to execute current and future doctrine as described in the Decision Driven Data

CONOPS. The Mission Command Center of Excellence within the TRADOC Combined Arms Center (CAC) will lead data stewardship responsibilities Command & Control Information Systems with support from the associated Centers of Excellence.

(3) Initiative Lead. The CIO; ASA(ALT); CG, TRADOC; and CG, AFC will lead. Support will be provided by the DCS, G-3/5/7; DCS, G-6; DCS, G-8; and Director, OEM.

(4) Timeline.

(a) The CIO will update the Army Data Plan and related policies to align with above policy no later than three months from the date of this directive.

(b) The ASA(ALT) will define a data reference architecture no later than three months from the date of this directive. As applicable, programs will ensure new contracts include reference architecture conformance as a contracted requirement for software development efforts no later than six months from the directive date.

(c) Data Stewards and Functional Data Managers will identify needed data products to support "Fix/Pivot" and Army 2030 division as the unit of action design no later than six months from directive date. With initial technical oversight from the Army Chief Digital and Artificial Intelligence Office and assistance from the DCS, G3/5/7, the CG, CAC (through the Mission Command Center of Excellence) will establish the data products needed for this effort.

l. Initiative 12—Enhance Talent Management To Develop Digitally Skilled Workforce.

(1) Background. Modern software practices require a skilled workforce to ensure the Army continues to advance cutting edge digital skills while creating a culture of continuous development necessary to keep pace with the changes required to meet mission needs.

(2) Policy.

(a) The Army will expand the use of specialized training programs for select technical workforces. Organizations across the requirements, acquisition, contracting, sustainment, testing, and cyber communities will develop plans to upskill their respective workforces to enable modern software development practices. The plans will identify roles and responsibilities, competencies, and training required; and identify recurring training requirements to ensure the workforce remains up to date on evolving software development practices.

(b) Functional domain leads, identified at enclosure 3, will comply with training requirements established by the Director, OEM.

(c) The Assistant Secretary of the Army (Manpower & Reserve Affairs) (ASA(M&RA)) will explore innovative ways to attract and retain technical talent, including the use of special pay scales.

(d) The ASA(M&RA) will develop career progression maps to inform career development for the digital workforce that exists across career fields.

(3) Initiative Leads. The ASA(ALT); CIO; Director, OEM; DCS, G-6; CG, AFC; CG, AMC; CG, ATEC; and ASA(M&RA) are the leads for their respective workforces. Support will be provided by the DCS, G-1.

(4) Timeline.

(a) The ASA(ALT); CIO; Director, OEM; DCS G-6; CG, AFC; CG, AMC; and CG, ATEC will submit plans to upskill their respective workforces to enable modern software development practices to the Undersecretary of the Army and the Vice Chief of Staff of the Army no later than three months from the date of this directive.

(b) The ASA(M&RA) will submit to the USA and VCSA recommendations to attract and retain technical talent no later than three months from the date of this directive.

6. Governance. The Undersecretary of the Army and Vice Chief of Staff of the Army will monitor progress in implementing the requirements of this directive. Initiative leads will provide monthly updates. The Undersecretary of the Army will designate one organization responsible for managing implementation and ensuring continued progress between monthly updates.

7. Proponent. The ASA (ALT) has oversight responsibility for this policy and will ensure that proponents incorporate its provisions into the following Army regulations (ARs) within 2 years of the date of this directive:

a. The ASA(ALT) will update AR 70–1, AR 73-1, and AR 700–127.

b. The DCS, G-3/5/7 will update AR 5–22.

c. The DCS, G-8 will update AR 5–11 and AR 71–9.

8. Duration. This directive is rescinded on publication of the revised regulations.

Encls

Christine E. Wormuth

DISTRIBUTION: (see next page)
Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Futures Command
U.S. Army Pacific
U.S. Army Europe and Africa
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Strategic Command
U.S. Army Cyber Command
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Human Resources Command
U.S. Army Corrections Command
Superintendent, U.S. Military Academy
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency
Executive Director, Military Postal Service Agency
Director, U.S. Army Criminal Investigation Division
Director, Civilian Protection Center of Excellence
Superintendent, Arlington National Cemetery
Director, U.S. Army Acquisition Support Center

CF: (see next page)

CF:
Principal Cyber Advisor
Director of Enterprise Management
Director, Office of Analytics Integration
Commander, Eighth Army

