

Army Regulation 190–15

Military Police

Physical Security of the Alternate Joint Communications Center (AJCC)

**Headquarters
Department of the Army
Washington, DC
6 May 1994**

Unclassified

SUMMARY of CHANGE

AR 190-15

Physical Security of the Alternate Joint Communications Center (AJCC)

This revision--

- o Assigns the Director of Information Systems for Command, Control, Communications, and Computers as the Army executive agent for staff management and coordination of the Alternate Joint Communications Center (para 1-4a).
- o Assigns the Deputy Chief of Staff for Operations and Plans staff responsibility for physical security of the Alternate Joint Communications Center (para 1-4b).
- o Assigns the Commanding General, U.S. Army Military District of Washington, overall responsibility for implementing the Department of Defense Alternate Joint Communications Center protection program (para 1-4d).
- o Prescribes additional requirements for inclusion in the physical security plan (para 1-5b).
- o Mandates that waivers and exceptions be approved at the Headquarters, Department of the Army level (para 1-6a).
- o Prescribes the review of exceptions at least every 2 years (para 1-6b).
- o Authorizes inspection of packages and materials entering Site R (paras 2-2a(2) and 2-3b).
- o Identifies new specification series for chain-link security fences (paras 2-2b and 2-4a).
- o Prescribes the use of a backup power supply for electronic security systems (para 2-2d).
- o Establishes additional requirements for the application of the intrusion detection systems (para 2-5).
- o Mandates requirements to test security force personnel on assessing and responding to security incidents (para 2-6c).
- o Revises abbreviations and terms in glossary.
- o Contains a subject index as prescribed in AR 25-30.

Effective 6 June 1994

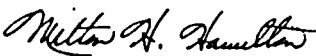
Military Police

Physical Security of the Alternate Joint Communications Center (AJCC)

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:



MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army

History. This printing publishes a revision of this publication. Because the publication has been revised extensively, the changed portions have not been highlighted.

Summary. This publication prescribes physical security policies, standards, and procedures for safeguarding property and

personnel at the Department of Defense Alternate Joint Communications Center. It implements DODD 5210.64, Alternate Joint Communications Center Protection Program.

Applicability. This regulation applies to members of the Active Army, the Army National Guard, and the U.S. Army Reserve assigned or employed at the Alternate Joint Communications Center. This regulation is applicable during full mobilization.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Operations and Plans. The proponent has the authority to approve exceptions to this publication that are consistent with controlling law and regulation. Proponents may delegate this approval authority, in writing, to a division chief under their supervision within the proponent agency who holds the grade of colonel or the civilian equivalent.

Internal control systems. This regulation

is not subject to the requirements of AR 11-2. It does not contain internal control provisions.

Supplementation. Supplementation of this regulation, and establishment of command and local forms are prohibited without prior approval of HQDA (DAMO-ODL-S), 400 Army Pentagon, WASH, DC 20310-0400.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. Users of this regulation are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to HQDA (DAMO-ODL-S), 400 Army Pentagon, WASH, DC 20310-0400.

Distribution. Distribution of this publication is made in accordance with the requirements on DA Form 12-09-E block 3183, intended for command levels C, D, and E for Active Army; none for Army National Guard and U.S. Army Reserve.

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

Physical security plans • 1-5, page 1

Waivers and exceptions • 1-6, page 1

Chapter 2

Site Security Systems, page 1

General • 2-1, page 1

Site facilities • 2-2, page 1

Access controls • 2-3, page 1

Perimeter barriers and lighting • 2-4, page 1

Intrusion detection systems • 2-5, page 2

Security forces • 2-6, page 2

Appendix A. References, page 3

Glossary

Index

*This regulation supersedes AR 190-15, 1 November 1983.

RESERVED

Chapter 1 Introduction

1-1. Purpose

This regulation prescribes policies, responsibilities, standards, and procedures for physical security of the Alternate Joint Communications Center (AJCC).

1-2. References

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

1-3. Explanation of abbreviations and terms

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

1-4. Responsibilities

a. The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) is the Army Executive Agent for staff management and coordination of the AJCC.

b. The Deputy Chief of Staff for Operations and Plans (DCSOPS) has staff responsibility for developing policies, standards, and procedures for the physical security of the AJCC.

c. The Commanding General (CG), US Army Intelligence and Security Command (INSCOM), has responsibility for operations security (OPSEC) support to the AJCC as prescribed in the Army Regulation (AR) 380-, 381-, and 530-series. This will include—

(1) OPSEC evaluations as requested.

(2) Threat information reported to the CG, U.S. Army Military District of Washington (MDW), and tenant activities of the AJCC.

d. The CG, MDW, has overall responsibility for implementing the Department of Defense (DOD) AJCC protection program. The responsibility will be to—

(1) Manage, integrate, and coordinate a formal physical security program for the AJCC.

