DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
1401 DESHLER STREET SW
FORT MCPHERSON, GA 30330-2000
1 July 2001

***USARC Memorandum 530-1**

Operations and Signal Security

HEADQUARTERS, U.S. ARMY RESERVE COMMAND OPERATIONS SECURITY (OPSEC)

For the Commander:

JOHN A. YINGLING
Brigadier General, USA
Chief of Staff

Official:
ARTHUR R. TAYLOR
Army Reserve Chief Information Officer

History. This is the second printing of USARC Memorandum 530-1. It was originally published 1 May 1994.

Applicability. This memorandum applies only to Headquarters, U.S. Army Reserve Command (USARC) staff personnel.

Proponent and exception authority. The proponent of this memorandum is the Deputy Chief of Staff, Operations (DCSOPS). The proponent has the authority to approve exceptions to this memorandum that are consistent with controlling law and regulation. Proponents may delegate this approval authority in writing to a division chief within the proponent agency in the grade of colonel or the civilian equivalent.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028, Recommended Changes to Publications and Blank Forms, to the DCSOPS, ATTN: AFRC-OPO-O.

Distribution: C

1. Purpose

To provide policy and guidance for Operations Security (OPSEC) within the Headquarters (HQs), U.S. Army Reserve Command (USARC).

2. References

a. Required publication. Army Reg 530-1, Operations Security (OPSEC). Cited in para 5a (7)(8) and para 5c (4).

b. Related publications are:

(1) AR 380-5, Department of the Army Information Security Program.

(2) Joint Pub 3-54, Joint Doctrine for Operations Security.

(3) JCS Pub 5-02.2, Joint Operation Planning System.

(4) CJCS MOP 29, Joint Operations Security.

(5) DOD Directive 5230.24, Operation Security Program.

3. Explanation of abbreviations and terms

Abbreviations and terms used in this memorandum are explained in the glossary.

4. General

Operations Security is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and activities to--

a. Identify those actions that can be observed by adversaries.

b. Determine indicators that could be interpreted or pieced together to derive critical information.

c. Select and execute measures that eliminate or reduce to an acceptable level friendly vulnerabilities.

5. Responsibilities

a. *The DCSOPS.* Serves as the Commander's principal staff officer for overall management of the OPSEC Program. Designates responsibility to the Command OPSEC Officer. The OPSEC Officer will--

(1) Prepare and recommend USARC OPSEC policy.

(2) Chair the Command OPSEC working group.

(3) Develop and recommend OPSEC measures to be implemented within the Command.

(4) With the assistance of the DCSINT, develop and recommend Essential Elements of Friendly Information (EEFI) for the Command. See appendix A.

(5) Conduct OPSEC reviews of operational plans and reports to ensure adherence to OPSEC policies and procedures.

(6) Ensure training exercises include realistic OPSEC considerations and any evaluation of the

*This memorandum supersedes USARC Memorandum 530-1, 1 May 1994

headquarters participation in a training exercise includes an evaluation of OPSEC procedures. Further, ensure pre-exercise OPSEC briefings are conducted incorporating the threat, EEFI, and countermeasures.

(7) Coordinate with the Public Affairs and Freedom of Information Act officer (CIO) to ensure an OPSEC review is conducted prior to the release of information concerning the command and command programs/projects.

(8) Ensure OPSEC training, in accordance with AR 530-1 and this memorandum, is conducted.

(9) Integrate intelligence, counter-intelligence, Force Protection and Information Operations information into OPSEC planning and practice as appropriate.

(10) Monitor the OPSEC program of USARC subordinate organizations by reviewing OPSEC plans, survey results, exercise evaluations, and Inspector General reports.

(11) Perform other duties and responsibilities as defined in AR 530-1.

b. Staff Directors and Chiefs will--

(1) Ensure appropriate OPSEC measures are taken within their agencies to preserve essential secrecy.

(2) Integrate OPSEC into all activities to provide maximum protection of all functions and activities.

(3) Implement the OPSEC Program, including the appointment of a staff agency OPSEC coordinator.

c. The Staff Agency OPSEC Coordinator will--

(1) Provide OPSEC guidance to his/her agency director/chief in the preparation of OPSEC annexes, plans, and other documentation.

(2) Recommend and assist in the development of OPSEC measures to be implemented within their agency.

(3) Develop and recommend EEFI for their agency.

(4) Ensure that OPSEC training, in accordance with AR 530-1 and this memorandum, is conducted.

(5) Perform other duties and responsibilities as defined in this memorandum.

(6) Act as the OPSEC working group member for his/her agency

(7) Review his/her staff agencies' Intranet web pages to check for classified, sensitive, or inappropriate content prior to being published on the USARC Intranet Website.

d. All Headquarters' USARC, personnel will--

(1) Comply with established OPSEC and security practices for critical and sensitive information.

