

Army Regulation 525–15

Military Operations

**Software
Reprogramming
Policy for
Electronic
Warfare and
Target Sensing
Systems**

**Headquarters
Department of the Army
Washington, DC
23 July 2010**

UNCLASSIFIED

SUMMARY of CHANGE

AR 525-15

Software Reprogramming Policy for Electronic Warfare and Target Sensing Systems

This major revision, dated 23 July 2010--

- o Changes the title of the publication to Software Reprogramming Policy for Electronic Warfare and Target Sensing Systems (cover).
- o Updates guidance for software reprogramming of electronic warfare and target sensing systems (throughout).
- o Makes administrative changes (throughout).

Effective 23 August 2010

Military Operations

Software Reprogramming Policy for Electronic Warfare and Target Sensing Systems

By Order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:


JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

History. This publication is a major revision.

Summary. This regulation sets forth U.S. Army policy for software reprogramming for electronic warfare and target sensing systems. It covers managerial requirements necessary to implement electronic warfare and target sensing systems operations and training oversight for actions in peacetime and wartime, to include U.S. wartime reserve modes in order to administer counter threat changes. It establishes responsibility for Army counter-threat-change capabilities.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to all proponent agencies involved in research and development, acquisition, life cycle support, intelligence, planning and integration, and operations activities of electronic

warfare and target sensing systems requirements.

Proponent and exception authority.

The proponent of this regulation is Deputy Chief of Staff, G–3/5/7. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains management control provisions and identifies key management controls that must be evaluated (see appendix B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–3/5/7 (DAMO–ODE), Washington, DC 20310–3200.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and

Blank Forms) directly to Headquarters, Department of the Army (DAMO–ODE), Washington, DC 20310–3200.

Committee Continuance Approval.

The Department of the Army committee management official concurs in the establishment and/or continuance of the committee(s) outlined herein. AR 15–1 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the U.S. Army Resources and Programs Agency, Department of the Army Committee Management Office (AARP–ZA), 2511 Jefferson Davis Highway, 13th Floor, Taylor Building, Arlington, VA 22202–3926. Further, if it is determined that an established “group” identified within this regulation, later takes on the characteristics of a committee, as found in the AR 15–1, then the proponent will follow all AR 15–1 requirements for establishing and continuing the group as a committee.

Distribution. This regulation is available in electronic media only and is intended for command levels A, B, C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

*This regulation supersedes AR 525–15(S), dated 1 February 1993.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, *page 1*

Purpose • 1-1, *page 1*

References • 1-2, *page 1*

Explanation of abbreviations and terms • 1-3, *page 1*

Responsibilities • 1-4, *page 1*

Program objectives • 1-5, *page 1*

Chapter 2

Responsibilities, *page 1*

Assistant Secretary of the Army (Acquisition, Logistics, and Technology) • 2-1, *page 1*

Deputy Chief of Staff, G-2 • 2-2, *page 2*

Deputy Chief of Staff, G-3/5/7 • 2-3, *page 2*

Deputy Chief of Staff, G-4 • 2-4, *page 2*

Chief Information Officer/G-6 • 2-5, *page 2*

Deputy Chief of Staff, G-8 • 2-6, *page 2*

Commanding General, U.S. Army Materiel Command • 2-7, *page 2*

Commanding General, U.S. Army Training and Doctrine Command • 2-8, *page 3*

Commanding General, U.S. Army Intelligence and Security Command • 2-9, *page 3*

Commanders of Army Service Component Commands • 2-10, *page 4*

Commanders of Army Service Component Commands serving Geographic Combatant Commands • 2-11, *page 4*

Chapter 3

Counter-Threat-Change Strategic Overview, *page 4*

New and changed threats • 3-1, *page 4*

Rapid software reprogramming strategy • 3-2, *page 4*

Appendixes

A. References, *page 5*

B. Internal Control Evaluation, *page 6*

Glossary

Chapter 1 Introduction

1–1. Purpose

This regulation establishes policy, assigns responsibilities, and provides strategy for integration and interoperability of electronic warfare (EW) and target sensing systems (TSS). It also is the basis for Army policy for EW and TSS mission data programming; development and use of rapid software reprogramming (RSR); and operation of Army capability to identify and counter changes to threat system composition, capabilities, and signatures, to include providing the U.S. Army with effective counters to hostile introduction of new threat systems and changes to threat systems that impact the Army's ability to detect, classify, and engage the threat; providing security and preservation of friendly forces or equipment; providing the U.S. Army with an RSR capability that will assist commanders to attain tactical superiority, achieve surprise, gain and retain the initiative, and obtain decisive results; and maintaining vigilant data collection efforts to detect introduction of new threat systems or changes to existing threats to counter the new or changed threats.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Responsibilities

Responsibilities are listed in chapter 2.

