1

March 1992/Number 3-92

security awareness bulletin

Inside:

OPSEC

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

Staff Writer
Tracy Gulledge

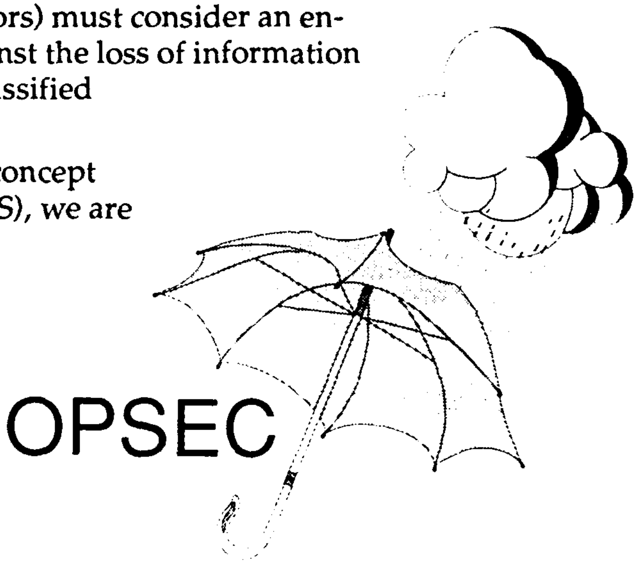
The *Security Awareness Bulletin* is produced by the Department of Defense Security Institute, Educational Programs Department, c/o Defense General Supply Center, Richmond Virginia 23297-5091; (804) 279-3824/4223, DSN 695-3824/4223. Primary distribution is to DoD components and contractors cleared for classified access under the Defense Industrial Security Program and Special Access Programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and educational methods as well as through distribution of textual material for direct training application.

Administrative inquiries, new distribution, address changes: please refer as follows:

Army activities: HQ DA (DAMI-CIS), Washington, DC 20310
Navy & Marine Corps: Security Policy Div (OP-09N), Washington, DC 20350
Air Force: Headquarters AFSPA/SPGB, Kirtland AFB, NM 87117
DIS activities: HQ DIS/V0954
DISP contractors: Cognizant Security Office
Other government agencies: Headquarters security education office

OPSEC: A Broader Umbrella

In this issue of the *Bulletin* we again address the problem of protecting a wider range of information than that which is formally designated US classified. It follows from National Security Decision Directive 298, that Federal agencies (and when directed by user agencies, defense contractors) must consider an enhanced countermeasures program to protect against the loss of information that would in the aggregate reveal sensitive or classified aspects of an operation.



By way of introducing our readership to this concept and to the Interagency OPSEC Support Staff (IOSS), we are reproducing their monograph, "The National OPSEC Program" and a second contribution by a member of the IOSS staff, "OPSEC: It's not what you think it is." Admittedly there is a certain amount of confusion in both government and industry about what OPSEC is and what it isn't. We hope that these articles will help to clear up misunderstandings. In this issue we also provide a listing of publications on the development and implementation of OPSEC programs distributed by IOSS by request.

We also include an interesting first-person account of OPSEC training during the recent Gulf Crisis. The author, Carl Roper, is an instructor in the Security Management Department here at the Department of Defense Security Institute. And we conclude this issue with an unusual espionage case study. In what appears to be the first case of its type, a US service member has been convicted and sentenced to 34 years for attempting to sell unclassified but sensitive operations information.

In a future issue of the *Bulletin* we will be looking at OPSEC procedures from the perspective of DoD User Agencies and defense contractors. In addition, we will review the new Department of Defense Acquisition Systems Protection Program which incorporates many OPSEC principles and procedures.

The National OPSEC Program

by Samuel R. Raskin

In today's information age, the effective conduct of government activities requires increased efforts to ensure that our adversaries do not obtain data that would allow them to achieve their objectives or undermine ours. Concerns over the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities and intentions led the President to approve a National Security Decision Directive (NSDD) establishing a National Operations Security Program. The NSDD sets up a national operations Security (OPSEC) structure and requires each Executive Department and Agency, assigned or supporting national security missions with classified or sensitive activities establish an OPSEC program.

