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

CS-SEC-SC-039

SAIS-CS (25-1rrrr)

2 August 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Mobile Applications Vetting and Approval Guidance

1. References.

a. AR 25-2 (Army Cybersecurity Program).

b. HQDA CIO/G-6 memorandum (Mobile Application Authorization Process for Vetting and Analyzing Mobile Applications), 06 January 2017.

c. National Information Assurance Partnership (Protection Profile for Mobile Device Fundamentals), Version 3.3, 12 September 2022.

d. DoDI 8510.01 (Risk Management Framework for DoD Systems).

2. Purpose. This memorandum provides the mobile application authorization process and outlines the steps required for authorizing officials (AOs) to take when authorizing mobile applications that connect to Army Systems in Commercial and DoD mobile application stores. In addition, this policy identifies three paths for deployment that are available for Army mobile applications.

3. Applicability.

a. Per Army Regulation (AR) 25-2, para 2-7, the Army Chief Information Officer (CIO), on behalf of the Secretary of the Army, establishes policy, resourcing, and oversight of the Army Cybersecurity Program. This policy memorandum meets provisions outlined in AR 25-2, para 1-8, where the Army CIO, when needed, will issue policy memoranda to amplify guidance for the policies in AR 25-2. This guidance applies to all Army mobile applications to include training and non-training mobile applications.

b. This policy memorandum applies to any new mobile application that will connect to Army Systems for data systems.

4. Background.

a. U.S. Army Training and Doctrine Command's Army University (ArmyU), Vice Provost for Digital Education (VPDE), Mobile Division developed a process endorsed by the Army Audit Agency that ensures mobile application content is validated, approved, and does not duplicate existing solutions. In June 2016, ArmyU, VPDE Mobile Division was trained by DISA to vet applications and given access to all tools and processes necessary for evaluating mobile applications to DISA standards.

b. Nett Warrior has an established path to production for tactical mobile application feature enhancements, mission specific needs, code analysis, app deployments and fielding using the Watchtower Tactical Marketplace.

5. Policy. Effective upon signature, this memorandum rescinds reference b and provides updated guidance on mobile application vetting and approval and establishes the mobile application authorization process in this memo as the authoritative process to evaluate and approve Army mobile applications.

6. Roles and Responsibilities.

a. ArmyU, VPDE, Mobile Division and AOs will follow the process established by DISA:

(1) Establish and maintain a phased mobile application submission and evaluation process, internally developed apps and followed immediately by mobile applications submitted through their process and approved for release by associated commands.

(2) Evaluate Army mobile applications in accordance with DISA and National Information Assurance Partnership Protection Profile requirements.

(3) Ensure mobile applications meet the criteria specified in the "Non-tactical Pathway to Production" listed below, before being approved for use on Army information technology and networks.

(a) Analysis - Content and Data Review / Determine Needs.

(b) Analysis II - Nomination Process and Review by Board.

(c) Design and Development Review.

(d) Approval Board for AOs:

- Staff Judge Advocate
- Foreign Disclosure
- Public Affairs Office
- Operation Security
- Cybersecurity/Information Assurance

(e) Implementation of Approved Mobile Product.

(f) Release to Commercial Application Stores or DoD Mobility Unclassified Capability (DMUC) DISA Store for Government devices.

(4) Complete the required remediation and mitigation of identified deficiencies or vulnerabilities in the mobile application code.

(5) Produce the Army mobile application risk acceptance letter for Army CIO signature.

(6) Load all desired apps and necessary artifacts into DISA's DoD Application Vetting Environment (D.A.V.E.) system for tracking.

(7) Coordinate with DISA Mobility Program Management Office for government devices, to ensure Army apps and signed artifacts are uploaded into the D.A.V.E. system, to ensure:

(a) Vetted and authorized Army mobile applications are available in the DMUC Mobile Application Store within five days of receipt of artifacts from the Army DCS G-6.

(b) A label within the mobile device manager is created to segregate Army mobile applications from non-Army users.

(8) Publish to Mobile App Gateway Database within five days of Risk Acceptance letter.

b. Army AOs will follow these requirements for AO approval of a mobile app to a commercial phone store.

(1) Clean source code scan (no Category I, or Category II).

(2) Source code committed and stored to a government approved code repository.

(3) Ports and Protocols in accordance with DISA requirements.

(4) Application signing keys in accordance with DoD requirements.

(5) Encryption of data at rest and in transit in accordance with DoD standards.