(2) Know the HQs, USARC EEFI (see appendix A) and the EEFI for their areas.

(3) Be aware of adversary intelligence collection threat.

(4) Be familiar with this memorandum and where to obtain additional OPSEC guidance if needed.

(5) Report violations to their staff agency OPSEC Coordinator.

6. OPSEC Measures

Specific OPSEC measures must be developed for USARC activities. Assistance in the development of OPSEC measures is available from the DCSOPS OPSEC Officer. The measures listed below are offered as a guide.

a. Administrative.

(1) Avoid open posting of planned schedule notices which reveal when sensitive events will occur.

(2) Control the issuance of orders, movement of units, programs, or key personnel.

(3) Control trash and housekeeping functions to conceal sensitive activities.

(4) During periods of increased operational activity, follow normal leave policy and working hours to maximum extent possible to preserve the outward sense of normalcy.

(5) Ensure personnel maintain the ability to travel, as necessary, so that preparation for sensitive travel will not generate unusual activity.

(6) Screen discussions or releases to the media with public affairs personnel.

(7) Control access to the Headquarters' buildings and escort those personnel not assigned.

(8) Be prepared to implement a "clean desk" on 1 hour notice in the event of visitors.

b. Communications.

(1) Make maximum use of secure communications, telephone, fax, classified email and U.S. Message Text Format messages.

(2) Limit release of information until latest possible date or until activities are complete.

(3) Limit reading file distribution to personnel with need to know. Control distribution of non-classified, sensitive information in accordance with distribution markings for technical and operational information as stated in DOD Directive 5230.24, Operation Security Program, and the requirements stated in the Command EEFI (see appendix A).

(4) Strict compliance with command Artificial Intelligence System/ EEFI policy on the use of all computer system operation to include small computers.

c. Readiness.

(1) Safeguard reports on unit personnel to include attendance at special schools.

(2) Limit distribution on rosters which identify personnel by position, Military Occupation Specialty/Area of Concentration, grade, or security clearance.

d. Travel.

(1) Travel in civilian clothes whenever possible. Do not carry briefcase, or bags which identify you as a member of the Command.

(2) Use a passport in lieu of military orders whenever possible.

(3) Do not discuss assignment, duties, or reason for travel unless absolutely necessary (e.g., with security, customs, or immigration personnel).

7. OPSEC Process

The OPSEC process applies to all phases of an activity, function, or operation and is used in the development of OPSEC plans. The five fundamental steps are:

a. Critical information is needed by adversaries to effectively plan an act to degrade the operational effectiveness of the Command. The development of EEFI is part of the OPSEC process. The EEFI are the key questions about friendly intentions, capabilities, and activities asked by adversary decision makers. The EEFI list may be classified. Remember, EEFI are the questions the adversary is going to ask, the answers to the questions are the items that must be protected. When the traditional security programs cannot maintain protection, OPSEC must provide an OPSEC measure (see glossary).

b. *Analysis of threat*. Adversary collection efforts are identified. The aim is to neutralize or manipulate the threat to the U.S.'s advantage. Detailed information about specific intelligence efforts is available from the USARC DCSINT. The five questions that must be answered are:

(1) What critical information is already known by the adversary?

(2) What gaps exist in the adversary information base that prevent him/her from deriving critical information?

(3) What intelligence collection assets are available that will enable adversaries to exploit friendly actions?

(4) What friendly actions might reveal critical information? (see appendix B)

(5) What are potential OPSEC vulnerabilities?

c. *Analysis of vulnerabilities (appendix C).* Analysis of vulnerabilities identifies tentative OPSEC measures required to maintain essential secrecy. The most desirable OPSEC measure combines the highest protection with the least effect on USARC operational effectiveness. There are three conditions of an OPSEC vulnerability:

(1) Action control. Alternate ways of conducting actions and activities which avoid indicators which create vulnerabilities. Actions taken by/within USARC Headquarters to eliminate (prevent) or control indicators.

(2) Countermeasures. Disruption of adversary information collection or gathering.

(3) Counteranalysis. Actions to cause misinterpretation of indicators by analysts.

d. Assessment of risk. Because implementation of OPSEC measures usually presents a risk to operational, logistic, or procedural effectiveness, an analysis must be made prior to the decision to implement measures. The OPSEC Coordinator makes recommendations on each measure based on these questions:

(1) What is the risk to operational effectiveness if an OPSEC measure is implemented?

(2) What is the risk to operations and the Command mission success if an OPSEC measure is not implemented.

(3) What risk is likely to result if the OPSEC measures fail to be effective.

e. *Application of appropriate OPSEC measures*. The OPSEC measures are selected based on decisions in the previous step (para 7d).