The NSDD describes OPSEC as "...a systematic and proved process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive government activities."

This monograph attempts to present an overview of the origins of OPSEC, how it works, what the NSDD requires, and why OPSEC is important enough to be the subject of a Presidential Directive.

There Is Nothing New About OPSEC

There is nothing new about the principles underlying OPSEC. If you have given a surprise birthday Party, or attempted to make your house look lived in while you were on vacation by arranging for someone to pick up your newspapers and installing a light timer, you have practiced OPSEC. OPSEC is applicable to any situation where you want to deny information to an outsider in order to achieve your mission goals. What is relatively new is the development of a methodology whereby the principles behind OPSEC can be applied in a consistent and thorough manner

OPSEC as a methodology originated during the Vietnam conflict when a small group of individuals were assigned the mission of finding out how the enemy had been obtaining advance information of certain combat operations in Southeast Asia. This team was established by the Commander in Chief, Pacific and given the cover name Purple Dragon. Their initial mission was to review several air operations. It soon became apparent to the team that although traditional security and intelligence countermeasures programs were in place in Southeast Asia, reliance solely upon them was insufficient to deny critical information to the enemy, especially information relating to intentions and capabilities. A new approach was needed to deal with unclassified information and indicators that could be pieced together by enemy intelligence to derive critical information. The group conceived and developed the methodology of analyzing U.S. operations from the enemy viewpoint to find out how the enemy obtained the information. They determined what information needed protection, obtained information on the enemy's intelligence capabilities, uncovered the vulnerabilities of the U.S. operations to enemy exploitation, assessed the risk of exploitation, and devised ways to thwart the enemy's collection or use of the data. They then recommended corrective actions to the local commanders for adoption. They were successful in what they did and, to name what they had done, they coined the term "operations security."

This OPSEC methodology has now been around for more than 20 years. Over the years it became increasingly apparent that OPSEC had utility in virtually every government program that had information needing protection to assure program effectiveness. Techniques have been modified and improved by OPSEC practitioners as experience has been gained with many different organizations and in areas far afield from military combat operations. Today it is understood that OPSEC is as equally applicable to an administrative or research and development activity as it is to combat operations.

How OPSEC Works

One of the most important lessons l.arned over the last two decades of OPSEC experience is that most government activities involve a stereotyped sequence or pattern of events, some planned and some unplanned, unique to that organization or activity. Those events and their components, which occur during the planning, preparatory, and execution stages of an activity, create vulnerabilities that even in the securest of environments may be subject to adversary exploitation. Through the analysis of actions and data relating to these stages, it can be determined how adversaries can obtain an organization's critical information even if completely denied access to all classified and sensitive aspects of the activity by effective security measures and intelligence countermeasures.

The detectable activities and bits of data that can be pieced together to derive classified or sensitive information are called indicators. Typically the individual indicators are considered unclassified, and often beyond the purview of traditional security programs to even identify, let alone classify and protect. Indicators may occur throughout a broad spectrum of activities, both undertaken by the organization involved and in supporting organizations. Usually, indicators most easily accessible to the adversary occur in support activities like administration, budgeting, communications, databases, logistics, maintenance, etc.

In the past, many indicators were naturally protected by distance and time. Information processing, storage and transmission has evolved, over the years, to a point that most information is very susceptible to adversary acquisition. In addition, even the most unsophisticated adversaries have at their disposal collection devices and techniques which reflect the technological age in which we live--a technology which can be used to overcome many of the protective techniques conceived in a much simpler world.

Today, if OPSEC is not integrated into sensitive and classified government activities, chances are very great that our adversaries will acquire significant information about the activities. It probably would have been difficult for the Purple Dragon team to foresee that twenty years later the methodology they had developed would become a national program. However, in retrospect, it seems inevitable that such an evolution should have occurred.

The Five-Step OPSEC Process

The NSDD formalized OPSEC and described it as a five-step process: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of countermeasures.