1–5. Program objectives

The principal objective of providing EW and TSS operational software programming support is to detect and classify new and changed threats, and to provide mitigation to these changes in order to maintain the commander's operational tempo. Failure to respond to these changes in threat composition or signature may disrupt operations and negatively impact mission objectives. An emphasis on reducing ambiguity is required because of the covert nature of new and changing threats. The following objectives contribute to the Army's principal objective:

- a.* Field U.S. Army EW and TSS, target sensing smart weapons, and jammer systems that are software configurable and/or hardware modular that are able to adapt to hostile introduction of new and changed threats.
- b.* Field U.S. Army battlefield capabilities that incorporate counter threat changes.
- c.* Operate a sustained program to collect and evaluate employment, deployment, and signature information for systems operating in the electromagnetic spectrum. This program will be essential for providing friendly electronic protection and to successfully engage or defeat hostile or potentially hostile systems.
- d.* Maintain essential data about the U.S., Allied Forces, and coalition partner RSR and their counters to enemy capabilities while ensuring effectiveness of capabilities through thorough testing and evaluation.
- e.* Support U.S. forces and others with RSR as required.
- f.* Reduce the effects of new and changed enemy introduced threats.
- g.* Increase the friendly RSR effectiveness during operations.
- h.* Identify, assess, and develop common and multisensor EW and TSS that can identify threats in order to reduce the susceptibility of U.S. systems to enemy introduction of new and changed threats. Support situational awareness capability.

Chapter 2 Responsibilities

2–1. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

The ASA (ALT) will—

- a.* Ensure that sensor-based weapons and EW systems are developed using software reprogrammable signature detection, classification, and response capabilities.
- b.* Coordinate with the Deputy Chief of Staff, G–2 (DCS, G–2) and the Deputy Chief of Staff, G–3/5/7 (DCS, G–3/5/7) to support the direction and control of requirements development for the data production and database capabilities needed to support signature software reprogramming.
- c.* Provide staff coordination with the DCS, G–2, the DCS, G–3/5/7 (DAMO–ODE), and the Deputy Chief of Staff, G–8 (DCS, G–8) (DAPR–FDI) for the development of essential EW, TSS, and RSR identified through the Research, Development, and Acquisition Planning, Programming, Budgeting, and Execution System.

d. Coordinate with U.S. Army Materiel Command (AMC), within the scope of the National Disclosure Policy–1 (NDP–1), to encourage allied incorporation of friendly RSR capabilities into appropriate systems.

2–2. Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Coordinate with the Chief Information Officer/G–6 (CIO/G–6), the DCS, G–3/5/7, and the Commanding General (CG), AMC to ensure that sensor signature requirements are funded and integrated as requirements for collection, intelligence production, database maintenance, and research and development efforts as required by DODD 5250.01.

b. In coordination with the DCS, G–3/5/7, represent the Army Staff in Joint intelligence forums that discuss changes to threat system composition, capabilities, and signatures, and the means to counter those changes.

2–3. Deputy Chief of Staff, G–3/5/7

The DCS, G–3/5/7 will—

a. Validate the Army’s EW and TSS operational support infrastructure efforts to ensure that timely and effective software reprogramming is available to meet mission requirements.

b. Coordinate with the appropriate EW organization within Army Commands, Army Service Component Commands (ASCCs), Direct Reporting Units, and the Joint community to ensure the Army Reprogramming Analysis Team (ARAT) EW, TSS, and RSR operations are integrated, as applicable.

c. Develop RSR policy, programs, and force requirements for Active Army, Army National Guard/Army National Guard of the United States, U.S. Army Reserve, and U.S. Army Special Operations Command.

d. In coordination with AMC, ASA (ALT), and U.S. Army Training and Doctrine Command (TRADOC), ensure EW and TSS RSR are addressed in system requirements documents.

e. In coordination with the CIO/G–6, ensure EW and TSS electronic attack (EA) systems deconfliction within the electromagnetic spectrum. Provide spectrum management necessary to protect communications while permitting essential EA operations.

f. Coordinate RSR matters with the other military Services and allies, as permitted by disclosure and security classification guidance.

g. Validate and oversee the Army’s contribution to North Atlantic Treaty Organization Emitter Database and U.S. Electromagnetic System Database.

h. In coordination with the DCS, G–2, represent the Army Staff in Joint intelligence forums that consider counter-threat-change matters and advise other counterparts.