(2) Plan for and provide manpower and budget resources for the physical protection of the AJCC.

(3) Conduct physical security surveys and inspections of the AJCC as prescribed in AR 190-13.

(4) Provide physical security support to tenant activities. Interservice support agreements will be developed outlining tenant activity physical security responsibilities.

(5) Develop an AJCC security threat assessment.

(6) Conduct OPSEC surveys as prescribed in AR 530-1.

(7) Report significant developments affecting security of the AJCC to Headquarters, Department of the Army (HQDA) (DAMO-ODL).

1-5. Physical security plans

a. A physical security plan for the AJCC will be developed and maintained per AR 190-13.

b. The physical security plan format outlined in FM 19-30 will be used as a guide. The plan will include AJCC access controls and security force requirements to include augmentation forces. The plan will also include contingency plans for hostage situations, bomb threats, civil disturbances, and closing the AJCC. The plan will include actions to withstand or repel penetration, including airborne and helicopter assault, and seizure efforts by militants, terrorists, demonstrators, or other criminal elements. The plan will also include rules of engagement and use of force per AR 190-14, coordination with appropriate civilian authorities, and chain of command notification. Lock and key control procedures will be included in the plan per AR 190-51 and AR 190-11 for arms, ammunition, and explosives.

1-6. Waivers and exceptions

a. Requests for waivers and exceptions will be submitted in writing to HQDA (DAMO-ODL), WASH, DC 20310-0400. Requests will include complete justification, compensatory measures in effect, the action being taken to correct the deficiency, and date the deficiency is due to be corrected.

b. Waivers will not be granted in excess of 24 months. All exceptions will be reviewed at least every 2 years to determine if they need to be continued.

Chapter 2 Site Security Systems

2-1. General

This section prescribes minimum security standards for AJCC facilities and personnel and procedural requirements.

2-2. Site facilities

a. Site R.

(1) All entrances to the outer tunnel of Site R will be protected by a minimum of two barriers with intrusion detection systems (IDS). Entrances will be adequately lighted during the hours of darkness or reduced visibility. The entrances will also be under continuous surveillance using electronic measures (closed circuit television (CCTV)) or by dedicated security personnel.

(2) The vehicular and personnel entrances from the outer tunnel into the inner tunnel of the AJCC will be protected by two blast doors with electronic surveillance at the entrances of both doors. Personnel, vehicles, and packages/materials entering the first blast door will be inspected prior to entering the second door.

b. *Site RT.* Site RT will be protected by two permanent barriers meeting the requirements of the U.S. Army Corps of Engineers (USACE) Standard Details for Chain Link Security Fences, Drawing Code STD 872-90-00 series, with a minimum height of 6 feet and an 18-inch top guard. A clear zone will extend 20 feet inside and outside the outer perimeter barrier and the perimeter will be lighted during hours of darkness and reduced visibility. Perimeter IDS sensors will be installed at the discretion of the CG, MDW.

c. *Site security control center (SSCC).* A SSCC will be dedicated to provide overall control of security force personnel, communications, CCTV monitors, lighting, and alarm systems for the AJCC. It will have a backup power supply to provide an uninterrupted emergency power source for its operation.

d. *Backup power supply.* All electronic security, surveillance, and entry control systems will have primary and auxiliary power sources capable of maintaining full operation of the systems for a minimum of 4 hours. Switchover to the auxiliary power source will be automatic upon failure of the primary power source.

2-3. Access controls

a. The AJCC will be designated and posted as a restricted area as outlined in AR 190-13.

b. Strict personnel and vehicular access control procedures will be established to ensure positive identification and visitor control. Procedures for inspection and movement of packages, materiel, and property will be established.

c. Access control measures will include as a minimum, the use of security cards and badges and a duress system. Electronic access control systems are permitted as determined by the CG, MDW, and must meet the technical approval of the Weapons System Manager for Physical Security Equipment (WSM-PSE), Belvoir Research, Development, and Engineering Center, Fort Belvoir, VA 22060-5606.

2-4. Perimeter barriers and lighting

a. Limited and exclusion areas will be protected by perimeter barrier fencing (USACE Drawing Code STD 872-90-00 series) with a minimum height of 6 feet and an 18-inch top guard. Clear zones will be maintained using guidance in FM 19-30.

b. Indoor and outdoor security lighting will be provided at points of entry into the limited and exclusion areas. Protective lighting for the perimeter of limited and exclusion areas should be applied per FM 19-30.

2-5. Intrusion detection systems

a. The IDS is an essential part of the physical security system.

