ARMY REGULATION

No. 381-25

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, DC, *15 March 1980*

MILITARY INTELLIGENCE

SAFEGUARDING INFORMATION PERTAINING TO CERTAIN HUMINT ACTIVITIES (U)

Effective 15 April 1980

(U) Local limited supplementation of this regulation is permitted, but is not required. If supplements are issued, HQDA agencies and major Army commands will furnish one copy of each to HQDA (DAMI-ISH), WASH DC 20310; other commands will furnish one copy of each to the next higher headquarters.

(U) Interim changes to this regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

	Paragraph
Purpose	1
Applicability	2
Scope	3
Policy	4
Army participation	5
Responsibilities	6
General procedures	7
Transmission	8
Receipt and destruction certificates	9
Classification, downgrading, and marking instructions	10
Storage and retirement	11
Compromise or possible compromise of RODCA information or material	12

1. (U) **Purpose.** This regulation prescribes policy, responsibilities, and procedures on Army use of the RODCA communication channel.

2. (U) **Applicability.** *a.* (U) This regulation applies to and is binding on all Department of the Army (DA) HUMINT collection management and operating elements and activities.

b. (U) This regulation does not apply to the Army National Guard and the US Army Reserve.

c. (U) This regulation does not apply to Army commands, units, or agencies not listed in the RODCA Control Points Directory. (This directory is published by DIA and provided to RODCA control points.)

3. (U) **Scope.** *a.* (C) [redacted] (C)." 5 USC 552 (b) (1)

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject
To Criminal Sanctions.

NOT Rreleasable
TO FOREIGN
NATIONALS

WARNING NOTICE
SENSITIVE INTELLIGENCE
SOURCES AND METHODS
INVOLVED (WNINTEL)

CONFIDENTIAL

Classified by [redacted] CSI
Review [redacted] 2000
Reason: Para 1-301c(3) DOD 5200.1-R

[redacted] 5 USC 552 (b) (1)

b. (C) [redacted]

5 USC 552 (b) (1)

c. (U) The Defense Intelligence Agency (DIA) established the RODCA communications channel to handle and transmit the types of information included in, but not limited to, those listed below:

(1) (C) [redacted]

(2) (C) [redacted]

(3) (C) [redacted]

(4) (C) [redacted]

(5) (C) [redacted] 5 USC 552 (b) (1)

(6) (C) [redacted] 5 USC 552 (b) (1)

5 USC 552 (b) (1)

5 USC 552 (b) (1)

4. (U) Policy. *a.* (U) All designated DA elements will use the RODCA communications channel when transmitting communications containing information described in paragraph *3c*.

b. (U) Normally, dispatch RODCA message traffic between RODCA control points by General Service (GENSER) communications channels. However, time and operational reasons may require use of the Special Security Office (SSO) communications channels. Local commanders will authorize such use on a case-by-case basis when necessary. To prevent abuse of this departure from normal RODCA transmissions, commanders will conduct periodic reviews of the need to use other communication channels. When no longer justified, such deviation will be discontinued. See paragraph *8b*(6) for procedures to transmit HUMINT sensitive operational messages to commands, units, or agencies that do not use the RODCA channel.

c. (U) Give RODCA material maximum protection under existing security regulations governing protection of sensitive sources and methods.

d. (U) Do not normally use the RODCA channel for collection objectives, requirements, information papers, or derivative documents.

e. (U) Transmit replies to RODCA communcations in the RODCA channel to—

(1) (U) Protect the integrity of the channel

(2) (U) Ensure quick routing to the recipient

(3) (U) Limit distribution, and

(4) (U) Prevent activities who do not know of the original communication from receiving responses.

f. (U) Protect the integrity and security of the RODCA communications channel at all times.

g. (U) Authorized RODCA communications channel users are limited to those listed in the RODCA Control Points Directory. Do not send RODCA messages to addressees not listed in the directory. See paragraph *8b*(6) for more guidance on dispatch of messages outside RODCA channels

h. (U) Communications are sent in the RODCA communications channel only on a point-to-point basis between DOD elements listed in the RODCA Control Points Directory.

i. (U) Commanders of designated elements will appoint RODCA control officers. These persons may be commissioned, warrant, or noncommissioned officers, or DA civilians (professional intelligence or security personnel GS–7 or above).

j. (U) This regulation does not relieve agencies and activities of their responsibilities to submit requests and reports required by other regulations.

k. (U) This regulation does not authorize the transmittal of information if the acquisition, retention, or dissemination of the information is otherwise constrained or controlled by Executive Order or regulation.

5. (U) Army participation. *a.* (*U*) *Authority*. Use of the RODCA channel by DA is based on statutory responsibilities in Section 102, National Security Act of 1947, as amended, and guidance from the Director of Central Intelligence and the Director,

Defense Intelligence Agency. Policies and procedures for the DOD RODCA communications channel are in DIAM 58-11 (Defense Intelligence Agency Human Resources Intelligence Collection Management Manual, Short Title: DIHUM (U)).

b. (C) Goal. [redacted]

5 USC 552 (b) (1)

6. (U) Responsibilities. *a.* (U) The Assistant Chief of Staff for Intelligence (ACSI) will—

(1) (U) Establish policy and procedures for Army use of the RODCA communications channel.

