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

**ZA-SEC-SC-015**

SAIS-ZA (25-1rrrr) 1 March 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Software as a Service Usage and Management

1. References: See enclosure.

2. Purpose. Establish Army guidance for sponsorship and usage of Software as a Service (SaaS) applications.

3. Applicability.

a. This guidance addresses three main topics:

(1) Headquarters, Department of the Army (HQDA) visibility of Army requests for Cloud Service Offering (CSO) Provisional Authorizations (PA) sponsorship.

(2) Enforcement and accountability of continuous monitoring of SaaS.

(3) Reinforcement of SaaS Cybersecurity Requirements.

b. This guidance applies to Army organizations and activities using SaaS (as defined in reference 1a).

4. Background.

a. The use of SaaS is increasing throughout the Army, resulting in growing amounts of Army data residing in SaaS applications. The Army must be prepared to respond in the event of a cybersecurity incident involving SaaS applications.

b. This guidance aims to minimize the risk of such incidents by providing clear direction on the sponsorship and usage of SaaS applications.

5. Guidance.

a. Submit all new requests to sponsor a Cloud Service Provider or CSO for a Department of Defense (DoD) PA to the Army Enterprise Cloud Management Agency

(ECMA) for review and approval via email; see the point of contact (POC) at paragraph 9b.

(1) The request will minimally include the name of the SaaS application and the impact level.

(2) The request must be submitted prior to engagement with the DoD Cloud Authorization Services (DCAS) team. This process ensures visibility and oversight of Army-sponsored SaaS applications and enables the ECMA to assess potential risks and benefits associated with each request.

b. Submit a request for all use of non-Army authorized (for example, Joint authorized) SaaS applications to ECMA for review and approval via the POC at paragraph 9b.

c. In accordance with the Deputy Under Secretary of the Army's guidance (see reference 1b), all SaaS usage must be coordinated with ECMA prior to acquisition, via the POC at paragraph 9b.

d. System Owners and Authorizing Officials (AOs).

(1) System Owners must ensure APMS records are properly updated to reflect current use of SaaS applications.

(2) System Owners and AOs are responsible to ensure CSOs operating under their purview have a valid DoD Provisional Authorization (PA) in accordance with references 1c and 1d. System Owners must verify an Army ATO for the SaaS application is approved prior to processing Army data within the SaaS application.

(3) AOs are fully accountable for operating SaaS applications at an acceptable level of risk to the Army. AOs must perform due diligence to ensure cybersecurity risks are minimized in the operation of all SaaS applications. Due diligence must include a comprehensive review of artifacts from the Defense Information Systems Agency (DISA) cloud authorization process such as (but not limited to) third party assessment organization (3PAO) assessment results, System Security Plans (SSPs), Security Assessment Reports (SARs), and Plan of Actions & Milestones (POAMs).

(4) System Owners and AOs must satisfy essential cloud cybersecurity requirements (see references 1e and 1f) and provide evidence upon request.[*]

[*] Sub-paragraphs 5c(5)(a)–(f) are addressed in DFARS 252.239-7010. Sub-paragraphs 5c(5)(g)–(h) are addressed in DFARS 252.204-7012(c).

(a) The System Owner must implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG).

(b) The System Owner must report all cyber incidents that are related to the cloud computing service via https://dibnet.dod.mil/dibnet/.

(c) The System Owner must discover and isolate malicious software in connection with a reported cyber incident.

(d) The System Owner must preserve and protect images of all known affected information systems identified in a cyber incident and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report.

(e) The System Owner must provide access to additional information or equipment that is necessary to conduct a forensic analysis.

(f) When a damage assessment is required, the System Owner must ensure all of the damage assessment information is gathered in accordance with sub-paragraph (5)(d).

(g) System Owners must ensure cyber incidents are reported within 72 hours of discovery.

(h) When the System Owner discovers and isolates malicious software in connection with a reported cyber incident, System Owners must submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3.

(i) System Owners must ensure system activities are logged to an immutable destination. Such logs must provide an audit trail that support the functions outlined in Department of Defense Instruction (DoDI) 8530.01 (see reference 1g).

(j) While FedRAMP and the DISA Cloud Assessment Division are responsible for administering the Continuous Monitoring (ConMon) processes, Army AOs are still responsible to review the results of continuous monitoring processes such as (but not limited to) Plan of Action & Milestones (POA&Ms), continuous monitoring data, DISA's Authorization Recommendation and PA memos, FedRAMP continuous monitoring reports, Detailed Finding Reviews (DFRs), and Corrective Action Plans (CAPs) to ensure SaaS applications are operated at an acceptable level of risk to the Army.

6. Implementation. System Owners are responsible for ensuring compliance with this guidance and any future updates.

7. Exceptions. Army organizations may request an exception to this guidance in writing.
a. Submit requests to ECMA via the POC at paragraph 9b.

b. Requests for exception must include a justification (including cost and mission impacts) and ECMA will adjudicate each request based upon cost and risk.

8. Expiration and review. This guidance is effective immediately and remains in effect until superseded or rescinded. ECMA will review this guidance for update annually no later than 1 October of each calendar year.

9. POCs:

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

b. ECMA Inbox: armycloud@army.mil

c. ECMA: Ms. Rosalynn Pittman, (571) 644-8631, rosalynn.s.pittman.civ@army.mil

GARCIGA.LEONEL.T.1186170411 Digitally signed by GARCIGA.LEONEL.T.1186170411 Date: 2024.03.01 15:22:40 -05'00'

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
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
(CONT)

DISTRIBUTION: (CONT)

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

## REFERENCES


a. NIST SP 800-145 (The NIST Definition of Cloud Computing), September 2011, p. 2. Available at https://csrc.nist.gov/pubs/sp/800/145/final

b. DUSA memorandum (Army Enterprise Cloud Services and Modernization), 15 January 2021. Available from usarmy.pentagon.hqda-cio.mbx.policy-inbox@army.mil

c. DFARS SUBPART 239.76—Cloud Computing. Available at https://www.acq.osd.mil/dpap/dars/dfars/html/current/239_76.htm

d. DoD Cloud Computing Security Requirements Guide, Version 1, Release 4. Available at https://public.cyber.mil/dccs/

e. DFARS 252.239-7010 (Cloud Computing Services). Available at https://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7010

f. DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting). Available at https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

g. DoDI 8530.01 (Cybersecurity Activities Support to DoD Information Network Operations). Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf

h. DFARS 252.239.7009 (Representation of Use of Cloud Computing). Available at https://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7009

i. DoDI 8500.01 (Cybersecurity). Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

j. Office of the DoD CIO, Requirements for the Acquisition of Digital Capabilities Guidebook, February 2022. Available at https://dodcio.defense.gov/Library/

k. GO 2020-01 (Assignment of Functions and Responsibilities within Headquarters Department of the Army)

l. AR 25-1 (Army Information Technology)

m. AR 25-2 (Army Cybersecurity)

n. AR 380-5 (Army Information Security Program)

o. AFARS, Appendix HH. Available at https://www.acquisition.gov/afars/appendix-hh-table-contents