

DEPARTMENT OF THE ARMY
MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
OPERATIONS CENTER
661 SHEPPARD PLACE
FORT EUSTIS, VA 23604-1643

SDDC Regulation
No. 380-2

JUL 19 2005

Security
SDDC OPERATIONS SECURITY (OPSEC) PROGRAM

Supplementation of this regulation is prohibited. Submit comments and suggested improvements to HQSDDC (SDDC-IS) on DA Form 2028 (Recommended Changes to Publications and Blank Forms)

<u>Paragraph</u>	
Purpose	1
Applicability	2
References	3
Terms	4
Policy	5
Responsibility	6
Procedures	7
Appendices	
Appendix A-Critical Information Listing	
Appendix B-OPSEC Training Guide and Sample Briefing Outline	

1. PURPOSE

This regulation provides policy and prescribes procedures for the implementation of AR 530-1, Operations Security (OPSEC) and the SDDC Operations Security (OPSEC) Program Plan.

2. APPLICABILITY

This regulation is applicable to all Surface Deployment and Distribution Command (SDDC) staff elements, subordinate commands and activities including Army Reserve units OPCON to SDDC during mobilization or contingencies.

3. REFERENCES

- DODD 5205.2, DOD Operations Security (OPSEC) Program
- Joint Pub 3-54, Joint Doctrine for Operations Security

FOR OFFICIAL USE ONLY

- AR 1-201, Army Inspection Program
- AR 25-400-2, The Army Records Information Management System (ARIMS)
- AR 380-381, Special Access Programs (SAPS) and Sensitive Activities
- AR 381-12, Subversion and Espionage Directed Against the U.S. Army (SAEDA)
- AR 381-14, Technical Counterintelligence (TCI)(C)
- AR 525-21, Battle Field Deception (C)
- AR 530-1, Operations Security (OPSEC)
- SDDC Operations Security (OPSEC) Program Plan

4. TERMS

See AR 530-1, Glossary, for abbreviations and terms used in this regulation.

5. POLICY

a. The Deputy Chief of Staff for Intelligence and Security, G2, will establish and manage the overall SDDC OPSEC program.

b. Subordinate commands and activities will establish an effective local OPSEC program and implement OPSEC initiatives consistent with the intent of AR 530-1 and commensurate with operational necessity.

c. OPSEC is a command responsibility. Commanders/directors of SDDC activities must ensure that OPSEC is deliberately considered and made an integral part of all military plans, operations, exercises, tests and activities. The worldwide scope of SDDC operations creates vast opportunities for the collection of information by foreign intelligence services (FISs). Coordinated OPSEC efforts in all functional areas will minimize this threat to operations.

d. All SDDC personnel (soldier, civilian, and contractor) will receive an OPSEC briefing within 30 days of assignment, at least annually thereafter, and prior to participation in any operation, exercise or test.

6. RESPONSIBILITY

a. The Deputy Chief of Staff for Intelligence and Security, G2, will exercise staff supervision over the provisions of this regulation and will designate the SDDC OPSEC Program Manager.

b. Subordinate commanders/directors are responsible for the operations security of their command/activity.

(1) Commanders/directors must develop policy, instruction and training procedures adequate to maintain an effective operations security posture for their activity.

(2) Commanders/directors will designate an OPSEC Officer/alternate, in writing, to assist in this responsibility. A copy of the duty appointments must be provided to G2 within 30 days of designation. In order to be effective, the OPSEC Officer must be intimately familiar with the day-to-day operation of the command/activity, and have a thorough knowledge of friendly capabilities, intentions, and operations which require the establishment and maintenance of essential secrecy. OPSEC Officers will attend OPSEC programs of instruction that teach skills necessary to prepare OPSEC estimates and planning guidance, write OPSEC annexes, give formal briefings, and prepare and supervise the execution of OPSEC measures. Training can be arranged by contacting the following agencies:

- Interagency OPSEC Support Staff (IOSS), 6411 Ivy Lane, Suite 400, Greenbelt, MD 20770, telephone: DSN 689-4677 or commercial (443) 479-4677. For further information, click on <http://www.ioass.gov/> or email at ioass@radium.ncsc.mil.
- U.S. Army Space and Missile Defense Command (USASMDC), Building 5220 (Werhner Von Braun Complex), Martin Road, Redstone Arsenal, Huntsville, AL 05808 telephone: DSN 645-2521 or commercial (256) 955-2521, or email at belchem@smdc.army.mil

c. The SDDC OPSEC Program Manager, G2, is responsible for developing, administering, and monitoring the Command OPSEC Program, and will advise the command on all OPSEC related issues.

d. The OPSEC Officer will be the point of contact for all matters concerning operations security within the command/activity. Primary responsibility for the OPSEC Officer is to prevent or minimize hostile intelligence collection of sensitive information on unit plans, readiness and operations. This is systematically accomplished by identifying those sources which would reveal Critical Information (CI) to an adversary, and acting to eliminate, neutralize, or cause the information to be inconsequential to friendly intentions.

e. Within SDDC, OPSEC Coordinators will be designated by the staff principals as points of contact for matters related to the OPSEC Program, and is sufficiently trained to represent the staff element on all aspects of the Command OPSEC Program.

