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

CS-SEC-RI-026
26 April 2024

SAIS-CS (25-1rrrr)

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Amplifying Guidance for an Interim Authorization to Test Under Army Risk Management Framework 2.0

1. References.

a. AR 25-2 (Army Cybersecurity).

b. DA PAM 25-2-14 (Risk Management Framework for Army Information Technology).

c. DA PAM 25-2-12 (Authorizing Official).

d. NETCOM (RMF 2.0 Implementation Operational Tactics, Techniques, and Procedures (TTP)).

e. NETCOM (Control Assessor TTP).

2. Purpose. Provide amplifying guidance to references 1a–e on the roles and responsibilities of an Interim Authorization to Test (IATT) under the Army Risk Management Framework (RMF) 2.0.

3. Background. The ability to rapidly test and securely deploy capabilities is a critical component of Army modernization. Within the Army RMF, a System Authorizing Official (SAO) may permit testing in the form of an IATT after meeting specific cybersecurity requirements. Reference 1d provides guidance on granting an IATT; however, this guidance does not address the RMF 2.0 processes (e.g., the role of a Network Authorizing Official (NAO), the relation to an Authority to Connect (ATC)). Information System Owners (ISO)/Program Managers (PM)s have experienced challenges and delays in receiving an IATT due to ambiguity in these process and responsibilities. This policy provides HQDA guidance to clarify and synchronize the conditions and responsibilities to grant and maintain an IATT.

4. Policy. Operation of a system under an IATT in an operational environment is for testing purposes only (i.e., the system will not be used for operational purposes during the IATT period).

a. IATTs shall be granted only when an operational environment or live data is required to complete specific test objectives.

b. IATTs shall expire at the completion of testing (shall not exceed 18-months).

c. For full and independent operational testing, an ATO (rather than an IATT) may be required if operational testing and evaluation is being conducted in the operational environment or on deployed capabilities.

d. The SAO, in granting an IATT, shall:

(1) Determine which of the ATC Critical Controls (reference 1d) is appropriate.

(2) Make the IATT decision based on a Security Assessment Report from a Security Controls Assessor (SCA) in accordance with reference 1e. A SCA-Organization may perform this function. This does not require review by the SCA-Army, U.S. Army Network Enterprise Technology Command (NETCOM).

(3) Document the IATT decision in eMASS to ensure visibility.

(4) Provide the list of all network services and cybersecurity requirements to the applicable NAO.

(5) Report IATT plan to the NAO so the NAO can provide guidance.

e. While an IATT does not require an ATC, a Network Authorizing Official may apply additional conditions for specific DoDIN area of operations, as per 4.d.(5).

5. Effective Date. This memorandum is effective upon signature and remains in effect until rescinded or superseded.

6. Points of contact.

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

b. SAIS-CS: Mr. Mack Bessemer, (571) 314-3846 or william.g.bessemer.civ@army.mil.

GARCIGA.LEONEL.T.1186170411
Digitally signed by GARCIGA.LEONEL.T.1186170411
Date: 2024.04.26 10:58:42 -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
- 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