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

ADS-GOV-NA-020

SAIS-ADS (25-1rrrr)

24 April 2024

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Chief Information Officer Guidance for Interoperability of Information Technology, Including National Security Systems

1. References. See Enclosure 1.

2. Purpose. This memorandum refines policy and provides direction for certifying the interoperability of Information Technology (IT) and National Security Systems (NSS) pursuant to Sections 2222, 2223, and 2224 of Title 10, United States Code.

3. Background.

a. Pursuant to Title 10, Section 2223 (reference 1a), the Army Chief Information Officer (CIO) is responsible for ensuring that Army IT and NSS are interoperable with other relevant IT and NSS of the Government and the Department of Defense.

b. The CIO is responsible for Army IT and NSS meeting Department of Defense (DoD) interoperability requirements for new acquisitions or updates to existing systems, pursuant to Title 40 U.S. Code Section 11315 (reference 1b), Department of Defense Directive (DoDD) 5000.01 (reference 1c), Department of Defense Instruction (DoDI) 5000.02 (reference 1d), and DoDI 8330.01 (reference 1e).

c. On 03 May 2023, HQDA EXORD 157-23 in support of (ISO) Army Interoperability Certification (AIC) (reference 1f) provided guidance for modernizing AIC mission functions.

d. Pursuant to DoDI 8330.01, the Army CIO shall establish policy and guidance and provide oversight for developing a capability-focused, architecture-based approach to achieve IT interoperability.

4. Guidance.

a. The Army OCIO will coordinate with ASA(ALT), Program Executive Offices (PEOs) or Program Managers (PMs) to execute the following:

(1) PMs will develop and execute test process(es) with sufficient rigor to validate IT and NSS interoperability and submit the proposed test process(es) to the Army CIO for certification. The ASA (ALT), PEOs, or PMs are authorized to certify systems and software as interoperable.

(2) ASA (ALT), PEOs, or PMs will meet Army-Defined Trigger Definitions (Enclosure 2) for IT and NSS prior to fielding. When fielding IT and NSS that do not meet Army-Defined Trigger Definitions, follow the Revised Non-Interoperability Self Determination Process (reference 1g).

(3) PMs will certify that IT and NSS are interoperable within their intended environment prior to fielding and comply with Army and DoD interoperability regulations, directives, and instructions per paragraph 3a.

(4) PMs will submit IT and NSS certifications to the appropriate Milestone Decision Authority and Materiel Release Authority as required.

(5) PEOs can approve interoperability waivers or exemptions when IT and NSS have no interoperability requirement. The approved IT and NSS waiver or exemption must be submitted to the appropriate Milestone Decision Authority and Materiel Release Authority.

(6) PMs will submit IT and NSS certifications, waivers, and exemptions in a timely manner to HQDA, DCS G-6.

(7) ASA (ALT) will provide the OCIO with an initial assessment identifying plans to support and resource the test and certification mission.

b. HQDA, DCS G-6 is the functional sponsor for the operational interoperability and interface requirements that ASA (ALT), PEOs, or PMs will use to execute interoperability certification testing.

c. This guidance further clarifies prior guidance related to Army Interoperability Certification provided in AR 25-1 and DA Pam 25-1-1.

5. Expiration and review.

a. This guidance is effective immediately and remains in effect until superseded or rescinded.

b. The OCIO Standards and Compliance Division will review this guidance for updates annually by 1 October of each calendar year.

6. Points of contact.

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

b. OCIO Standards and Compliance Division: Dr. Gregory C. Smoots, (703) 692-0537, gregory.c.smoots.civ@army.mil.

GARCIGA.LEONEL.T.1186170411 Digitally signed by GARCIGA.LEONEL.T.1186170411 Date: 2024.04.24 16:34:31 -04'00'

Encls

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 Human Resources Command
U.S. Army Corrections Command
U.S. Army Recruiting Command
(CONT)

DISTRIBUTION: (CONT)
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. Title 10, United States Code, Section 2223 (2011)

b. Title 40, United States Code, Section 11315 (2012)

c. DoDD 5000.01 (The Defense Acquisition System)

d. DoDI 5000.02 (Operation of the Adaptive Acquisition Framework)

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

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

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

h. DoDI 4120.24 (Defense Standardization Program)

i. AR 25-1 (Army Information Technology)

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

k. HQDA EXORD 157-23 m(ISO Army Interoperability Certification (AIC) Modernization), 03 May 2023

l. HQDA, DCS G-6 memorandum (Revised Non-Interoperability Self Determination Process), 25 June 2023

Army-Defined Trigger Definitions

AIC Testing Triggers:
(DoDI 8330.01 – September 2022)
Any new capabilities that impact the following net-ready capabilities will trigger an AIC.

Net Ready Capabilities
- Technical Exchange of Information
- Data
- Services
- End-to-end operational effectiveness

Army Defined
- Message Formats
- System Features (interface with SoS)
- Ports & Protocols
- Data Exchanges
- Gateways

Trigger	Definition	Examples
Message Formats	Associated with a new and untested communication standard.	VMF 6017, 6017A
System Features	Associated with a new and untested capability that sends, receives, or manipulates data and information to an external system. PM defined hardware dependency.	Map Engines, Chat, Collaboration Tool
Data Exchanges	Associated with a new and untested interchange of data and its transformation between a SUT and external system, or significant modification to existing data exchange.	Direct DB exchange, New system interface, Meta Data Tagging
Ports and Protocols	Associated with the incorporation of a new and untested network protocol that determine how data is received or transmitted to an external system.	SSH (22), DNS (53), HTTPS (443)
Gateways	Associated with a new and untested change to the flow of information, data, or communication to an external system. A significant modifications to existing exchange (i.e., DDS content or rule-sets (DAP / DSP))	DDS, C2IVM