The following paragraphs discuss the elements and application of the OPSEC process. Although the NSDD describes the process as discrete steps, they are most often applied in parallel with some elements repeated several times. The process must be tailored to the specific organization and activity being analyzed. Most importantly, the process is a cycle where after countermeasures are implemented, evaluation must continue.

1) Identification of critical information. Basic to the process is determining *what information, if available to one or more adversaries, would harm an organization's ability to effectively carry out the operation or activity*. This critical information constitutes "core secrets" of the organization, i.e., the few nuggets of information that are central to the organization's mission or the specific activity. Critical information usually is, or should be, classified or at least protected as sensitive unclassified information. Sometimes the information that is critical and must be protected is another organization's core secrets, this being especially true in support functions.

2) Analysis of threats. Knowing *who the adversaries are and what information they require to meet their objectives* is essential in determining what information is truly critical to an organization's mission effectiveness. In any given situation there is likely to be more than one adversary and each may be interested in different types of information. For example, a terrorist may want information about a dignitary's movements, while a hostile country's intelligence service may want to know what that person is working on.

The adversary's ability to collect, process, analyze, and utilize information, i.e., the threat, must also be determined. The objective is to know as much as possible about each adversary and the strategies available for targeting the organization. It is especially important to tailor the adversary threat to the actual activity and, to the extent possible, determine what the adversaries' capabilities are for the specific time and place of the activity.

3) Analysis of vulnerabilities. Determining the organization's vulnerabilities involves systems analyses of *how the operation or activity is actually conducted by the primary and supporting organizations*. The organization and the activity must be viewed as the adversaries will view it, thereby providing the basis for understanding how the organization really operates and what are the true, rather than hypothetical, vulnerabilities. The chronology of all events, the timing of actions, and the flow of information and materials must be reviewed. Actions that can be observed or data that can be interpreted or pieced together to derive critical information must be identified. An assessment should be made of the vulnerability to the adversary actually collecting the data that can provide the critical information.

4) Assessment of risks. Vulnerabilities and specific threats must be matched. *Where the vulnerabilities are great and the adversary threat is evident, the risk of adversary exploitation is expected*. Therefore, a high priority for protection needs to be assigned, and corrective action taken. Where the vulnerability is slight and the adversary has a marginal collection capability, the priority should be low.

5) Application of countermeasures. *Countermeasures should be developed* that will do away with the vulnerabilities, threats or utility of the information to the adversaries. The possible countermeasures should include alternatives that may vary in both effectiveness, feasibility and cost. Countermeasures may include procedural changes, deception and perception management, intelligence countermeasures, traditional security measures or anything that is likely to work in the particular situation.

The impact of the loss of the critical information on the effectiveness of the activities is balanced against the cost of implementing corrective measures. The probability that the information will be collected and used by the adversary are then factored in. The manager can then implement those countermeasures that are deemed appropriate and cost effective. The authority for determining where and how countermeasures will be applied must rest with the decision maker who has ultimate responsibility for mission accomplishment and resource management.

In some cases, there may be no way to protect the information because of cost or other factors, making implementation impossible. When this occurs, the manager must decide to either accept the degradation to effectiveness or cancel the operation.

The OPSEC process should be carried out by operations elements of an organization or component with the advice and assistance of OPSEC and other technical experts as required. OPSEC must be integrated into the activity from conception and initiation of planning and extend throughout the life of the activity.

By using the OPSEC process, managers will have a better understanding of how their organization actually operates, what information may be available to adversaries, the impact of the loss of the information on mission effectiveness, and ways to protect that information. Most significant, the decision of whether to implement countermeasures must be based on the manager's cost benefit analysis and an evaluation of the overall program objectives.

OPSEC is a systematic process that can be applied by organizations to deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified information and evidence of the planning and execution of sensitive and classified activities.

OPSEC Program Requirements

The NSDD requires formal OPSEC programs, describes the OPSEC process and provides guidance on the application of the OPSEC process within departments' and agencies' activities. The NSDD recognizes that not all agencies are directly involved in classified or sensitive activities. It exempts those agencies with only minimal activities that could affect national security from establishing formal programs. However, they must cooperate with other departments and agencies to minimize damage to national security when OPSEC problems or vulnerabilities arise relating to their own or to other department or agency programs.

