DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

AD-GOV-SV-042

SAIS-AD (25-1rrrr)

27 August 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Software Management and Response Team Agile Software Development Project Support Requests

1. References. See Enclosure 1.

2. Purpose. To provide guidance on the criteria to initiate an agile software development project support request, also referred to as a “Phoenix Project” request, in accordance with reference 1a.

3. Applicability. This memorandum expands upon the existing policy guidance established in reference 1a and applies to the following:

a. Organizations: Regular Army, Army National Guard, and the U.S. Army Reserve.

b. Equipment: 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.

4. Background. Per reference 1a, the CIO established the Software Management and Response Team (SMART) on 10 April 2024 to provide distributed support to, and conduct peer reviews of, all software development efforts conducted by ACOMs, ASCCs, DRUs, and other Army organizations.

a. The CIO authorized SMART to perform the following functions: (1) assist with the development and deployment of software; (2) perform technical assessments of software development artifacts; (3) evaluate progress of software development efforts; (4) review software architectures; and (5) review Requests for Information (RFIs) and Requests for Proposals (RFPs) before release; and (6) review contracts and agreements before execution.

b. This guidance establishes criteria to initiate an agile software development support request in coordination with SMART and receive their continued support to enable a project’s successful software development.

5. Guidance.

a. A Phoenix Project is defined as an advisory review of a software development project. All Phoenix Projects will be approved by the CIO to be performed by SMART, also referred to as Team Phoenix. CIO may adjust Phoenix project scope.

b. All Phoenix Project requests must be endorsed by a GS-15/O-6 or SES/GO level organizational sponsor and shall be submitted to the Phoenix Project Office, by way of the Director of Team Phoenix, for approval by the CIO. For contact information to submit project requests, reference Section 7 of this memorandum.

c. The project request shall include: 1) Contact information for the requesting organization; 2) a problem statement which describes the project issue and/or challenge to be addressed, and 3) key area(s) of project support that are needed. Categories of SMART Team Phoenix support include:

(1) Overall Software Modernization Support: Includes, but not limited to, user interface/user experience (UI/UX); continuous integration/continuous delivery (CI/CD) adoption; software architecture upgrades; and user/developer feedback loops. Potential software outcomes and recommendations could also include streamlined software development practices, agile methodologies, low-code no-code platforms which could result in a reduction in cost, application redundancy, overhead or need for custom development wholistically.

(2) Software Contract Support: Involves, but not limited to, evaluating contract type and translating technical requirements into contract language for further contract assistance and execution; evaluating and advising on the utilization and effectiveness of software contracts and Software-as-a-Service contracts; reviewing contract deliverables, structure, and statement of work to ensure government and vendor specific responsibilities are clearly defined; incorporating and optimizing a CI/CD model for execution and delivery; and coordinating with the Army Contracting Command and the Digital Capabilities Center of Excellence to streamline and shorten acquisition timelines and processes with modern agile software delivery language.

(3) Cybersecurity Assessment: Involves analyzing software modernization needs to advance the security of the application, by identifying common vulnerabilities and exposures (CVE) reductions; architecture; and capitalize security automation throughout the software lifecycle.

(4) Soldier Safety: Includes modernizing how information is gathered, aggregated, used, or displayed within the U/I at the application layer to ensure PII and other sensitive data is properly protected and secured within the application.

(5) Legacy System Funding Reductions: Includes recommendations on a modern way to deliver a legacy software capability through modern CI/CD models, potentially reducing cost or redundancies.

d. Once a Phoenix Project request is approved, Team Phoenix will:

(1) Provide advisory and lifecycle support for software efforts to include software customization, integration or modification of commercial-off-the-shelf (COTS) or government-off-the-shelf (GOTS) solutions; software-as-a-service; and/or Development, Security, and Operations (DevSecOps) practices.

(2) Provide advisory support for software developed, or acquired, outside of the formal acquisition processes by ACOMs, ASCCs, DRUs, or other Army organizations.

(3) Provide advisory support to ACOMs, ASCCs and DRUs for requirements development, capability needs statements, RFIs, RFPs, source selection criteria, contract language and agreements pertaining to those software development efforts.

(4) Provide technical assessments of the software development efforts to include software architecture design reviews and recommendations; evaluations of software development progress; contracting evaluations before execution; application security reviews; CI/CD pipeline facilitation; and agile methodology implementation support.

(5) Provide advisory recommendations to the CIO as to whether a software development effort should become a formalized acquisition Program of Record. If affirmed, the CIO will leverage established processes to provide the recommendation to the appropriate authorizing organization.

(6) Provide advisory support for COTS software purchases.

e. Phoenix Projects, to include approved advisory support services, are centrally funded by the CIO and shall be completed within three (3) to six (6) months upon approval.

6. Duration. This guidance is effective immediately and stays in effect until superseded, rescinded, or incorporated into Army regulation. The OCIO, Architecture Data and Standards Directorate will review this memorandum for updates annually by 1 October of each calendar year.

