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

CS-SEC-SC-016

SAIS-CS (25-1rrrr)

15 April 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Cross Domain Solution Assessment and Authorization Policy

1. References: See enclosure.

2. Purpose: To establish a Cross Domain Solution (CDS) Assessment and Authorization (A&A) policy and assign responsibilities for the interconnection of information systems (IS) of non-intelligence security domains using CDS devices in accordance with the authority in DoDI 8540.01.

3. Applicability:

a. This policy governs all CDS devices of non-intelligence security domains and applies to Headquarters Department of the Army (HQDA) elements, Army Commands (ACOM), Army Service Component Commands (ASCC), Direct Reporting Units (DRU), and Army National Guard and Reserve components.

b. This policy applies to all Army secret and below interoperability (SABI) CDSs governed by the DoD connection approval process and managed by the Army HQDA G–6 Cybersecurity Directorate.

c. This policy is not applicable to the Joint Worldwide Intelligence Communications System for TOP SECRET–sensitive compartmented information (TS–SCI) or Special Access Program (SAP) systems.

4. Background:

a. Cross Domain Solutions are a key component to information dominance and warfighter operations by providing the ability to manually or automatically access or transfer information between different security domains. The introduction of commercial cloud technologies and issuance of Department of the Army (DA) Pamphlet 25-2-1 (Army Cross Domain Solution and Data Transfer Management) significantly changes the process for CDS utilization. The Army must strictly adhere to National Cross Domain Strategy and Management Office (NCDSMO) Raise the Bar (RTB) requirements.

b. Past instances of CDS were deficient from a development, deployment and use perspective. In November 2017, a revised RTB strategy for improving cross-domain cyber security was established. This RTB strategy is continually updated to align with emerging technologies and to ensure requirements are adjusted as needed.

c. Army CDS owners will maintain awareness of and ensure compliance with newly published NCDSMO and National Security Manager guidance to include National Manager Binding Operational Directives (NM BOD), National Security Manager (NSM) Emergency Directives (ED) and other regulatory guidance. Failure to comply can have negative impacts on CDS operations.

5. Roles & Responsibilities:

a. The Army Cross Domain Management Office (ACDMO) is the cross-domain support element (CDSE) for the Army, and provides CDS oversight at the Headquarters, Department of the Army (HQDA) level. ACDMO provides the following support related to the DoD connection approval process for SABI CDSs:

(1) Requirements.

(a) Requirements Approval: Unit requesting CDS must provide the ACDMO a cross domain validation and approval request (CDVAR). The CDVAR must be signed by a GS15/O6 with authority to obligate the necessary resources to purchase and maintain the CDS.

(b) Requirements Validation: The ACDMO will validate the operational requirement for a CDS on the DoDIN.

(2) CDS technology identification.

(3) Coordination with DoD agencies.

(4) Army sponsorship at CDS approval boards and/or panels.

b. The Army Enterprise Cloud Management Agency (ECMA) manages and maintains all approved CDS cloud service offerings for Cloud Army (cArmy).

c. System and Network Authorizing Officials are the senior federal officials/executives (SES/General Officer) with the authority to formally assume responsibility for operating, maintaining, and connecting the CDS at an acceptable level of risk to organizational operations.

d. The Information System Owner (ISO) is responsible for identifying the mission requirements for a CDS and initiates the CDS request process with the ACDMO.

6. Policy:

a. Army organizations and program offices must only request use of CDSs approved by the National Cross Domain Strategy and Management Office (NCDSMO). The baseline list of authorized CDSs can be found on SIPRNET at https://intelshare.intelink.sgov.gov/sites/ncdsmo. The ACDMO will validate the operational requirement for a CDS. Organizations and programs must then receive Defense Security/Cybersecurity Authorization Working Group (DSAWG) and Information Security Risk Management Committee (ISRMC) approval prior to implementation. The Army ACDMO office sponsors all Army CDS requirements packages through the DoD approval process.

b. All non-cloud CDSs requiring enterprise, tactical, or Point-to-Point (P2P) services are approved by the DSAWG and ISRMC. Use of an Enterprise Cross Domain Service Provider (ECDSP) is preferred. If a non-enterprise P2P solution is required, that organization may obtain a P2P exemption through the Army Chief Information Security Officer (CISO). This exception is only for the use of a non-enterprise P2P CDS that is on the approved NCDSMO list.

c. Information flow across different security domains is authorized by the responsible Network Authorizing Official (NAO) through the Authority to Connect (ATC), which is granted after DSAWG/ISRMC approval.

d. An independent Authority to Operate (ATO) is required for each network enclave CDS. The CDS authorization cannot be included in another authorization boundary and must have a unique eMASS record to identify the ATO. The Information System Owner (ISO) will ensure all CDSs are aligned for Defensive Cyber Operations (DCO) support. DCO is defined as the ability to utilize blue cyberspace capabilities to protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity.