2–4. Deputy Chief of Staff, G–4

The DCS, G–4 will—

a. Ensure that logistical policies support the capability to perform software installation and RSR at the platform or weapons level.

b. In conjunction with the DCS, G–2, ensure the Army Reprogramming Analysis Team–Program Office (ARAT–PO) is involved in the development, delivery, and maintenance of any RSR capability provided under foreign military sales.

2–5. Chief Information Officer/G–6

The CIO/G–6 will—

a. Serve as the liaison to relevant Army and Joint technical and user groups served by ARAT for EW, TSS, and RSR to ensure proper bandwidth and priority.

b. Ensure and support secure and classified communications, information management, and information technology capability for RSR functions.

c. Coordinate RSR information management and information technology hardware, infrastructure, and access requirements with ARAT–PO.

2–6. Deputy Chief of Staff, G–8

The DCS, G–8 will—

a. Coordinate with AMC (ARAT–PO) for review and validation of requirements to compete for resources during the program objective memorandum and program budget review process.

b. Plan and program resources for ARAT research, development, test, and evaluation activities.

2–7. Commanding General, U.S. Army Materiel Command

The CG, AMC will—

a. Designate via the Communications-Electronic Command (CECOM), the ARAT–PO as the CECOM-Life Cycle Management Command Software Engineering commander for—

(1) The EW and TSS software reprogramming infrastructure.

- (2) The RSR capability assessment for operational EW and TSS.
- (3) Support of EW and TSS research and development programs.
 - b.* Provide the ARAT-PO with the resources and facilities necessary to provide timely EW and TSS software reprogramming as necessary to meet Warfighter operational requirements.
 - c.* Coordinate with and provide DCS, G-2 and the ARAT-PO with the support necessary to continuously conduct system engineering evaluations. These evaluations will assess the potential effectiveness of RSR capabilities and provide technical solutions to identified deficiencies.
 - d.* Initiate hardware and software engineering efforts when required to develop new capabilities to meet changes in threat composition, capability, or operation.
 - e.* Provide listing of identified technical deficiencies to TRADOC to use in modifying friendly RSR tactics, techniques, and procedures (TTP).
 - f.* Require reprogrammable memory for all EW and TSS. Direct and provide resources to ARAT-PO to support the software requirement for all EW and TSS systems to be reprogrammable at the organizational maintenance or operator level.
 - g.* Ensure deconfliction strategies and capabilities necessary to protect communications while still permitting essential EA operations to be incorporated into all EA, EW, and TSS.
 - h.* Incorporate RSR capabilities into systems being developed through combined cooperative efforts, and ensure that operations security guidance is observed during system acquisition, deployment, and operation.
 - i.* Ensure that RSR designs provide for Joint and allied interoperability of systems that are intended for use during Joint and/or combined operations and for those systems sold under foreign military sales.
 - j.* Ensure ARAT-PO has appropriate resources to establish the organic postproduction software support environments for fielded EW and TSS.
 - k.* Direct ARAT-PO to maintain interface with the EW community. This will include, but is not limited to, providing input to Army EW reprogramming policy documents and maintaining involvement with the Joint Services EW working groups.

2-8. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC will—

- a.* Develop TTP in support of Army EW and TSS software reprogramming by theater, operational area, or mission and provide guidance for the planning, execution, and evaluation of RSR activities in operations and training.
- b.* Identify gaps in EW and TSS capability training, doctrine, and tactics, and provide solutions to the deficiencies as determined under capabilities based assessments.
- c.* Ensure that the principles of the RSR process and the ARAT infrastructure are taught at Army institutions as appropriate.
- d.* Submit priority intelligence requirements to CG, U.S. Army Intelligence and Security Command (INSCOM) using prescribed procedures and methods. Submit requests for materiel support for capability development and development of counter capabilities in accordance with AR 381-11.
- e.* Ensure electromagnetic spectrum requirements and impacts for EW and TSS are considered in capabilities based assessment.
- f.* Ensure that all requirements documentation addresses RSR capabilities. Integrate RSR capabilities into doctrinal publications and establish employment authority consistent with U.S. Army and Joint policy.