7. PROCEDURES

a. The SDDC OPSEC Program Manager will develop a command OPSEC program plan and provide staff interpretation and guidance at every level of command. The incumbent will:

(1) Conduct OPSEC briefings, reviews, assessments, inspections and surveys in accordance with AR 530-1 and provide an OPSEC annex for all OPLANS/OPORDS. OPSEC considerations must be included in all plans and activities.

(2) Maintain liaison with foreign threat intelligence and counterintelligence support and ensure OPSEC related intelligence is reviewed and analyzed.

(3) Develop and recommend the Critical Information List for command approval.

(4) Advise commanders/directors regarding OPSEC threats to specific unit activities, operations or exercises and offer recommendations that close vulnerability gaps and lowers risk.

(5) Participate as a crisis action team member, and provide appropriate OPSEC analysis support and countermeasure recommendations.

(6) Assess and coordinate requirements for Open Skies Treaty OPSEC measures with subordinate commands/activities, continuously monitor effectiveness, and adjust countermeasures as needed.

(7) Review requests for technical counterintelligence (TCI) support in accordance with AR 381-14 (C), or other similar request for technical assistance.

(8) Administer a command-wide OPSEC education and training program, which provides a thorough awareness of current security threats to global SDDC activities.

(9) Interface with OPSEC professionals and command OPSEC points of contact on issues that affect the command at large.

(10) Participate as a subject matter expert in the Organizational Inspection Program (OIP), in accordance with AR 1-201, to review, assess and evaluate command/activity OPSEC programs.

(11) Prepare and submit to HQDA the command Annual OPSEC Report in accordance with AR 530-1, Appendix I.

b. Staff OPSEC Coordinator will:

(1) Maintain awareness of staff and organizational activities and advise staff principals and appropriate personnel on OPSEC measures for those activities.

(2) Assist in the development and refinement of the Command Critical Information List and identify Critical Information for specific operations, activities, exercises, functions, or tests that involve the staff element, and advise the staff principal and Command OPSEC Program Manager.

(3) Establish an internal document OPSEC review policy for the staff element to preclude the inadvertent disclosure of sensitive information to unauthorized sources and to ensure distribution statements and classification markings are applied when appropriate.

(4) Participate in, and provide insight to, the OPSEC Working Group.

c. OPSEC Officer will:

(1) Conduct OPSEC surveys, assessments, reviews, briefings and debriefings, and ensure appropriate OPSEC considerations are included in all command/activity operations. Establish internal

operating procedures to ensure OPSEC measures are implemented in accordance with paragraph 7d(2) of this regulation. Comply with the letter and intent of the SDDC OPSEC Program Plan.

(2) Develop and publish an OPSEC plan or standing operating procedure.

(3) Ensure all personnel receive an initial OPSEC briefing within 30 days of arrival, prior to the implementation of an operation or exercise in which they are involved, and at least annually thereafter. OPSEC training will be recorded and maintained on file within the activity in accordance with AR 25-400-2.

(4) Maintain liaison with security and intelligence agencies, and counterintelligence personnel to obtain and analyze information for the development of the OPSEC survey.

(5) Organize and provide oversight to the OPSEC Working Group. If the SDDC command or activity is a tenant to a garrison or installation, the OPSEC Officer will participate in the garrison or installation level OPSEC Working Group.

(6) When required, process requests for TCI support in accordance with AR 381-14 (C) through command channels to G2.

(7) Review prime contractor OPSEC requirements specified on DD Form 254, Contract Security Classification Specification, to include those requirements specified by the prime contractor for subcontracts, and contractor OPSEC plans.

(8) Submit recommendations to G2 for the realistic simulation of adversary intelligence collection capabilities and techniques during training exercises. The OPSEC Officer will monitor and evaluate OPSEC exercise scenarios, debrief exercise participants, and prepare lessons learned information papers in coordination with the SDDC OPSEC Program Manager. The intent of these procedures is to further development and refinement of Critical Information.