e. ISOs will not procure CDS technology prior to gaining DoD level approval.

f. Army organizations must receive an Authorization to Operate (ATO) from a System Authorizing Official (SAO) and an Authority to Connect (ATC) from a Network Authorizing Official (NAO) to deploy, sustain and connect a CDS to its authorization boundaries. The SAO is responsible for making a risk-based authorization decision to operate and maintain the CDS. The NAO is responsible for a threat informed risk-based authorization decision to connect the CDS to the DoDIN-Army. The ISO retains the responsibility to deploy and operate a CDS, adhering to all CDS operational requirements from development until decommission. The ISO is responsible for producing the CDS concept of operations (CONOPS) document detailing the implementation of cross domain data workflows. Each CDS must receive a stand-alone (i.e., unique SIPRNET eMASS record) ATO and ATC for operational use. When a CDS and associated data crosses authorization or network boundaries (e.g., SIPRNET to MPE), the CDS requirement owner (ISO) and associated Network Authorizing Official (NAO) assume overall risk and responsibility.

g. CDS's that are specifically built for a platform (e.g., Abrams Tank) are novel entities. Platform CDS's will fall under a Type Accreditation know as Repeatable Accreditation Criteria. These systems will only need one eMASS record for each Platform with a notation showing how many are currently in operation (e.g., eMASS note: 1480 currently operating).

h. The ACDMO will maintain records of operational Unclassified, Secret and Coalition Army CDS and is the Army central authority for compliance oversight for non-intelligence community CDS.

i. Any CDS operating without an approved ATO/ATC or found to be non-compliant with approved security configurations will be reported immediately to the Authorizing Official and ADCMO. Non-compliant CDSs will be referred to the DSAWG/ISRMC for risk determination on continued use.

j. The HQDA, DCS, G-2 maintains records of operational intelligence community and Tops Secret–SCI CDS and is the Army central authority for compliance and oversight for intelligence community CDS.

7. POCs:

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

b. HQDA CIO Cybersecurity Directorate, Oversight and Compliance Division: Mr. Mack Bessemer, 850-384-1366, William.G.Bessemer.civ@army.mil

c. For CDS questions, contact HQDA DCS-G6: ACDMO, 703-545-4239; UNCLASSIFIED: usarmy.pentagon.hqda-cio-g-6.list.cdmo@army.mil; SECRET: usarmy.pentagon.hqda-cio-g-6.mbx.cdmo@mail.smil.mil

d. For questions about the use of a CDS in the ECMA cARMY cloud: Mr. Darek Kitlinski, 703-545-7133 or E-mail to armycloud@army.mil

GARCIGA.LEONEL.T.1186170411 Digitally signed by GARCIGA.LEONEL.T.1186170411 Date: 2024.04.15 10:00:13 -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
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
(CONT)

DISTRIBUTION: (CONT)
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. DoDI 8540.01 (Cross Domain Policy). Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/854001p.pdf

b. DA PAM 25-2-1 (Army Cross Domain Solution and Data Transfer Management). Available at https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1003057

c. NCDSMO (CDS Design and Implementation Requirements: 2021 Raise the Bar Baseline Release Version 4.1), 11 Jul 2022. Available via Intelink: https://www.nsa.gov/Cybersecurity/Partnership/National-Cross-Domain-Strategy-Management-Office/

d. NIST SP 800-53 Rev. 5 (Security and Privacy Controls for Federal Information Systems and Organizations), September 2020. Available at https://doi.org/10.6028/NIST.SP.800-53r5

e. DCPG Version 6.1, August 2023. Available at https://dl.dod.cyber.mil/wp-content/uploads/connect/pdf/unclass-DISN_CPG.pdf

f. Emergency Directive 2023-005 (Reducing Risk of Cross Domain Solutions for Internet Accessible Networks). Available on Intelink at https://intelshare.intelink.gov/sites/ncdsmo/Shared%20Documents/Policies/BOD,%20ED,%20NMM/NM%20ED-2023-005.pdf

g. DAMI-IM Policy No. CSP-MGMT-CA-010_A_A (Guidance for Army Non-Cryptologic SCI Systems Revision 1), 27 Jan 2021. Available on Intelink at https://intelshare.intelink.gov/sites/hqdag2/policy/default.aspx

h. DAMI-IM Policy No. CSP-TECH-SC_022_Army (Non-Cryptologic SCI CDS Policy), 20 May 2020. Available on Intelink at https://intelshare.intelink.gov/sites/hqdag2/policy/default.aspx

i. Defense IA Security Accreditation Working Group document (Criteria for Repeatable Accreditation Cross Domain Solutions, Version 1), 14 Nov 2014. Information at https://public.cyber.mil/connect/dsawg/