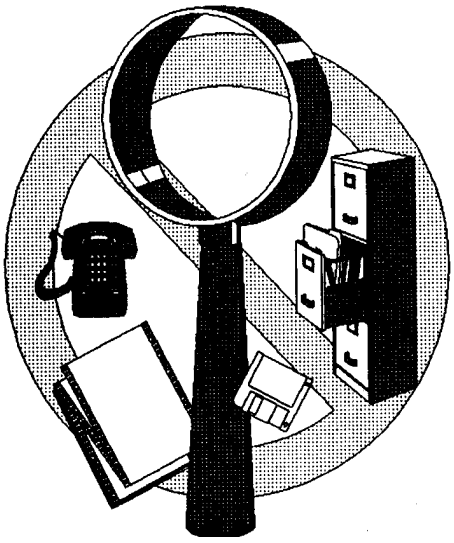
U.S. Army Center for Health Promotion and Preventive Medicine

Just the Facts

94-001-0994

Operations Security (OPSEC)



- **Freedom of Information Act**
- **Responsibility**
- **Adversary**

What is OPSEC?

Operations Security or OPSEC is the process of analyzing friendly actions pertaining to military operations and other activities to:

- Identify those actions that can be observed by adversary governments.
- Determine the informational data hostile governments might obtain that could be interpreted or pieced together to derive critical information. The most sought-after information, in order of its appeal to adversaries, is:
  - Top Secret
  - Secret
  - Confidential
  - Unclassified Sensitive
  - Unclassified
- Select and execute measures that reduce or eliminate the vulnerabilities of friendly actions to hostile exploitation.

When is OPSEC Required?

The release of information from Department of the Army records must comply with the directive requirements of the Freedom of Information Act (FOIA).

At the same time, sensitive information concerning military operations and activities must be protected from disclosure to hostile intelligence agencies.

OPSEC applies to all plans, projects, operations, equipment tests, and routine support activities.

OPSEC measures are required not only to protect combat operations during periods of crisis and war, but also to prevent the disclosure of logistical, personnel, training, medical research, development, test and other activities during low intensity conflict and peacetime.

What are Your Responsibilities?

- Use the Secure Telephone Unit (STU-III) in the secure mode whenever discussing sensitive information. Remember, all of your nonsecure telephone conversations can be monitored.
- Use telecommunications center facilities to process sensitive information via message format and secure facsimile.
- Use appropriate distribution restriction statements on documents which contain operational information, and limit distribution accordingly.
- Ensure information to be released is reviewed and authorized for release so that the proper distribution statement is used.
- Consult with your FOIA advisor, your supervisor, the Public Affairs Office, or the Security Manager as appropriate.
- Ensure the “need-to-know” requirement is met before the release of sensitive information.
- Shred appropriate documents instead of trashing them.

U.S. Army Center for Health Promotion and Preventive Medicine (Provisional)
Security Office, Aberdeen Proving Ground, MD 21010-5422
DSN 584-4220 or Commercial 410-671-4220
Email: mchbch@aehal.apgea.army.mil