2-9. Commanding General, U.S. Army Intelligence and Security Command

The CG, INSCOM will—

- a.* Provide EW and TSS threat, signature, EW, electronic intelligence, and applicable all-source data, upon request, necessary to identify changes in the threat composition or operation to the ARAT-PO for rapid reprogramming of EW and TSS capabilities.
- b.* In coordination with DCS, G-3/5/7, develop and maintain threat tools and parametric databases to support current and future EW and TSS requirements.
- c.* In coordination with DCS, G-3/5/7, provide required Army contribution to the EW, and measurement and signal intelligence reprogramming databases, as appropriate.
- d.* In coordination with CECOM/ARAT-PO and the Research, Development, and Engineering Command/Communications-Electronics Research, Development, and Engineering Center, review and validate input from ASCCs. Review and approve, if appropriate, ASCC-recommended procedures for receiving new and changed threat data from geographical Intermediate Processing Centers. Ensure procedures exist to rapidly distribute these changes to subordinate units, ARAT, and other Army organizations affected by the change.
- e.* Provide and resource all EW and TSS threat, signature, and intelligence data necessary to identify changes in threat composition or operation.

f. Review ARAT-PO intelligence production requirements and provide data as appropriate.

2-10. Commanders of Army Service Component Commands

The commanders of ASCCs will—

- a. Ensure Army intelligence representatives to the combatant command staff are trained on counter-threat-change capabilities and ARAT infrastructure and activities.
- b. Ensure deploying units and crews receive training on the current software and TTP for all EW and TSS required for military operations.
- c. Develop procedures for implementing TRADOC's stated TTP, training, doctrine, and other responses to enemy introduction of new or modified existing threats.
- d. Exercise established procedures to exchange data electronically with Joint Services for EW reprogramming, operations, and tactics.
- e. Exercise RSR procedures in accordance with respective command authorities.
- f. Include RSR objectives in exercises and training events.
- g. Ensure that counter-threat-change objectives are planned and coordinated with appropriate Service operations and intelligence organizations.

2-11. Commanders of Army Service Component Commands serving Geographic Combatant Commands

The commanders of ASCCs serving geographic combatant commands will—

- a. Direct the use of friendly wartime reserve mode (WARM) as dictated by the threat or as directed by the geographic combatant commander. This authority may not be delegated.
- b. Notify Electronic Warfare Coordination Centers and ARAT-PO when U.S. WARM capabilities have been used and when hostile WARM use is detected or suspected.
- c. Ensure standing operating procedures or reporting requirements include notification of both operators and the ARAT-PO.

Chapter 3

Counter-Threat-Change Strategic Overview

3-1. New and changed threats

- a. Adversaries are expected to employ both high and low technology systems with constantly changing tactics and methods. The EW and TSS require RSR capability to adapt to or preempt these changes.
- b. The largest volume of new and changed threats will most likely be employed at the beginning of hostilities. This creates the following problems for Army forces:
 - (1) Establishing existing threats.
 - (2) Identifying when the changes to existing threats occur.
 - (3) Determining how to counter the threat changes.
 - (4) Implementing appropriate changes to counter the new or changed threat.

3-2. Rapid software reprogramming strategy

The ARAT RSR strategy focuses on the following four strategies to achieve success:

- a. *Detect the change.* Perform continuous analysis of collected intelligence to identify when new threats, or modifications to existing threats, are introduced that may affect EW and TSS performance or TTP.
- b. *Assess the change.* Make use of automated tools and software models to identify or flag when changes may adversely impact EW and TSS system performance, either globally or regionally.
- c. *Develop the response.* Use threat parametric, signature, and employment information to rapidly develop, test, and accept a response to the change. Responses may be software updates, hardware modifications, changes in TTP, or a combination of all three.
- d. *Implement the change.* Transmit and implement the change (hardware, software, and TTP) to the system at the operator level.

Appendix A References

Section I Required Publications

The following publication is available on the Army Publishing Directorate Web site (<http://www.apd.army.mil>).

AR 381-11

Intelligence Support to Capability Development (Cited in para 2-8d.)

