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

ADS-GOV-CP-011

SAIS-ADS (25-1rrrr)

23 April 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Chief Information Officer, Army Information Technology (IT) Standards and Compliance Policy

1. References. See Enclosure 1.

2. Purpose. This memorandum provides the Army IT Standards and Compliance Policy (ASCP) within the Department of the Army (DA). The ASCP ensures that Army IT, including its National Security Systems (NSS), meets Department of Defense (DoD) IT standards for new acquisitions and updates to existing systems, as per Title 10 of the United States Code (U.S.C.) (reference 1a) and DoD Instruction (DoDI) 8310.01 (reference 1b).

3. Background. The Army Chief Information Officer (CIO) develops, coordinates, and implements an assessment process that applies to the Department (DoD Directive (DoDD) 5144.02 (reference 1c) and DoDI 8310.01.

4. Applicability. The provisions of this guidance apply to all Army organizations responsible for developing, updating, or procuring Army IT, including its NSS.

5. Guidance. All Army organizations developing, updating, or procuring IT, including its NSS, must use applicable IT standards, including data standards, prescribed in the DoD IT Standards Registry (DISR). Appropriate IT standards are critical to achieving system interoperability across the force.

a. All Army organizations developing, updating as applicable, or procuring IT, including NSS, must submit a change request or waiver (see Enclosure 2) to the OCIO if they use standards other than mandated or emerging for an acquisition program.

b. All Army organizations developing, updating as applicable, or procuring IT, including NSS, must ensure compliance with IT standards prior to fielding and have record available to the OCIO, reflecting system conformance.

c. The Office of the Chief Information Officer (OCIO) will recommend, advocate for, and coordinate new or retired IT standards and ensure system conformance to the

approved standards within the DISR accessible from the Joint Assessments and Standards Management (JASM) portal (https://jasm.apps.mil).

d. The OCIO will provide assessments according to the CIO guidance memorandum (reference 1d) for compliance with 40 U.S.C. (the Clinger-Cohen Act) (reference 1e).

e. The OCIO will provide support to Army IT systems requiring a change request or waiver to use IT standards other than mandated or emerging for acquisition programs. All Army organizations will coordinate their requests for approval through the Milestone Decision Authority (MDA), the Army OCIO, and the DoD CIO. (See Enclosure 2 for a waiver request template.)

f. The OCIO will complete reviews of standards-based artifacts to support the management of IT standards compliance for the Army.

g. The OCIO will establish policy and provide oversight and governance of Army IT standards management in support of IT system interoperability across the Army, the Joint Force and Multinational partners (to include Federated Mission Networking (FMN) and American, British, Canadian, Australian, and New Zealand (ABCANZ) standards).

6. Benefits. The ASCP will enable compliance and effective IT standards management, supporting the development of new acquisitions and updates to existing systems. It will also allow the OCIO to advocate for change while ensuring the maintenance of system interoperability.

7. Effective date. This clarifying guidance on the ASCP is effective immediately and will be revised in the AR 25-1 and DA PAM 25-1-1 revisions on the next version.

8. Points of contact.

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

b. Dr. Gregory C. Smoots, Chief, Standards and Compliance, at gregory.c.smoots.civ@army.mil.

GARCIGA.LEONEL.T.1186170411 Digitally signed by GARCIGA.LEONEL.T.1186170411 Date: 2024.04.23 06:13:27 -04'00'

Encls

LEONEL T. GARCIGA
Chief Information Officer

DISTRIBUTION: (see next page)

SAIS-ADS (25-1rrrr)
SUBJECT: Chief Information Officer, Army Information Technology (IT) Standards and Compliance Policy

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 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

REFERENCES

a. Armed Forces, 10 U.S.C., Sections 2222, 2223, and 2224 (2016).

b. DoDI 8310.01 (Information Technology Standards in the DoD).

c. DoDD 5144.02 (DoD Chief Information Officer (DoD CIO)).

d. CIO memorandum (U.S. Army Chief Information Officer Standardization of Clinger-Cohen Act Compliance Guidance), 01 December 2023.

e. Clinger-Cohen Act 40 U.S.C., Subtitle III, Section 11315 (1996).

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

g. DA Pam 25-1-1 (Army Information Technology Implementation Instructions)

h. Executive Order 12333 (United States Intelligence Activities), as amended.

i. Executive Order 13231 (Critical Infrastructure in the Information Age), as amended.

j. DoDI 5000.82 (Requirements for the Acquisition of Digital Capabilities).

k. DoDI 8330.01 (Interoperability of Information Technology, Including National Security Systems).

l. DoDI 4120.24 (Defense Standardization Program).

m. DoDI 5000.75 (Business Systems Requirements and Acquisition).

n. DoDI 8320.07 (Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense).

o. DoD JESC (Standard Operating Process (SOP)), 21 December 2022.

p. Secretary of the Army (Army Digital Transformation Strategy), 12 October 2021.

WAIVERS To Army IT STANDARDS POLICY. ICW OSD, Army CIO may approve, in coordination with the DoD CIO, waivers to use other than mandated or emerging standards for acquisition programs where the Component head is the MDA.

DoD IT Standard Compliance Waiver Request for DoD CIO Approval		
System Name:	**System Acronym:**	**System DITPR ID:**
Requesting Organization:		
Organizational POC Name, Phone, and Email:		
Program Manager's Name, Phone, and Email:		
IT Standard Identifier for this waiver request: **(E.g., IEEE 802.10b)**	**IT Standard Title for this waiver request:** **(E.g., Secure Data Exchange, 1992)**	
What is the rationale for using this IT standard that is retired or not registered in the DISR?		
What are the risks or operational limitations due to implementing this IT standard that is retired or not registered in the DISR?		
How will these risks or operational limitations be mitigated?		
What are the risks or operational impacts if the waiver request is denied?		
What is the Plan of Action and Milestones for future implementation of an applicable IT standard that is registered in the DISR as mandated or emerging?		
Requestor Digital Signature:		
DoD CIO Decision and signature: **Approved; Approved with Conditions; or Disapproved: _____** **Comments/Conditions:** **DoD CIO E-Signature:**		
JESC Waiver Identifier (assigned by the DoD JESC Secretariat):		