(6) AO review and approval of end-user authentication and authorization.

c. The CISO will:

(1) Serve as the designated HQDA element that accepts risk on behalf of the Army by reviewing and signing the Army Mobile Application Risk Acceptance letter prepared by the organization.

(2) Acknowledge, accept, and authorize mobile applications which are for Army and joint partner use.

d. HQDA DCS G-6 will:

(1) Publish implementation guidance to provide operational level direction on the mobile application lifecycle within the Army enterprise, as required.

(2) Provide analysis and recommendation to the Army CIO, for mobile applications, properly vetted through the agreed process.

(3) Ensure the Army leverages the DoD mobile enterprise capabilities and tools as required.

7. Process. Watchtower Tactical Marketplace mobile applications and updates will follow this path to production:

a. The AO approves the mobile application for operational use.

b. The tactical mobile code is uploaded to the Watchtower portal to see and manage apps. Nett Warrior program office will oversee how the application is fielded.

c. Developers will submit app releases for review by the Nett Warrior's program office.

d. App releases will be reviewed and tested by Nett Warrior's program office for security, change requests and configurations and to ensure that application does not inhibit Nett Warrior functionality.

e. Upon AO, program and cybersecurity reviews and approval, app releases can be used but releases will be available based on operational and position needs. Additional testing (Army interoperability certification/Army tactical network) is required for applications with tactical interoperability requirements.

f. Government-owned and government unlimited rights source code must be stored and maintained in an authorized government repository.

8. Certification. Command CIOs will certify compliance in writing with the requirements set forth herein, as used by TRADOC, to the Office of the CIO Cybersecurity Directorate/Policy Division for Army CIO approval.

9. Policy Review. The OCIO Policy & Risk Governance Division (SAIS-CSP) will review this policy annually, or as required, and update as appropriate.

10. Points of contact.

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

b. SAIS-CSP Policy Team: usarmy.pentagon.hqda-cio.mbx.sais-csp@army.mil.

c. HQDA CIO, Army Analytics Group (AAG): Ms. Lauren Pavlik, lauren.c.pavlik.civ@army.mil.

d. HQDA DCS G-6: Mr. John R. Walsh, john.r.walsh46.civ@army.mil.

GARCIGA.LEONEL.T.1186170411 Digitally signed by GARCIGA.LEONEL.T.1186170411 Date: 2024.08.05 18:01:43 -04'00'

Encl

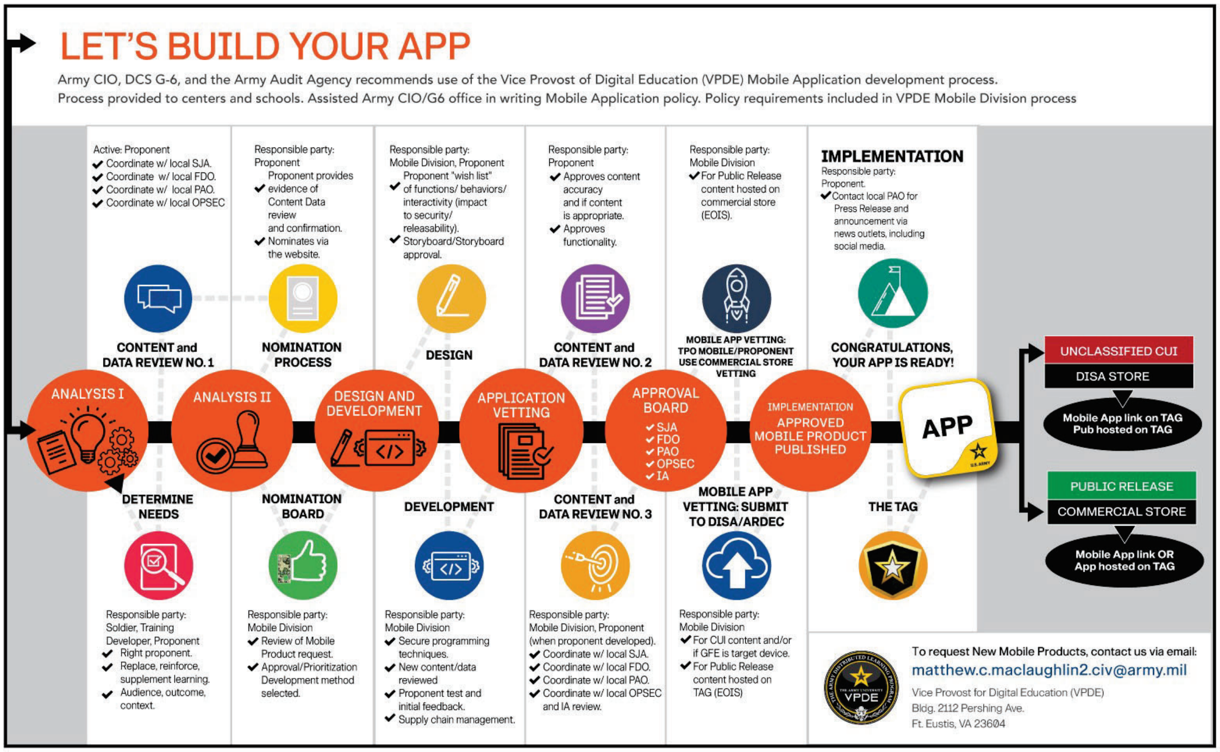
LEONEL T. GARCIGA
Chief Information Officer