REFERENCES

a. Title 10, United States Code, section 2460 (10 U.S.C. 2460) (Definition of depot-level maintenance and repair)

b. 10 U.S.C. 2464 (Core logistics capabilities)

c. 10 U.S.C. 2466 (Limitations on the performance of depot-level maintenance of materiel)

d. Federal Acquisition Regulation, Title 48 (Federal Acquisition Regulations System), Chapter 1 (Federal Acquisition Regulation)

e. Government Accountability Officer (GAO), GAO-23-105867 (Defense Software Acquisitions: Changes to Requirements, Oversight, and Tools Needed for Weapon Programs), July 2023

f. GAO-23-106059 (2023 Weapon Systems Annual Assessment), June 2023

g. Defense Federal Acquisition Regulation Supplement, Part 201 (Federal Acquisition Regulations System)

h. Department of Defense (DoD) Directive 5000.01 (The Defense Acquisition System), 9 September 2020, incorporating Change 1, effective 28 July 2022

i. DoD Instruction 5000.02 (Operation of the Defense Acquisition System), 23 January 2020; incorporating Change 1, effective 8 June 2022

j. DoD Instruction 5000.74 (Defense Acquisition of Services), 10 January 2020, incorporating Change 1, effective 24 June 2021

k. DoD Instruction 5000.75 (Business Systems Requirements and Acquisitions), 2 February 2017, incorporating Change 2, effective 24 January 2020

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

m. DoD Instruction 5000.81 (Urgent Capability Acquisition), 31 December 2019

n. DoD Instruction 5000.85 (Major Capability Acquisition), 6 August 2020, incorporating Change 1, effective 4 November 2021

o. DoD Instruction 5000.87 (Operation of the Software Acquisition Pathway), 2 October 2020

p. DoD Instruction 5000.89 (Test and Evaluation), 19 November 2020

q. DoD Instruction 5000.90 (Cybersecurity for Acquisition Decision Authorities and Program Managers), 31 December 2020

r. DoD Instruction 5000.91 (Product Support Management for the Adaptive Acquisition Framework), 4 November 2021

s. DoD Financial Management Regulation 7000.14-R, Budget Formulation and Presentation Volume 2A, Chapter 1 (Para 2.12.2.3), October 2008

t. DoD Directive 8115.01 (Information Technology Portfolio Management), October 2005

u. DoD Instruction 8115.02 (Information Technology Portfolio Management Implementation), October 2006

v. DoD Instruction 8510.01 (Risk Management Framework (RMF) for DoD Information Technology), 19 July 2022

w. DoD Software Modernization Implementation Plan, March 2023

x. Under Secretary of Defense for Acquisition and Sustainment memorandum (Use of the Software Acquisition Pathway for Defense Business Systems), 24 August 2022

y. Department of Defense Digital Engineering Strategy, June 2018

z. DoD Defense Science Board Task Force (Design and Acquisition of Software for Defense Systems), February 2018

aa. DoD Defense Innovation Board (Software Acquisition and Practices (SWAP) Study Report), May 2019

bb. Army Federal Acquisition Regulation Supplement, Part 5101 (Federal Acquisition Regulation System)

cc. Army Regulation (AR) 5–11 (Management of Army Modeling and Simulation), 30 May 2014

dd. AR 5–22 (The Army Force Modernization Proponent and Integration System), 13 July 2023

ee. AR 25–1 (Army Information Technology), 15 July 2019

ff. Army Regulation 70–1 (Army Acquisition Policy), 10 August 2018 gg. Army Regulation 71–9 (Warfighting Capabilities Determination), 29 June 2021

hh. Army Regulation 73–1 (Test and Evaluation Policy), 8 June 2018

ii. Army Regulation 700–127 (Integrated Product Support), 22 October 2018

jj. Secretary of the Army memorandum (Army Knowledge Management (AKM) Guidance Memorandum – Capabilities-Based Information Technology (IT) Portfolio Governance), 20 July 2005

DEFINITIONS

Business Mission Area (BMA). Includes all information technology investments characterized as Defense Business Systems. (AR 25-1)

Capability Need Statement (CNS). A high-level capture of mission deficiencies or enhancements to existing operational capabilities, features, interoperability needs, legacy interfaces and other attributes that provides enough information to define various software solutions as they relate to the overall threat environment. (DAU)

Continuous Authority to Operate (cATO). The core concept of a cATO is to build software security into the software development methodology so that the authority-to-operate process (as with the testing process) is executed alongside development. If executed correctly, an authority to operate is nearly guaranteed once the software is release ready. (DoDI 5000.87)

Cost-Reimbursement Contract. Cost-reimbursement types of contracts provide for payment of allowable incurred costs, to the extent prescribed in the contract. These contracts establish an estimate of total cost for the purpose of obligating funds and establishing a ceiling that the contractor may not exceed (except at its own risk) without the approval of the contracting officer. (FAR 16.301)

Data Reference Architecture. A data reference architecture is a set of documents that provides recommended structures and integrations of products and services to form a solution to enable to exchange of data products.