(1) Only the DCSOPS can approve each OPSEC measure based on the answers to these questions (para 7d(1) - (3)). After these questions are answered, two decisions must be made. They are:

(a) Which, if any, OPSEC measures should be implemented?

(b) When should selected OPSEC measures be implemented?

8. OPSEC Review Process/Requirements

a. Overview. An evaluation of the OPSEC posture of an official document to ensure that sensitive or critical information is properly protected. Official documents may consist of memorandums, letters, messages, briefings, contracts, news releases, technical documents, proposals, plans, orders, annexes to plans or orders, Freedom of Information Act (FOIA) requests, and other documents.

b. Procedures:

(1) The OPSEC review may be either directed or requested. A request for OPSEC review may be initiated by any individual to the staff agency OPSEC Coordinator or the OPSEC Officer.

(2) All FOIA requests will be sent to the USARC FOIA officer (CIO) for processing.

(3) All news releases will be reviewed by the Public Affairs OPSEC Coordinator.

(4) When corrective action is deemed appropriate, to include a classification review, the OPSEC officer will document in writing to the appropriate official for immediate action.

(5) Technical papers and reports must contain an appropriate distribution statement.

Appendix A
Command Essential Elements of Friendly Information (EEFI)

The EEFI are key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. Answers to the EEFI constitute critical information that must be protected. The EEFI below are common to many types of activities and form the basis for specific EEFI for each activity and operation.

1. What missions and contingencies are being planned?
2. What are the WARTRACE relationships between USAR units and supported Commander in Chiefs.
3. What artificial intelligence systems are in use to connect to contractor facilities?
4. What contracts contain classified elements?
5. Where are the program and project command and control nodes? Support activities?
6. What are current and planned command and control arrangements?
7. Which computers are capable of processing classified documents? Which ones are connected to a Local Area Network (LAN)?
8. What are the levels of security within the Headquarters complex?
9. Is there a secure telephone in use? Is it controlled?
10. Where are personnel going on temporary duty (TDY)? What are the purposes of their TDY?
11. What projects are assigned to which branches? What are the responsibilities of each action officer?
12. What are the methods used to carry information while on TDY?
13. With what nations are discussions being held for operations, support, and joint development? What are the subjects of these discussions?
14. Are there unannounced inspections of trash containers?
15. What are the intended counter (terrorist, narcotics) operations procedures?
16. What counterintelligence support does the organization receive?
17. What deceptions are planned? In operation? Who is conducting?
18. What political constraints have been placed on planning?
19. What intelligence and capabilities are internal to the Command?
20. What are the emergency action procedures? Who is contacted?
21. Does the unit have any type of nuclear capability?
22. Does the unit support any nuclear capable units?
23. Does the unit have any type of special operations or unconventional warfare capability or support functions?

Appendix B
OPSEC Indicators

B-1. Indicators are friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive critical information. They are categorized as:

a. Profile Indicators. Information about a unit or activity which shows normal operation and activity procedures.

b. Deviation indicators. Information which shows changes to standard operations and procedures.

c. Tip-off Indicators. Information which point to an operation or activity, and needs no other explanation.

B-2. Administration

a. TDY Orders.
b. Meeting or conference notification.
c. Transportation, housing arrangements.
d. Individual or unit schedules.
e. Changes to administrative workload.
f. Changes to distribution plans.
g. Use of words indicating irregular activity (e.g. Critical, Priority, Rush, Sensitive).
h. Changes to personnel assignments.
i. Security classification Guides.
j. Unusual security clearance requirements.
k. Tables of Organization and Equipment/ Distribution and Allowances.
l. Unit readiness reports, or information which is a component of the report (e.g. personnel assigned).
m. Canceling leaves/recalling personnel to unit.
n. Changes to off-limits or controlled access areas.

B-3. Activities

a. Changes in THREATCON.
b. Repositioning of command assets.
c. Deviations/cancellation of training.
d. Increased activities by special units.
e. Change in normal training activities including language training and special training.
f. Conduct of security briefings.
g. Movement of specially qualified personnel.
h. Friendly reactions to national level exercises or hostile actions.
i. Assignment of liaison officers.
j. Conduct of rehearsals/exercises.
k. Unprogrammed changes to in-place security measures.

B-4. Communications

a. Increased volume of message traffic/secure communications.
b. Changes to reporting procedures/schedules.
c. Imposition of COMSEC procedures.
d. Increased coordination among headquarters.

B-5. Intelligence

a. Increased requests for area/country studies.

b. Special requests for maps.

c. Priority requests for threat briefings.

B-6. Supply and logistical support

a. Increased volume and priority of requisitions.

b. Pre-positioning or movement of equipment.

c. Requests for special equipment/munitions.

d. Increased maintenance activities.

e. Transportation requests.

f. Requests for medical/transportation support.

g. Increased or unusual requests for computer support.