The responsibility for the development, implementation and maintenance of a department's or agency's OPSEC program rests with the head of the department or agency. The NSDD allows a great deal of latitude on how the program should be implemented; but it does require that all programs have, as a minimum, the followng features:

- specific assignment of responsibility for OPSEC direction and implementation;
- specific requirements to plan for and implement OPSEC in anticipation of, and where appropriate, during department or agency activity;
- direction to use OPSEC analytic techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures, i.e., change of proeedures, enhanced security, deception, etc.;
- enactment of measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of adversary intelligence threats and understand the OPSEC process;
- annual review and evaluation of the OPSEC procedures to improve OPSEC programs;
- provision for interagency support and cooperation with respect to OPSEC programs.

Heads of executive departments and agencies are also required to advise the National Security Council (NSC) on OPSEC measures required of other departments and agencies in order to achieve and maintain effective operations or activities.

Executive Agent For OPSEC Training

The NSDD assigned the Director of the National Security Agency (NSA) as the Executive Agent for interagency OPSEC training. The Executive Agent was given the responsibility to assist Executive departments and agencies to establish OPSEC programs; develop and provide interagency OPSEC training courses; and establish and maintain an interagency OPSEC support staff (IOSS), whose membership would include as a minimum, a representative of the Department of Defense, the Department of Energy, the Central Intelligence Agency, the Federal Bureau of Investigation, and the General Services Administration.

In order to carry out his NSDD responsibilities, the Director, NSA appointed a Director of Operations Security and established the IOSS. The Director of Operations Security has the responsibility for oversight and support of IOSS activities on behalf of the Executive Agent. In addition, the Director of Operations Security is responsible for implementation, direction and oversight of OPSEC within the NSA and the cryptologic community.

The Interagency OPSEC Support Staff

The NSDD stipulates that the IOSS will carry out national-level interagency OPSEC training for executives, program and project managers, and OPSEC specialists; act as consultant to Executive departments and agencies in connection with the establishment of OPSEC programs and OPSEC surveys and analyses; and provide an OPSEC technical staff, as required, for the NSC.

The IOSS was established in January 1989. The IOSS is located in suburban Maryland, just outside of Washington D.C. The IOSS is a distinctly interagency organization. The staff is comprised of individuals from the Executive departments and agencies required by the NSDD to provide representation. In addition, other organizations have been invited to assign persons to the IOSS to help provide OPSEC support to their parent organization and as a way to gain valuable OPSEC experience. The IOSS is comprised of individuals with both OPSEC and various technical expertise, and with experience in many different aspects of government activities.

The IOSS operates as a government "consulting firm" providing OPSEC advice and services to Executive departments and agencies. It can provide help in the areas of program development, training, briefings, developing reference materials and audiovisual aids, and providing or arranging for support to OPSEC surveys and other OPSEC activities. Initially, the IOSS is concentrating on assisting organizations in implementing OPSEC programs. The IOSS will also develop materials to assist organizations in establishing and maintaining their OPSEC programs. The IOSS sponsors a National OPSEC Conference, seminars on OPSEC related subjects and community of interest working groups.

Conclusion

The National OPSEC program was established as a response to the increasing need for and interest in, OPSEC by government departments and agencies. Interest has been increasing for three main reasons: (1) OPSEC practitioners have been improving and refining the OPSEC process making it more useful and easier to apply; (2) there has been a realization of OPSEC's natural potential in non-military as well as military activities; and most important, (3) there has been a general recognition that adversary intelligence collection capabilities are improving, the vulnerability to exploitation is increasing, and the impact of loss of data is escalating.

In the "information age" indicators, the category of information OPSEC was originally developed to protect, have become more difficult for organizations to control and much easier for adversaries to exploit. The loss of critical information to our adversaries has reached serious proportions and is impacting adversely on government activities. OPSEC has proved to be an essential element in ensuring effective operations of departments and agencies assigned or supporting national security missions with classified or sensitive activities.