7. Points of Contact (POCs):

a. CIO Policy Inbox: usarmy.pentagon.hqda-cio.mbx.policy-inbox@army.mil

b. OCIO, Army Analytics Group: Ms. Lauren C. Pavlik, Director of Team Phoenix, at lauren.c.pavlik.civ@army.mil.

c. OCIO, Architecture Data and Standards Directorate: Dr. Gregory C. Smoots, Deputy Director, at gregory.c.smoots.civ@army.mil.

GARCIGA.LEONEL.T.1186170411
Digitally signed by GARCIGA.LEONEL.T.1186170411
Date: 2024.08.27 15:53:43 -04'00'

3 Encls
1. References
2. Project Submission Guidelines
3. Definitions

LEONEL T. GARCIGA
Chief Information Officer

DISTRIBUTION
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 Corrections Command
U.S. Army Human Resources 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 Investigative Division
(CONT)

DISTRIBUTION: (CONT)
Director, Civilian Protection Center of Excellence
Director, U.S. Army Joint Counter-Small Unmanned Aircraft Systems Office
Superintendent, Arlington National Cemetery
Director, U.S. Army Acquisition Support Center

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

REFERENCES

a. AD 2024-02 (Enabling Modern Software Development and Acquisition Practices), 11 March 2024.

b. DoD CIO (DoD DevSecOps Fundamentals Guidebook: DevSecOps Activities & Tools), Version 2.2, 25 May 2023. [Online]. Available: https://dodcio.defense.gov/Library/

c. DoD CIO (DoD Software Modernization Implementation Plan Summary), March 2023 [Online]. Available: https://dodcio.defense.gov/Library/

d. DoD CIO (DoD Software Modernization Strategy), Version 1.0, Nov 2021 [Online]. Available: https://dodcio.defense.gov/Library/

e. DoD CIO (DoD Enterprise DevSecOps Strategy Guide), Version 2.1, September 2021 [Online]. Available: https://dodcio.defense.gov/Library/

f. DoD CIO (DoD Enterprise DevSecOps Fundamentals), Version 2.1., September 2021 [Online]. Available: https://dodcio.defense.gov/Library/

g. DoD CIO (DoD DevSecOps Playbook), Version 2.1, September 2021 [Online]. Available: https://dodcio.defense.gov/Library/

h. DoD CIO (DoD Enterprise DevSecOps Pathway to a Reference Design), September 2021 [Online]. Available: https://dodcio.defense.gov/Library/

i. Defense Innovation Board (Software Acquisition and Practices (SWAP) Study Report), May 2019 [Online]. Available: https://innovation.defense.gov/software/

j. Office of the Deputy Assistant Secretary of Defense for Systems Engineering (DoD Digital Engineering Strategy), June 2018 [Online]. Available: https://apps.dtic.mil/sti/citations/AD1068564

k. AR 25-1 (Army Information Technology).

PHOENIX PROJECT SUBMISSION GUIDELINES

A Phoenix Project request must be endorsed by a GS-15/O-6 or SES/GO level organizational sponsor and shall be submitted to the Phoenix Project Office, by way of the Director of Team Phoenix, for approval by the CIO.

Prior to submitting a Phoenix Project request, ACOMs, ASCCs, and DRUs, should consider and internally evaluate the following:

1) Is this a technology or business process problem to be solved?

2) Are there other capabilities similar within the DoD?

3) Could a low-code / no-code platform be utilized to resolve this problem?

4) Is this a new Commercial off the Shelf product to be evaluated or a custom development need?

If a Phoenix Project request is not accepted / approved by the CIO, Team Phoenix will provide the requesting organization with recommendations to help address their problem statement. As an example, these recommendations may include, but are not limited to: 1) identifying an opportunity for the requesting organization to collaborate with another Army organization on software development; 2) offering assistance to facilitate a technical exchange discussion; 3) providing a recommendations on how Team Phoenix would resolve the problem; 4) providing a recommendation to submit a Capability Needs Statement to either the Army Business Council or Army Unified Network Council for approval to continue and receive an APMS record; and/or 5) providing suggestions to address elements which resulted in the request being denied.

DEFINITIONS

Continuous Build. Continuous build is an automated process to compile and build software source code into artifacts. The common activities of continuous build include compiling code, running static code analysis, and executing unit tests. The outputs from continuous build are build results, build reports, and artifacts stored into an artifact repository.

Continuous Delivery. Continuous delivery is a continuation of continuous integration to ensure that a team can release the software changes to production quickly and in a sustainable way. The outputs of continuous delivery are a release go/no-go decision and released artifacts, if the decision is to release.

Continuous Integration. Continuous integration goes one step further than continuous build. It extends continuous build with more automated tests and security scans. The outputs from continuous integration include the continuous build outputs, plus automation test results and security scan results.

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)

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)

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.