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

CS-SEC-RI-046

SAIS-CS (25-1rrrr)

4 October 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Amplifying Guidance for Type Authorization under Army Risk Management Framework

1. References.

a. AR 25-2 (Army Cybersecurity).

b. Office of the Secretary of Defense (Risk Management Framework (RMF) Knowledge Service (KS)). Online repository: https://rmfks.osd.mil.

c. NETCOM (RMF Implementation Operational Tactics, Techniques, and Procedures (TTP)).

d. HQDA, OCIO Memorandum (Information Technology Reciprocity Acceptance Guidance Memorandum), 03 November 2023.

2. Purpose. Provide initial guidance on Type Authorization (TA) roles and responsibilities to address current gaps in Army RMF execution, set conditions for integration of Department of Defense (DoD) Chief Information Officer (CIO) guidance, and develop business processes and policies critical for the implementation and execution of Unified Network Operations (UNO) across the Army.

3. Applicability.

a. Per Army Regulation (AR) 25-2, the Army 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, if applicable, will issue policy memoranda to amplify guidance for the policies in AR 25-2.

b. This policy applies to all Headquarters Department of the Army (HQDA) elements, Army Commands (ACOM), Army Service Component Commands (ASCC), Direct Reporting Units (DRU), and the Reserve Component (Army National and the Army Reserve).

c. This policy does not apply to Joint Worldwide Intelligence Communication System (JWICS) and Special Access Program (SAP) Networks.

4. Definition. TA is a reciprocity method for system authorization. It allows for a single security authorization package for a common version of a system and the issuance of a single authorization decision applicable to multiple, identical deployed instances of the same system into environments that meet the criteria stipulated in the authorization package and installation instructions. The system can then be deployed to multiple locations with any specific installation, security control, operational security and configuration requirements needs provided by the hosting enclave (reference 1b).

5. Background.

a. Current State. Army organizations execute TAs inconsistently and incompletely today. TA systems are operated by Army organizations across locations and Department of Defense Information Network (DoDIN) Areas of Operation (DAO). Consequently, TA systems are defended and continuously monitored differently across each location/DAO. Originating Organizations and System Authorizing Officials (SAO) cannot implement and assess all necessary security controls across all operating environment(s); therefore, Receiving Organizations must play an active role throughout system operations and coordinate continuous monitoring with Network Authorizing Officials (NAO).

b. Way Forward. The need to improve Army TAs is foundational to achieving UNOs, and the Army must take an iterative approach for this transition. This policy is an initial step that clarifies immediate roles and responsibilities. It is also the basis to develop and implement additional business processes (based on National Institute of Standards and Technology best practices) necessary to promote the required cybersecurity communication between Originating and Receiving Organizations. Once developed, the guidance will be institutionalized in follow-on policy and regulation.

6. Policy. The categorization, selection, implementation, assessment, authorization, and monitoring of TA systems are a shared responsibility, as follows:

a. System Authorizing Officials (SAO) will:

(1) Only conduct a TA for a system which does not have an approved authorization; for authorized systems, follow reciprocity guidance in reference d.

(2) Ensure TAs are appropriately categorized as such in the Enterprise Mission Assurance Support Service (eMASS).

(3) Ensure the information system owner (ISO)/program manager (PM) selects and implements controls appropriate for type authorized systems. The ISO/PM will tailor these controls to the archetype (common) version of a system. Follow-on policy and implementation guidance will standardize this process (to include notification of operating organization responsibilities) across the Army.

(4) Ensure the ISO/PM continuously monitors security controls in accordance with reference 1b for the common version of a system.

(5) Where practical, ensure the ISO/PM anticipates the operational environment(s) of the system and accounts for Authority To Connect (ATC) Critical Controls (reference 1c) early and throughout RMF.

(6) Authorize the common version of a system. This decision does not need to address operational, site-specific dependencies of the hosting environment for example, identification of a specific Cybersecurity Service Provider (CSSP), network topology and technical configurations external to the authorization boundary, operational personnel). Follow-on policy and implementation guidance will standardize this process of communicating responsibilities for operationally dependent controls across the Army.

(7) Include explicit statement in the Authorization to Operate (ATO) Terms and Conditions that security-relevant deviations from the TA will violate the Type ATO and establish a requirement for the system to be authorized by the organization who made the change.

(8) Ensure the ISO/PM communicates patches and updates in accordance with DoD and U.S. Cyber Command requirements and timelines, as feasible with current Army business processes until revised by policy.

(9) Ensure Receiving Organizations have access to the security authorization package and deployment instructions, including a current Plan of Action and Milestones (POA&M), as requested.

b. Control Assessors (CA) will formally evaluate the cybersecurity capabilities and services of Information Technology (IT) in accordance with reference 1c for TA systems.

(1) Evaluations will address all system security controls of the common version of a system that are applicable in the operational environment (for example, system access control, internal diagrams, logging).

(2) CAs will review security control tailoring as part of evaluations. This will help the SAO ensure the common version of a system implements the appropriate controls that do not depend on and/or vary by operational, site-specific dependencies of the hosting environment. CAs will document this as part of the authorization recommendation.

(3) Evaluations will not address security controls that depend on and/or vary by operational, site-specific dependencies of the hosting environment (for example, identification of a specific CSSP, network topology and technical configurations external to the authorization boundary, operational personnel). These controls will be evaluated as part of continuous monitoring. Follow-on policy and implementation guidance will standardize this process across the Army.

c. Receiving Organizations will:

(1) Deploy the system using configuration requirements in the security authorization package and deployment instructions.

(2) Provide all operationally dependent security controls, mitigations, or support functions required by the authorization. The critical task is to identify and integrate with an approved CSSP and execute continuous monitoring requirements.

(3) Notify Originating Organization ISO/PM of any new findings, such as new threats, discovered vulnerabilities, or similar information throughout the authorization life cycle.

(4) Coordinate with the NAO on any DAO-specific security requirements.

(5) Coordinate with the NAO when introducing baseline or configuration changes that deviate from the authorized common version of a system.

d. NAO will:

(1) Establish and enforce any DAO-unique security requirements.

(2) Ensure the Receiving Organizations address all operationally dependent security controls, mitigations, or support functions required by the authorization. The critical task is to ensure receiving organizations identify and integrate with an approved CSSP and execute continuous monitoring requirements.

(3) Determine if an additional assessment is required by the Receiving Organization for changes to any TA system.

7. Effective Date. This memorandum is effective immediately until rescinded.

8. Points of contact.

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

b. CIO RMF Inbox: usarmy.pentagon.hqda-cio-g-6.mbx.rmf-team@army.mil.

c. SAIS-CS: Ms. Suzanne Rodriguez, suzanne.p.rodriguez.civ@army.mil.

GARCIGA.LEONEL.T.1186170411
Digitally signed by GARCIGA.LEONEL.T.1186170411
Date: 2024.10.04 13:04:08 -04'00'

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
(CONT)

DISTRIBUTION: (CONT)
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