Data Stewards. Data stewards establish policies governing data access, use, protection, quality, and dissemination. (DoD Data Strategy)

Development, Security, and Operations (DevSecOps). An organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor. In DevSecOps, testing and security are shifted left through automated unit, functional, integration, and security testing - this is a key DevSecOps differentiator since security and functional capabilities are tested and built simultaneously. (DoDI 5000.87)

Defense Intelligence Mission Area (DIMA). A DoD-level Mission Area which includes IT investments within the Military Intelligence Program and Defense component programs of the National Intelligence Program. The Army is responsible for Army-specific intelligence IT systems. (AR 25-1)

Enterprise Information Environment Mission Area (EIEMA). Includes all IT investments that facilitate the implementation, operation, security, and enterprise services for the Army portion of the DOD Information Network. (AR 25-1)

Functional Data Managers. Functional data managers implement policies and manage day-to-day quality. (DoD Data Strategy)

Functional Domain. Collections of similar capabilities that are grouped at a high level in order to support decision-making, capability delegation, and analysis. (AR 25-1) A subset of the Mission Area portfolio that aligns to areas of common operational and functional requirements. (AR 5-1)

Low-Code/No-Code Development Activities. Software development consisting of rapid assembly of limited, customer-facing applications or solutions which require minimal or no manual computer programing effort.

Mission Area. A defined area of responsibility with functions and processes that contribute to mission accomplishment. (AR 25-1)

Microservices. Microservices are both an architecture and an approach to software development in which a monolith application is broken down into a suite of loosely coupled independent services that can be altered, updated, or taken down without affecting the rest of the application. (DoD Enterprise DevSecOps Reference Design Version 1.0 12 August 2019 Department of Defense (DoD), Chief Information Officer)

Modern Software Development Practices. Practices (e.g., lean, agile, DevSecOps) that focus on rapid, iterative development and delivery of software with active user engagements. Small cross-functional software development teams integrate planning, design, development, testing, security, delivery, and operations with continuous improvement to maximize automation and user value. (DoDI 5000.87)

Modular Open Systems Approach (MOSA). An approach to design systems with highly cohesive, loosely coupled, and severable modules that can be competed separately and acquired from independent vendors. (DAU)

Non-Traditional Software Packages. Software that is not developed for normal operating system such as linux and windows, but instead will operate on different systems such as mobile and embedded devices.

Software Development Effort. For the purposes of this directive, a "software development effort" is defined as: (a) development of a custom software solution; (b) customization, integration, or modification of a commercial software solution; and (c) software as a service.

Software Intensive. A system in which software represents the largest segment in one or more of the following criteria: system development cost, system development risk, system functionality, or development time. (DoDI 5000.87)

Warfighter Mission Area (WMA). Includes all IT investments related to mission-command, warfighting operations, training, and readiness. (AR 25-1)

MISSION AREA AND FUNCTIONAL DOMAIN LEADS

In accordance with references 1t, 1u, 1ee, and 1jj, information technology (IT) investments across the Department of Defense (DoD) are managed as portfolios to ensure IT investments support the DoD's vision, mission, and goals; ensure efficient and effective delivery of capabilities to the warfighter; and maximize return on investment. The Army categorizes IT investments within four mission areas, including the Business Mission Area, Enterprise Information Environment Mission Area, Warfighter Mission Area, and Army Component of the Defense Intelligence Mission Area. Within each mission area, IT investments are further grouped into subordinate functional domains based on common operational and functional requirements. The following mission area and functional domain organizational leads are responsible for IT investment decisions:

1. Business Mission Area (BMA) Lead: Director, OEM

Functional Domains	Leads
Acquisition	ASA (ALT)
Financial Management	ASA (FM&C)
Human Resources	ASA (M&RA) and DCS, G-1
Installations, Energy and Environment	DCS, G-9
Logistics and Sustainment	DCS, G-4
Training and Readiness	DCS, G-3/5/7

2. Enterprise Information Environment Mission Area (EIEMA) Lead: DCS, G-6

Functional Domains	Leads
Common Services Infrastructure	DCS, G-6
Common Transport	DCS, G-6
Cybersecurity	DCS, G-6
DoDIN Operations	CG, NETCOM
Information Technology Fiscal	CIO
Spectrum Management	DCS, G-6
Unified Network Operations	DCS, G-6

3. Warfighter Mission Area (WMA) Lead: DCS, G-3/5/7

Functional Domains	Leads
Battlespace Awareness	DCS, G-2
Focused Logistics	DCS, G-4
Force Application	DCS, G-8
Mission Command	DCS, G-3/5/7
Protection	DCS, G-3/5/7
Training	DCS, G-3/5/7

4. Army Component of the Defense Intelligence Mission Area (DIMA) and Domain Lead: DCS, G-2