NOTE. This listing is provided to give OPSEC coordinators an idea of some of the actions or information which can provide indication of what has happened, is happening, or is going to happen. These indicators must be looked at from the adversary point of view. Think of the indicators as being pieces of a large puzzle, as he/she collects each piece, the picture comes together. The adversary may not need every piece of the puzzle to see the overall picture of what we are doing. Specific indicators will be based on the actual activity.

Appendix C
OPSEC Vulnerabilities

C-1. Vulnerabilities are friendly actions which provide indicators that may be obtained and accurately evaluated by an adversary to provide a basis for effective adversary decision making. Vulnerabilities consist of stereotyped actions which habitually occur (patterns), and unique, detectable characteristics which identify a type activity or intention (signatures). These actions are the target of adversary intelligence collection efforts and should be considered when developing OPSEC measures. An OPSEC vulnerability exists when these three conditions exist:

a. An adversary has the capability to collect the indicator.

b. The adversary has the time to collect, analyze, report, and make a decision.

c. The adversary can react or take an action which will be harmful to our activities or mission.

C-2. Examples of Vulnerabilities

a. Failure to ensure that sensitive information is furnished to authorized persons only.

b. Inadvertent disclosure of classified and sensitive information.

c. Failure to follow security classification guidelines.

d. Unescorted visitors in areas with open storage of classified or sensitive information, or exposure of indicators.

e. Improper storage or handling of classified documents.

f. Publication and distribution of information without an OPSEC review.

g. Failure to declassify computer or automated information systems prior to allowing uncleared personnel to perform maintenance.

h. Allowing maintenance personnel to work on information systems unsupervised.

i. Assignment of uncleared personnel to duties that provide opportunity for access to sensitive information.

j. Inadvertent release of information to the media.

k. Improper disposal of sensitive or classified information.

l. Carelessness in OPSEC procedures based on lack of awareness of adversary information gathering capability or effort.

m. Failure to periodically review security and OPSEC procedures and requirements.

n. Failure to maintain or enforce access controls.

o. Failure to brief newly assigned personnel on internal OPSEC procedures and measures.

Glossary

Section I
Abbreviations

COMSEC.....communications security
EEFI.....Essential Elements of Friendly Information
FOIA.....Freedom of Information Act
LAN.....Local Area Network
OPSEC.....Operations Security
TDY.....temporary duty
USARC.....U.S. Army Reserve Command

Section II
Terms

Adversary
Those individuals, groups, or organizations that must be denied critical information to maintain friendly mission effectiveness. Adversaries may include hostile countries, terrorists, the media, and allied intelligence agencies.

Collection Threat
Collection of information on U.S. Army activities may be conducted by adversaries using various intelligence collection methods. These pieces of information provide an accurate portrayal of the commands overall intentions and/or operations.

Critical Information
Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act to guarantee the failure of friendly mission accomplishment.

Essential Elements of Friendly Information (EEFI)
Key questions adversaries are likely to ask about friendly intentions, capabilities, and actions so they can obtain answers critical to their operational effectiveness.

Essential Secrecy
The condition achieved from the denial of critical information to adversaries.

Human Intelligence Threat (HUMINT)
Collection of information by human sources for intelligence purposes. Gathered covertly by espionage agents, or overtly through information available to the general public, it is the most basic form of intelligence collection. HUMINT remains significant because it is often the only source with access to an opponent's intentions and plans.

Imagery Intelligence Threat (IMINT)
Collection of information by photographic, infrared, or radar imagery. Images can be gathered either by individuals or by remote means, such as aircraft or satellite. This method is valuable because it provides analysts with clues to other areas requiring examination. The IMINT includes unauthorized duplication of documents.

Indicators
Friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive critical information.

Measurement and Signature Intelligence (MASINT)
Scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical sensors to identify any distinctive features associated with the source, emitter, or sender. It is technical in nature.

Military deception
Actions executed to mislead foreign decision-makers, causing them to derive and accept desired appreciation of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives. Deception is an effective OPSEC measure which can be employed given prior coordination (e.g., cause adversary intelligence collection efforts to fail to target friendly activities, create confusion or misinterpretation of information obtainable from open sources).

OPSEC Measure
Methods and means to gain and maintain essential secrecy about critical information.

Sensitive Information
Any information, the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of Federal programs, but which has not been specifically authorized under an Executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy (PL 100-235, 8 Jan 88).

Signals Intelligence (SIGINT)
Collection of information by interception of electronic signals from communications equipment or non-communicative devices that emit an electronic signal, such as a radar beacon. It includes interception of communication and the interception and analysis of communication between pieces of equipment (e.g., LAN).

Vulnerabilities
Friendly actions which provide indicators and may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. Vulnerabilities exist when three conditions exist; adversary has capability to collect indicator, and adversary has time to process (report, analyze, take planning action), and the adversary must be able to react.