Mr. Raskin is currently assigned to the Interagency OPSEC Support Staff. He is an employee of the National Security Agency (NSA). His previous assignments have been in the NSA Operations, and Information Systems Security Organizations.

Pizza Intelligence: An Update

Earlier this year we reported that Domino's Pizza claims it can predict when the government is about to undertake some sort of major activity based upon the increase in its pizza deliveries to the Pentagon and the White House. Pizza orders increased substantially just prior to troop deployments to Grenada, Panama, and the Middle East. According to *The Washington Times* of August 21, 1991, during the early hours of the abortive Kremlin coup in August, Domino's "Pizza Meter" registered 102 deliveries to the Pentagon, breaking thc Gulf War record by one; the White House ordered 52 pizzas, breaking its Gulf War record by seven. The CIA, by contrast, learned its OPSEC lesson: there were only two orders, and they were quickly cancelled.

The OPSEC Indicator, Fall 1991

The Interagency OPSEC Support Staff announces the Third National OPSEC Conference to be held in Las Vegas, Nevada on 4-7 May 1992 at the Stardust Hotel and Nellis Air Force Base.

MAINTAINING THE COMPETITIVE EDGE

LAS VEGAS
NEVADA

For registration information, send your name and address to:

Third National OPSEC Conference
1000 North Payne Street, Suite 300
Alexandria, VA 22314-1676

or call (703) 549-3024.

OPSEC: It's Not What You Think

By Robert B. Wignall, Department of Defense

Operations Security, or OPSEC as it is commonly referred to, is not a new discipline. In name, it has been around since the Vietnam War; in theory, probably a lot longer. But what is OPSEC? The acronym is frequently bantered about within the Department of Defense, the Intelligence Community, and related activities, but it is commonly used interchangeably to refer to a variety of security disciplines. Hopefully the following will help to pin down more precisely what OPSEC is and whet it is not.

Briefly, OPSEC is a discipline involving an analytical process. The OPSEC process is that of identifying critical information or "core secrets," of an operation that must be kept from an adversary if the operation is to succeed, and applying necessary countermeasures to deny that information to the adversary. OPSEC deals with information that, collected in pieces and combined in aggregate form, could reveal sensitive or classified aspects of an operation. The entire process involves identification of critical information; threat, vulnerability, and risk assessments; and application of countermeasures.

The difficulty with OPSEC is that it has been mandated in certain sectors of the Federal Government, primarily those dealing with sensitive national security information, without being fully explained. National Security Decision Directive (NSDD) 298 establishes a National Operations Security Program requiring that "each Executive department and agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal OPSEC program..." The problem is that NSDD 298 only accomplishes part of the goal; it tells *what* needs to be done, but not *how* to do it—at least not in sufficient detail.

Because of the nature of the mandate, everyone involved is very anxious to appear to be implementing OPSEC, but many have, at best, only a vague idea of what OPSEC entails. Consequently, we have "OPSEC" being used to describe everything from COMSEC to physical security. We hear of "OPSEC" programs being strengthened by erecting new fences, or by lecturing employees about divulging classified information over nonsecure telephones, or by performing vigorous material inspections at building egress points. While all of these measures certainly supplement a strong *operational* security program, they do not really reflect any application of Operations Security (the specific discipline) or the OPSEC process.

To really practice OPSEC, one must first assume the role of the adversary. The operation in question must be assessed from the outside in. The question that needs to be answered is, "If I am the adversary, what information do I need about this operation and how do I get it?" The thorough OPSEC analyst will collect as much information on an operation as is available through non-privileged means, also known as "open sources." and then conduct an analysis, or reconstruction of the event. Examples of information that can be of vital interest are shipping documentation, financial transactions, types of personnel assigned to the operation, travel schedules, etc. The point to recognize is that most of this information is unclassified, and therefore is not subject to traditional security controls. By identifying these indicators of critical information, the OPSEC analyst can recommend countermeasures that are often no more than simple administrative changes.