(9) Prepare and submit to G2 the command/activity Annual OPSEC Report in accordance with AR 530-1, Appendix I, by 1 September each fiscal year.

d. Individuals will:

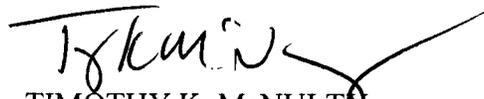
(1) Know how to apply and practice OPSEC in the performance of their daily tasks.

(2) Submit information proposed for posting to web sites or other disclosure to open sources for OPSEC review prior to release. This includes, but is not limited to, news releases, responses to Freedom of Information Act and Privacy Act requests, technical data, internal reports, financial and operations related information. Coordination with the OPSEC Officer is required.

(3) Have the requisite knowledge to safeguard Critical Information and know answers to the following questions:

- What is my organization's Critical Information?
- What Critical Information am I personally responsible to protect?
- How is the threat trying to acquire my particular Critical Information?
- What steps are being taken to protect my/our Critical Information?
- How do I report an OPSEC concern or ask an OPSEC question, and to whom?

FOR THE COMMANDER:



TIMOTHY K. McNULTY
Colonel, TC
Chief of Staff

APPENDIX A

SUBJECT: Critical Information Listing (FOUO)

1. Answers to the following questions are to be considered Critical Information (CI):

- What are the classified programs or activities in SDDC?
- What new undisclosed capabilities exist, or, are being developed?
- What are the funding constraints?
- What do vessel cargo manifests reveal?
- What are times/dates of cargo arrivals/departures?
- What are vessel sailing times?
- What are cargo destinations?
- What is revealed in movement tables?
- What are the designations of deploying units?
- What additional information is revealed by transportation documentation?
- What reserve unit call-ups may occur?
- What is the port throughput capacity (amount of tonnage moving through a port)?
- Where are the transportation routes?
- What are the volumes and priorities of requisitions?
- What does package/container labeling reveal?
- What cargoes are stockpiled and where are they pre-positioned?
- What is the planned or actual movement of sensitive items through a port, such as:
 - 1) Arms, Ammunition and Explosives (AA&E).
 - 2) Missiles and rockets.

A-1

FOR OFFICIAL USE ONLY

- 3) Nuclear components.
- 4) Chemicals.
- 5) High technology electronic and communications equipment.
- 6) Pharmaceutical items.

- What information is contained in personnel records?
- What political constraints may affect planning?
- What are the sensitivities and locations of Army Information Systems (AIS) and communications equipment?
- Who are the transportation contractors and what are their transport capabilities?
- What are the contingency plans at strategic seaports?

2. The above list is not all inclusive, and should be utilized as a baseline for operational planning.

APPENDIX B

SUBJECT: Operations Security (OPSEC) Training Guide and Sample Briefing Outline

1. At a minimum, OPSEC should be briefed to ensure that all personnel are familiar with the OPSEC program and are informed of the adversary intelligence threat, and their intention and capability to exploit national defense information in order to gain a strategic or economic advantage.

2. Orientation Training. Must be presented within 30 days of assignment and will include the following topics:

- Local Adversary Intelligence Threat (Identification and Background).
- Adversary Intelligence Gathering Methodologies.
- The OPSEC Process.
- How OPSEC Complements Traditional Security Programs.
- Protection of Critical Information (CI).

3. Awareness Training. This training will consist of, but is not limited to, the following topics and must be presented prior to each exercise and operation, and at least annually:

- Identifying OPSEC Indicators.
- Determining OPSEC Vulnerabilities.
- Effective OPSEC Practices and Countermeasures.

4. Sample Briefing Outline. The following sample outline is provided to assist OPSEC trainers in structuring their presentations. Local training should be tailored to the needs of the organization and specifics of the operation.

A. GENERAL.

- OPSEC Definition and History.
- Responsibilities.
- OPSEC Objective.

B. Planned Unit Operations and Activities.

C. Specific Threat Capabilities to Operations and Activities.

- Human Intelligence (HUMINT) Threat.
- Imagery Intelligence (IMINT) Threat.
- Signal Intelligence (SIGINT) Threat.
- Measurement and Signature (MASINT) Threat.

D. Critical Information (CI) List.

E. OPSEC Relationships to Other Programs and Effective Countermeasures.

- Information Security.
- Physical Security.
- Information Assurance
- Communications Security (COMSEC).
- Electronic Security (ELSEC).
- Military Deception (MD).
- Command, Control, and Communications Countermeasures (C3CM).
- Force Protection.
- Counterintelligence (to include Subversion and Espionage Directed Against the U.S. Army (SAEDA)).
- Additional Countermeasures (may be peculiar to a specific operation).