(2) (U) Review and approve the procedures of MACOMs and Army components of unified commands implementing this regulation to comply with established policy.

(3) (U) Appoint an RODCA control officer (and an alternate if needed) for HQDA to serve as the Army point of contact for operation of the Army RODCA communications channel.

(4) (U) Advise DIA of authorized Army RODCA control points.

b. (U) Major Army commands and Army components of unified commands will—

(1) (U) Designate Army organizations authorized to use the RODCA communications channel.

(2) (U) Advise OACSI of authorized RODCA points of contact within their commands and components.

(3) (U) Provide OACSI with copies of supplements to this regulation.

(4) (U) Appoint an RODCA control officer (and an alternate, if needed) to implement and ensure compliance with RODCA control procedures.

c. (U) Commanders of designated activities and elements will—

(1) (U) Appoint an RODCA control officer (and an alternate if needed) to implement and ensure compliance with this regulation and supplements issued by higher commands.

(2) (U) Limit access to RODCA material only to those properly cleared persons within the commands with a need-to-know consistent with operational and mission requirements. Commanders may authorize access to persons not within their command if such access is needed to conduct authorized activities.

(3) (U) Establish limited access areas within each headquarters where RODCA communication material is processed and stored. (See para 4c, AR 380-20.)

(4) (U) Arrange for the conduct of technical sweeps, as needed, of areas where RODCA material is stored, processed, or discussed.

d. (U) RODCA control officers will—

(1) (U) Maintain rosters of persons authorized access to specific operations.

(2) (U) Advise all persons authorized access to RODCA material of its sensitivity and of personal responsibility to safeguard it.

(3) (U) Monitor the safeguarding, storage, and dissemination of RODCA material prepared within or received by the unit or organization.

(4) (U) Provide servicing communications centers with adequate instructions to process, transmit, and limit dissemination of RODCA material only as determined by the originator.

(5) (U) Receive all RODCA material for the unit or organizational element and provide access on a need-to-know basis.

(6) (U) Assure RODCA material and files are properly retired when projects, operations, or sources are terminated.

7. (U) General procedures. *a.* (C) [redacted]

5 USC 552 (b) (1)

b. (U) Classification, downgrading, safeguarding, and transmittal of RODCA communications will comply with AR 380-5.

c. (U) The RODCA communications channel will be administered as prescribed in this regulation and in supplemental directives issued by MACOMs and Army components of unified commands to lower echelons.

8. (U) Transmission. Transmit RODCA communications by—

a. (U) Correspondence.

(1) (U) Prepare the minimum number of copies of correspondence to meet administrative and security requirements.

(2) (U) Prepare the document receipt for correspondence and place inside the inner envelope.

(3) (U) Mark the inner envelope as follows:

(*a*) (U) Conspicuously mark or stamp at the top, bottom, front, and back the caveat, "RODCA COMMUNICATION."

(*b*) (U) Affix proper security classification under Chapter 8, AR 380-5.

(*c*) (U) Clearly annotate in RED on the front the notation, "DELIVER TO RODCA CONTROL OFFICER ONLY."

(*d*) (U) Address the envelope to the attention of the addressee's RODCA control office using the proper office symbol in the RODCA Control Points Directory.

(4) (U) Address the outer envelope using the mailing address in the RODCA Control Points Directory.

(5) (U) Prepare DA Form 1965 (Delivery and Pick-up Service) as an envelope receipt when sealed envelopes are processed through mail and distribution centers or courier systems. If this form is not available prepare an equivalent receipt with proper number of copies.

(6) (U) Send all RODCA material authorized to be sent through US mails by registered mail. Mail to OCONUS RODCA addressees will only be addressed to APO/FPO serviced units. Transmittal through foreign postal facilities is strictly prohibited.

b. (U) Messages.

(1) (U) Address electronically transmitted RODCA communications only to official designated control points in the RODCA Control Points Directory. These will normally be dispatched by GENSER communication facilities. When properly justified, use SSO channels.

(2) (U) Show at the beginning of an RODCA message the following elements in the format shown below:

"(CLASSIFICATION) RODCA COMMUNICATION
DELIVER TO RODCA CONTROL OFFICER ONLY
FROM: (Enter designator/office symbol).
(NOTE: Only authorized RODCA users may send RODCA messages.)
TO: (Enter designator/office of intended recipient).
SUBJECT: _____"

(3) (U) State on message internal instructions "Pass to _____" when messages are intended for DOD persons or offices not designated as RODCA control points.

(4) (U) Keep the number of copies of messages sent out and kept on file to an absolute minimum. Retaining a file or suspense copy of messages by communications centers is prohibited beyond the mandatory 30 days retention required by TM 11-490-2.

(5) (U) Cut off immediately the RODCA caveat from incoming UNCLASSIFIED messages when UNCLASSIFIED responses must be sent to comply with the policy to keep all correspondence in the RODCA channel. Normally, RODCA messages will be classified CONFIDENTIAL or higher. UNCLASSIFIED information should not require RODCA protection. Removing the ROD CA caveat meets the standards to protect the integrity of the RODCA channel.