" ...everyone involved is very anxious to appear to be implementing OPSEC, but many have, at best, only a vague idea of what OPSEC entails."

The intent here is not to take anything away from the more "traditional" security measure that are taken to protect classified information. Vigorous physical security, personnel security, information security, technical security, and other measures ensure that an adversary must work hard to get the information he is after. *The goal of an effective OPSEC program is to address the information that "slips through the cracks"—to tie up loose ends, creating an impregnable "total security package."*

The subtlety of the OPSEC discipline, combines with a relative lack of knowledge of the subject, will continue to present obstacles to full-scale implementation of an effective and widespread OPSEC program. Only through a persistent program of education and awareness will we succeed. The point that must be made and understood is that OPSEC is more than the combination of traditional security measures taken to protect an operation—much more.

Interagency OPSEC Support Staff ★★★★★

Publications

Monograph and Publications Series

The following publications are available on request to the Interagency OPSEC Support Staff, 6411 Ivy Lane, Suite 400, Greenbelt, Maryland 20770-1405, (301) 982-2313/0323.

The National OPSEC Program	April 1990
The Great Conversation	April 1991
OPSEC Program Development Procedural Guide	April 1990
Compendium of OPSEC Terms	April 1991
OPSEC Program Evaluation	April 1991
Operations Security Planning	October 1991

Treaty Inspections Series

These publications may be ordered only by U.S. Government facilities and contractors that are subject to START Treaty inspection. Contact source above.

Overview of OPSEC for On-Site Treaty Inspection	October 1991
Treaty Inspections OPSEC Planning Guide	October 1991
Treaty Inspections OPSEC Survey Guide	October 1991
OPSEC Countermeasures for On-Site Treaty Inspections	October 1991
Treaty Inspections OPSEC Employee Handbook	October 1991
Facility Manager's Guide to Treaty Inspections OPSEC	October 1991
Program Manager's Guide to Treaty Inspections OPSEC	October 1991

Also available is the OPSEC Indicator, a newsletter which is published quarterly.

Due to the high volume of requests now coming in, there may be delays in receiving any of the above items.

OPSEC: Looking Back After The Storm

A First-Hand Account of OPSEC Training

by Carl A. Roper

> OPERATIONS SECURITY is the process by which information about our capabilities and intentions are denied to actual or potential adversaries by the identification, control, and protection of the planning and execution of current or future activities and operations. It focuses on the unclassified aspects of activities or operations. The ability of an adversary to deduce or infer meaning from such information could have proved very detrimental to our military forces stationed in the Persian Gulf region.

Desert Storm/Shield was a unique experience for military personnel deployed to Saudi Arabia and also for those stationed in the Continental United States.

The realities of war, the threat of terrorism, and the concerns of friends, families and co-workers, hit home very early. The 24th Infantry Division (Mechanized) (24th ID), Fort Stewart, Georgia, was one of the first Divisions to be alerted and deployed to Saudi Arabia. Some 17,000 personnel and all their equipment were, within a couple weeks, loaded and transported to Southwest Asia. Behind, they left a great many families, friends, and co-workers.

For individual members of units, regardless of type, the application of personal awareness to OPSEC really started for the troops upon arrival at Fort Stewart. Fort Stewart was used as a staging ground for activated reserve units who were getting training and briefings before embarking for the Middle East. What specific training was required for a unit, when they were scheduled to depart, where they were going within the theater of operations, etc., became closely held information.

The requirement to present initial security briefings to many units gave me almost a full-time job from the start. Further, reinforcing that briefing with realistic examples was critical to properly educating the troops. Some units might be on post only a "short" two weeks, while others could remain a month or longer, depending upon unit training requirements and their priority for movement overseas. Therefore, briefings needed to be scheduled around all other training requirements. This meant starting the day with some briefings at 6:30 a.m.; even giving them at 10:30 p.m. was not uncommon.

As the 24th ID departed in August, 1990, everyone knew day-to-day activities would not be the same at Fort Stewart. Everyone needed to live Operations Security [OPSEC] in what they did and didn't do, who they talked to, and what they said in various situations.