Section II Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

AR 70-1

Army Acquisition Policy

AR 71-9

Warfighting Capabilities Determination

AR 380-5

Department of the Army Information Security Program

AR 525-22

U.S. Army Electronic Warfare

AR 530-1

Operations Security (OPSEC)

FM 3-0

Operations

FM 3-13.10

Multi-Service Tactics, Techniques, and Procedures for the Reprogramming of Electronic Warfare and Target Sensing Systems

FM 3-36

Electronic Warfare in Operations

DODD 5250.01

Management of Signature Support within the Department of Defense (Available at <http://www.dtic.mil/whs/directives>.)

NDP-1

National Disclosure Policy (NDP-1, 1 Oct 1988) (Available at <http://www.dtic.mil/whs/directives/corres/pdf/523011p.pdf>.)

Section III Prescribed Forms

This section contains no entries.

Section IV Referenced Forms

DA Forms are available on the Army Publishing Directorate Web site (<http://www.apd.army.mil>).

DA Form 11-2

Internal Control Evaluation Certification

Appendix B Internal Control Evaluation

B-1. Function

The function covered by this evaluation is Software Reprogramming Policy for Electronic Warfare and Target Sensing Systems.

B-2. Purpose

The purpose of this evaluation is to assist the organizations designated in chapter 2 in evaluating the key internal controls listed. It is not intended to cover all controls.

B-3. Instructions

Answers must be based on the actual testing of key internal controls (for example, document analysis, direct observation, sampling, simulation, and so forth). Answers that indicate deficiencies must be explained and the corrective action identified in the supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that the evaluation has been conducted must be accomplished on DA Form 11-2 (Internal Control Evaluation Certification).

B-4. Test questions

- a.* Are sensor-based weapons and EW systems developed using reprogrammable software? (ASA (ALT) only)
- b.* Are policies and procedures in place to enable Rapid Software Reprogramming (RSR) across the Army, Services, Joint community, and allies, as necessary? (All-ASCCs address inside their command only.)

B-5. Supersession

Not applicable.

B-6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to Deputy Chief of Staff, G-3/5/7 (DAMO-ODE), Washington, DC 20310-3200.

Glossary

Section I Abbreviations

AMC

U.S. Army Materiel Command

AR

Army regulation

ARAT

Army Reprogramming Analysis Team

ARAT-PO

Army Reprogramming Analysis Team-Program Office

ASA (ALT)

Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

ASCC

Army Service Component Command

CECOM

Communications-Electronic Command

CG

commanding general

CIO/G-6

Chief Information Officer/G-6

DCS, G-2

Deputy Chief of Staff, G-2

DCS, G-3/5/7

Deputy Chief of Staff, G-3/5/7

DCS, G-4

Deputy Chief of Staff, G-4

DCS, G-8

Deputy Chief of Staff, G-8

DODD

Department of Defense directive

EA

electronic attack

EW

electronic warfare

INSCOM

U.S. Army Intelligence and Security Command

RSR

rapid software reprogramming

TRADOC

U.S. Army Training and Doctrine Command

TSS

target sensing systems

TTP

tactics, techniques, and procedures

WARM

wartime reserve mode

Section II**Terms****Electromagnetic spectrum**

The range of frequencies of electromagnetic radiation is from zero to infinity. It is divided into 26 alphabetically designated bands.

Electronic attack

Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.

Electronic protection

Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.

Electronic warfare

Electronic warfare is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: EA, electronic protection, and electronic support.

Electronic warfare support

Division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.

Operations security

A process of analyzing friendly action attendant to military operations and other activities to (1) Identify those actions that can be observed by adversary intelligence systems; (2) Determine indicators hostile intelligence systems might obtain that could be intercepted and pieced together to derive critical information in time to be useful to adversaries; (3) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to the adversary exploitation.

Rapid software reprogramming

Rapid software reprogramming is the deliberate alteration or modification of electronic warfare and target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment. These changes may be the result of deliberate actions on part of friendly, adversary or third parties; or may be brought about by electromagnetic interference or other inadvertent phenomena. The purpose of electronic warfare reprogramming is to maintain or enhance the effectiveness of electronic warfare and target sensing system equipment. Electronic warfare reprogramming includes changes to self-defense systems, offensive weapon systems, and intelligence collection systems.

Wartime reserve mode

WARM are characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. WARM are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use.

Section III**Special Abbreviations and Terms**

This section contains no entries.

UNCLASSIFIED

PIN 067882-000