IDS should be installed to ensure that—

- (1) Breaches of security boundaries are detected.
- (2) There is a timely detection of unauthorized access attempts.
- (3) Information regarding adversary movement toward a target is provided to the security force, where appropriate.
- (4) Equipment is safeguarded, and critical and vulnerable facilities are protected as determined by the CG, MDW.

b. The CG, MDW, determines the IDS to be integrated. Proposed IDS must meet the technical approval of WSM-PSE, prior to procurement, installation, and system integration.

c. Personnel monitoring the IDS will maintain records of alarms. These records will be used to evaluate IDS effectiveness (reliability, sensitivity, required adjustments or maintenance, and other data intended to maintain or increase security). Records will be retained for 1 year. Records will include the nature of the alarm, the date and time the alarm was received, the location, and the action taken in response to the alarm. These records will be reviewed by supervisor personnel to ensure proper actions were taken, and to identify and correct IDS reliability problems (false and nuisance alarms). DA Form 4930-R (Alarm Intrusion Detection Record) may be used to record alarms received. A reproduction copy of DA Form 4930-R is located in the back of the Physical Security Handbook 10-3, and prescribed by AR 190-11. A computer-generated printout of alarms may be used as a substitute, provided all required information has been included or supplemental information is included in a log.

d. All security-related detection equipment and components will have a regularly applied test, maintenance, and quality assurance program to ensure an effective and operable system. The tests will be conducted per manufacturer and or military technical manuals. A record of all tests will be maintained for 1 year. It will reflect the date of the test, the name of the person conducting the test, and any required corrective action resulting from the test.

2-6. Security forces

a. Primary security force personnel will be military.

b. The organization, duties, equipment, communications requirements, and training for security and augmentation forces will be determined by the CG, MDW, using guidance in FM 19-30.

c. Security force personnel will be tested regularly on assessing alarm activations, responding to intruders and other situations, and reporting suspicious activities or unusual circumstances.

Appendix A References

Section I Required Publications

AR 190-11

Physical Security of Arms, Ammunition, and Explosives. (Cited in paragraph 1-5*b*.)

AR 190-13

The Army Physical Security Program. (Cited in paragraphs 1-4*d*, 1-5*a*, and 2-3*a*.)

AR 190-14

Carrying of Firearms and Use of Force for Law Enforcement and Security Duties. (Cited in paragraph 1-5*b*.)

AR 190-51

Security of Unclassified Army Property (Sensitive and Nonsensitive). (Cited in paragraph 1-5*b*.)

AR 530-1

Operations Security (OPSEC). (Cited in paragraph 1-4*d*.)

Chain Link Security Fences.

Obtain USACE drawings from USA Engineer Division, Huntsville, ATTN: HN-DED-ES-1, Box 1600, Huntsville, AL 35807-4301.

Section II Related Publications

AR 15-6

Procedures for Investigating Officers and Board of Officers

AR 190-16

Physical Security

AR 190-22

Search, Seizure, and Disposition of Property

AR 190-40

Serious Incident Report

AR 210-10

Administration

AR 380-5

Department of the Army Information Security Program Regulation

AR 380-19

Information Systems Security

AR 380-19-1

Control of Compromising Emanations

AR 380-40

Policy for Safeguarding and Controlling Communications Security (COMSEC) Material

AR 381-12

Subversion and Espionage Directed Against the US Army (SAEDA)

AR 381-14

Technical Surveillance Countermeasures (TSCM) (U)

AR 381-20

The Army Counterintelligence Program

AR 420-43

Electrical Services

AR 525-13

The Army Combatting Terrorism Program

AR 600-8-14

Identification Cards, Tags, and Badges

DA Pam 190-51

Risk Analysis for Army property

DA Pam 350-38

Standards in Weapons Training

TM 5-853-1

Designing for Security

FM 19-30

Physical Security

Section III Prescribed Forms

This section contains no entries.

Section IV Referenced Forms

DA Form 4930-R

Alarm/Intrusion Detection Record

Glossary

Section I Abbreviations

ADP

automated data processing

AJCC

Alternate Joint Communications Center

DCSOPS

Deputy Chief of Staff for Operations and Plans

DISC4

Director of Information Systems for Command, Control, Communications, and Computers

IDS

intrusion detection system

INSCOM

U. S. Army Intelligence and Security Command

MDW

Military District of Washington

OPSEC

operations security

SSCC

site security control center

USACE

U.S. Army Corps of Engineers

WSM-PSE

Weapons System Manager for Physical Security Equipment

Section II Terms

Augmentation force

Additional personnel (or units) organized, trained, armed, equipped, and capable of augmenting site security forces as required.

Backup power supply

A separate and distinct source of power, internal to the site and in addition to the site's primary electrical power source (normally an engine or generator).

Barrier

A coordinated series of obstacles designed or employed to canalize, direct, restrict, delay, or stop the movement of an intruding force.

Closed circuit television

A means used for physical security. CCTV augments, but does not replace, existing IDS or security patrols. It is not used as a primary sensor, but rather as a means of assessing alarms.