When the 24th ID deployed, so did all its Intelligence & Security assets. Some regular Army personnel were left on base to continue day-to-day functions. Army Reservists, both individuals like myself, and entire units were then called to active duty to ensure the continued operation of the base, especially since Fort Stewart was a major training site for personnel preparing for Saudi Arabia.

I came to Fort Stewart and found a great deal needed to be accomplished in a hurry. The traditional OPSEC briefing, to which we are accustomed—which tends to be somewhat formal and structured—needed to be presented through a more personal and down-to-earth approach. Time constraints necessitated that OPSEC be combined with the subversion and espionage [SAEDA*] and terrorism awareness training. The subject matter had to be appropriately mixed to allow the military troops to receive the information in the context of how they would be "living it" in the very near future.

In past years, all of us have devoted many hours to developing and presenting OPSEC-specific training (usually as structured briefings) for our people. In the past, people would attend an OPSEC briefing then forget about it until next year's briefing was given. In the current world situation, people would have to remember!

In reading this article, the phrase "briefing" crops up over and over. When you see "briefing," read "educational training." Everything accomplished was training for the troops, the garrison and the dependants, whether formal or informal, structured or unstructured, on a stage, as a group gathered around a vehicle, or as a one-on-one discus-

**Subversion and Espionage Directed Against the Army* sion. I found the formal briefing presentation style we are accustomed to—a lecture, if you will—was not the way to go. I used an informal approach; an educational mix of facts with current examples which got the point across, was better received, and allowed for a greater interaction between the participants and myself.

OPSEC Briefing Concerns

The Division had left for Saudi Arabia in late August and, three weeks later, I was the first of several activated reservists arriving to fill the void within the Directorate of Security [DSEC]. One of the first tasks of the new counterintelligence [CI] office staff was the rapid development of real-world briefings concerning the intelligence, security, and terrorist threats the troops were up against. Such briefings also had to include appropriate handouts for the participants. The CI office had no major reference files or manuals since most left with the Division; the few remaining items were incomplete, non-applicable, or out-of-date.

Literally overnight, the CI office chief and myself, using our own materials—much of which had been accumulated over many years in the Army Reserve—culled specific information, "researched" our memories, and melded the information to meet the needs of the troops. Time was of the essence. Nobody knew when the balloon might go up, so the luxury of revision did not exist—it had to "work" the first time!

From Fort Gillem, GA came the Mobilization Operations Center [MOC], responsible for coordinating training for the numerous activated reserve units coming to Fort Stewart. Through the MOC I coordinated my training for each unit.

Another individual within the office reviewed hundreds of slides for possible use as briefing aids. As only a limited number of slides were usable, we created and made our own. Copies of some slides were used as view-graphs.

Figure 1 highlights the major OPSEC areas which I decided to cover during the briefings. Although the list may seem short, it covered a myriad of information topics and sub-areas that identify potential sources of damage to a unit, no matter what its size or mission.

Essential Elements of Friendly Information (EEFI)

gathered by foreign intelligence from indicators, such as

1 - Signatures:	Come from the mere presence of a unit
2 - Profiles:	Come from unit activity
3 - Patterns:	Come from doing things the same way

Although the above indicators are of great importance, the enemy is also very interested in learning everything about your:

Strengths

Mission

Key Individuals

Logistic shortages

Reinforcements

Unclassified Information Can be Sensitive

Figure 1

Security Training To The Units

Army Reserve units normally receive an annual OPSEC briefing at home station. In the context of Desert Shield, the units had neither the time nor the informational resources to develop and present one before leaving their home station; other concerns took precedence.

One problem that could not be solved, though, was the open disclosure of key unit personnel identification, equipment, recent past training, and generic mission statements for these units. Although such information is public knowledge in some cases, it may not be widely known. You see, activated units consist of "hometown" people. When activated, the local newspapers, radio, and television stations were right there to document everything. Past information about the unit and its personnel were pulled from news files and the information relating to past training and the unit mission, etc., became local headlines. Such specifics tied to a unit provide a wealth of information to a foreign agent.