(6) (U) Transmit sensitive messages that normally are sent over RODCA communications channels but which must be sent to commands and agencies not in the RODCA system, by using either SSO or the GENSER SPECAT EXCLUSIVE communications channel under paragraph 6-11, AR 105-31. This procedure limits distribution to only the offices indentified in the message. Do not mark these messages as RODCA communications. Although SPECAT EXCLUSIVE messages normally use persons' names as addressees, this is not a mandatory requirement and official titles are acceptable. All SPECAT EXCLUSIVE and SSO messages used for this purpose will include WNINTEL and NOFORN caveats.

c. (U) Internal handling. All RODCA material will be handcarried from one location to another within each organization (i.e., from originating office to coordinating office and to and from communications center) in a properly secure manner. Hand-carry all RODCA material unless the commander has approved an alternate procedure to ensure its secure delivery.

9. (U) Receipt and destruction certificates. All RODCA material requires a continuous receipt and destruction certificate system. The organization commander will decide to what extent continuous receipts are required (i.e., receipting within organizational elements is the most restrictive;

receipting only when document is transferred out of the organization is the least restrictive). In any case, destruction certificates are required on all RODCA documents when destroyed. These procedures apply to all RODCA documents, including those classified CONFIDENTIAL. Otherwise UNCLASSIFIED documents from which ROD CA markings have been removed are not considered to be RODCA documents.

10. (U) Classification, downgrading, and marking instructions. *a. (U) Classification and downgrading.*

(1) (U) Observe classification and downgrading guidelines in AR 380–5.

(2) (C) [redacted] 5 USC 552 (b) (1)

(3) (C) [redacted] 5 USC 552 (b) (1)

(4) (U) In addition to control markings, annotate RODCA information described in this regulation as follows:

(*a*) (U) If marked "Classified by ACSI, DA" type "Review on 20 years from date of origination."

(*b*) (U) As an exception to (*a*) above, foreign government classified information will be reviewed 30 years from date of origination.

(5) (U) Exceptions to above classification guidance or markings require OACSI approval in each instance.

b. (U) Marking.

(1) (U) All RODCA material will be conspicuoulsy marked or stamped in RED, "RODCA COMMUNICATION." Markings need only appear on the first page of each RODCA document.

(2) (U) Unclassified letters of transmittal used to forward RODCA inclosures will have the RODCA markings cut off when separated from inclosures.

(3) (U) The caveat "RODCA COMMUNICATION" is sufficient to show that dissemination is to be severely limited. If it is necessary to provide RODCA information to offices or agencies outside the RODCA channel, remove RODCA markings and place the following caveats on the material:

(*a*) (U) "WARNING NOTICE—SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED." (WNINTEL)

(*b*) (U) "NOT RELEASABLE TO FOREIGN NATIONALS." (NOFORN)

11. (U) Storage and retirement. *a.* (U) Store RODCA material in approved security containers under the storage provisions in AR 380–5. Do not incorporate RODCA material into general file repositories but maintain separately. Other related operational files may be stored with RODCA material.

b. (C) [redacted] 5 USC 552 (b) (1)

12. (U) Compromise or possible compromise of RODCA information or material. *a.* (C) [redacted] 5 USC 552 (b) (1)

b. (U) Individual responsibilities. Any DOD member who becomes aware of the loss, unauthorized disclosure, or any other possible compromise of RODCA material or any infraction of RODCA security requirements will report such violation without delay to his/her unit security or RODCA control officer who will in turn notify the responsible commander.

c. (U) Unit commander responsibilites. Unit commanders will conduct a quick and vigorous informal inquiry to determine if compromise has occurred or is probable, to determine the cir-

cumstances under which it occurred, and to fix responsibility for the compromise. If the facts reveal compromise or probable compromise, the commander will notify HQDA (DAMI-ISH) and the MACOM commander by electrical message of the nature, circumstances, and extent of compromise. The commander will immediately initiate an investigation under AR 380-5 and AR 15-6.

d. (*U*) *MACOM commander responsibilities.*

(1) (U) Upon notification that RODCA information has been compromised, the MACOM commander will take action to offset or minimize the impact. A report of action initiated or contemplated will be forwarded through the RODCA channel to HQDA (DAMI-ISH) within 48 hours of notification.

(2) (U) Forward the report of AR 15-6 investigation and final action by the MACOM commander through the RODCA channel to HQDA (DAMI-ISH).

e. (*U*) *HQDA action.* Upon receipt of the MACOM report, ACSI will—

(1) (U) Initiate any required national level action to minimize the impact on national security caused by the compromise.

(2) (U) Make any required notification to non-DA agencies.

The proponent agency of this regulation is the Office of the Assistant Chief of Staff for Intelligence. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) direct to HQDA(DAMI-ISH) WASH DC 20310.

By Order of the Secretary of the Army:

E. C. MEYER
General, United States Army
Chief of Staff

Official:

J. C. PENNINGTON
Major General, United States Army
The Adjutant General

DISTRIBUTION: Special

U.S. GOVERNMENT PRINTING OFFICE 1968 O - 337-346