Continuous surveillance

A continual watch of an area to preclude unobserved access. Surveillance may be

maintained by personnel. Electronic or mechanical measures may also be used to maintain surveillance.

Deadly force

Deadly force is that force which a person uses with the purpose of causing, or which the person knows, or should know, will create a substantial risk of causing death or serious bodily harm.

Duress system

A method by which personnel who control entry into, vouch for, or escort visitors into a limited and/or exclusion area can covertly communicate a situation of duress to other operating or security personnel.

Exception

Permanent exclusion from requirements of this regulation.

Entry control facility

A facility which is part of the perimeter security system and a point from which personnel, materials, vehicle control, and badge operations are conducted.

Exception

An approved permanent deviation from the provisions of this regulation that creates a security vulnerability and requires compensatory waivers.

Exclusion area

A restricted area containing the following:

a. A security interest or other matter that is of such nature that access to the area constitutes, for all practical purposes, access to such security interests or matter.

b. A security interest or other matter of such vital importance that proximity resulting from access to the area is treated as equal to *a* above.

Intrusion detection system

A system consisting of sensors capable of detecting one or more types of intrusion into the area protected by the system. The IDS will be an approved DOD standardized system, such as the Joint-Servicesy Interior Intrusion Detection System (J-SIIDS), or commercial equipment that will be approved by the CG, MDW, for purchase or lease and meets the technical approval of WSM-PSE.

Key control officer

A person, other than a locksmith, appointed by the commander in writing to manage the lock and key program for the AJCC.

Key custodian

A person, other than a locksmith, who has custody of the keys in use at the AJCC. A documented chain of custody is required at all times.

Keyed alike system

A system that allows a number of locks to be

operated by the same key. It is often used in perimeter applications.

Limited area

A restricted area containing a security interest or other matter in which unauthorized movement could permit uncontrolled access to such security interest or matter.

Operations security

The protection of military operations and activities resulting from the identification and elimination or control of intelligence indicators that are susceptible to hostile use.

Physical security plan

A comprehensive written plan providing proper and economical use of personnel and equipment to prevent or minimize loss or damage.

Postulated threat

An estimate of the potential adversary types, acts, capabilities, and combinations thereof that could constitute a risk to a facility or asset. A postulated threat is necessary when a specific threat cannot be determined or when an existing threat may change or grow during the projected life cycle of an asset or system faster than security improvements can be developed and implemented. The postulated threat allows for the consideration of future growth in adversary capabilities and is used as the basis for the design of security systems, equipment, and facilities.

Primary electric power source

The source of power, either external (commercial) or internal, that provides power to the site facilities on a day-to-day basis.

Real-time assessment

Instantaneous assessment of the actual cause for the activation of the sensor alarm by either direct visual assessment, or with the aid of electro-optical imaging equipment such as closed circuit television.

Restricted area

See AR 190-13.

Site CREED

The limited area on the west side of the AJCC with an underground building complex.

Site R

The Alternate Joint Communications Center (AJCC is located near Fort Ritchie, MD).

Site RT

The limited area at Site R where antennas are located.

Site Security Control Center

An area from which the security and augmentation forces are controlled. This area may include the alarm center, the visual assessment facilities, and other appropriate security capabilities.

Waiver

An approved temporary deviation from the provisions of this regulation that creates a security vulnerability and requires compensatory measures.

Section III**Special Abbreviations and Terms**

This section contains no entries.

Index

This index is organized alphabetically by topic and by subtopic within topic. Topics and subtopics are identified by paragraph number.

Augmentation force, 1-5

Budget, 1-4

Interservice support agreements, 1-4

Manpower, 1-4

Operations security, 1-4

Physical security measures

Access controls, 1-5, 2-3

Barriers, 2-2, 2-4

Clear zones, 2-2, 2-4

CCTV, 2-2

Duress system, 2-3

Fencing, 2-2, 2-4

Intrusion detection systems, 2-2, 2-5

Lock and key control, 1-5

Perimeter lighting, 2-2, 2-4

Physical security program, 1-4

Planning, 1-4, 1-5

Power supply, 2-2

Restricted areas, 2-3

Security cards and badges, 2-3

Security force, 1-5, 2-2, 2-5, 2-6

Site facilities

Site CREED, glossary

Site R, 2-2

Site RT, 2-2

SSCC, 2-2

Surveys and inspections, 1-4

Threat information, 1-4

Use of force, 1-5

Waivers and exceptions

Authority to grant, 1-6

Submission, 1-6

Unclassified

PIN 054460-000

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.45

PIN: 054460-000
DATE: 06-24-98
TIME: 10:41:35
PAGES SET: 10

DATA FILE: s280.fil
DOCUMENT: AR 190-15
DOC STATUS: REVISION