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
(CONT)

DISTRIBUTION: (CONT)
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
U.S. Army Recruiting 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
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

Non-tactical Pathway to Production



LET'S BUILD YOUR APP

Army CIO, DCS G-6, and the Army Audit Agency recommends use of the Vice Provost of Digital Education (VPDE) Mobile Application development process. Process provided to centers and schools. Assisted Army CIO/G6 office in writing Mobile Application policy. Policy requirements included in VPDE Mobile Division process

Active: Proponent
- ✓ Coordinate w/ local SJA.
- ✓ Coordinate w/ local FDO.
- ✓ Coordinate w/ local PAO.
- ✓ Coordinate w/ local OPSEC

CONTENT and DATA REVIEW NO. 1

Responsible party: Proponent
- ✓ Proponent provides evidence of Content Data review and confirmation.
- ✓ Nominates via the website.

NOMINATION PROCESS

Responsible party: Mobile Division, Proponent
- ✓ Proponent "wish list" of functions/ behaviors/ interactivity (impact to security/ releasability).
- ✓ Storyboard/Storyboard approval.

DESIGN

Responsible party: Proponent
- ✓ Approves content accuracy and if content is appropriate.
- ✓ Approves functionality.

CONTENT and DATA REVIEW NO. 2

Responsible party: Mobile Division
- ✓ For Public Release content hosted on commercial store (EOIS).

MOBILE APP VETTING: TPO MOBILE/PROPONENT USE COMMERCIAL STORE VETTING

IMPLEMENTATION

Responsible party: Proponent.
- ✓ Contact local PAO for Press Release and announcement via news outlets, including social media.

CONGRATULATIONS, YOUR APP IS READY!

ANALYSIS I

ANALYSIS II

DESIGN AND DEVELOPMENT

APPLICATION VETTING

APPROVAL BOARD
- ✓ SJA
- ✓ FDO
- ✓ PAO
- ✓ OPSEC
- ✓ IA

IMPLEMENTATION

APPROVED MOBILE PRODUCT PUBLISHED

APP

UNCLASSIFIED CUI

DISA STORE

Mobile App link on TAG Pub hosted on TAG

PUBLIC RELEASE

COMMERCIAL STORE

Mobile App link OR App hosted on TAG

DETERMINE NEEDS

Responsible party: Soldier, Training Developer, Proponent
- ✓ Right proponent.
- ✓ Replace, reinforce, supplement learning.
- ✓ Audience, outcome, context.

NOMINATION BOARD

Responsible party: Mobile Division
- ✓ Review of Mobile Product request.
- ✓ Approval/Prioritization Development method selected.

DEVELOPMENT

Responsible party: Mobile Division
- ✓ Secure programming techniques.
- ✓ New content/data reviewed
- ✓ Proponent test and initial feedback.
- ✓ Supply chain management.

CONTENT and DATA REVIEW NO. 3

Responsible party: Mobile Division, Proponent (when proponent developed).
- ✓ Coordinate w/ local SJA.
- ✓ Coordinate w/ local FDO.
- ✓ Coordinate w/ local PAO.
- ✓ Coordinate w/ local OPSEC and IA review.

MOBILE APP VETTING: SUBMIT TO DISA/ARDEC

Responsible party: Mobile Division
- ✓ For CUI content and/or if GFE is target device.
- ✓ For Public Release content hosted on TAG (EOIS)

THE TAG

To request New Mobile Products, contact us via email:
matthew.c.maclaughlin2.civ@army.mil

Vice Provost for Digital Education (VPDE)
Bldg. 2112 Pershing Ave.
Ft. Eustis, VA 23604

Enclosure