These details—unclassified but sensitive information—that some people wouldn't think twice about, suddenly became "most interesting." OPSEC, at home station, was something to be concerned about . . . . but it was too late; the information was already out in the public arena.

On a more positive note, however, Military Police and a few other units, having either CI or well-informed security personnel attuned to OPSEC, provided briefings to their personnel at home station. The briefings were pertinent and concise. These troops remembered them, and "loose talk" dropped dramatically within these units upon arrival at Fort Stewart.

For these troops, up-to-date information was a real necessity, and unit training sessions going on around the clock, even on weekends were used to educate the troops in regard to OPSEC: their time became my time. Day-to-day reviews of incoming message traffic, questions asked during previous briefings, and telephone inquiries were targeted areas of OPSEC concern. When items of interest were found, we rapidly updated the briefing content.

The Initial Briefing

During the first of two briefings that all deploying personnel received, we covered OPSEC, SAEDA, and terrorism, being combined in such a manner as to get the point across that security is everybody's job. Depending on how long a unit would be on base, a "training point" had to be made early that OPSEC is something that must be taken seriously.

Being on an open post, nobody knew who might be around attempting to obtain information, so the troops were told that during their stay at Fort Stewart, CI personnel (mainly, me) would attempt to strike up or listen in on their conversations in public areas. We did this to check out their practical application of OPSEC training, identify potential areas of concern, and to determine any areas needing to be shored up. I passed back to the unit any concerns which I observed with appropriate guidance on how to eliminate those OPSEC indicators.

Loose talk which we overheard that related to material requirements, unit personnel status reports and related listings, or a shortage of equipment, were of immediate concern. I found that much information could be gleaned by listening to or talking with the troops around the Post Exchange complex or at the laundromat. Based upon what was picked up, I also checked to see what could be obtained in terms of "hard copy" information; I looked at their trash which was discarded into the big dumpsters daily. [Amazingly enough, not even a handful of personnel recognized or paid attention to me; I was dressed "appropriately."]

The Follow-up Briefing

I reinforced the initial briefing with a second one about a week later. In the second briefing, examples of what had been learned or found—through conversations, listening and in the trash—were integrated. The point was brought home to the troops that if I can do it (and I didn't try very hard), so could an adversary. A foreign agent could possibly learn significant items of interest such as the unit's total personnel strength (or lack thereof), shortages, specialized equipment that the unit might have ordered or just received, what training was being accomplished, and how well the unit performed such training.

A check of the unit was again made a few days later. It showed that they were really getting the message and taking it seriously. Conversation that could be overheard while off-duty was limited to sports, home and family topics. The avoidance of specific OPSEC areas of concern was very noticeable. Paper in the trash became almost non-existent for some units; the base shredder got a lot of work.

Getting into the habit of protecting OPSEC sensitive information started at the unit, with everyone from the commander on down becoming involved. It seems everyone realized that once the unit got into the Gulf region, it would be too late to start thinking about how to protect this "unclassified and innocent" information. The points emphasized during both briefings were well received and acted upon by the units.

Using Expertise From Veterans

In developing my briefing content, I took advantage of knowledge from soldiers who had served in Vietnam. Over and over in the briefings, they were the first to pose questions about some of the finer points of security in the field. They had experienced the realities of war and were definitely concerned about OPSEC, SAEDA, and terrorism. These veterans of a distant war provided personal insights into the realities of armed conflict and showed other unit personnel where emphasis needed to be placed.

Unit commanders had these more experienced personnel present further training to their fellow soldiers: to show them how to increase both personal and unit security in a field environment.

Departure For The Persian Gulf Region

Units sometimes got word "through the grapevine" that they would depart on such-and-such date. We found that such dates were somewhat accurate, but mostly guess-work based upon completion of training.

One method the Fort Stewart command staff used for keeping the knowledge of departure dates and times to a minimum was to continue training to almost the last day and schedule a day or two as a training break "with more training to follow." Another was not to inform even the unit commander until about 24 hours ahead of time. Even then, the time could be slipped or speeded up.

In preparing the units for departure, troop movement was restricted to their barracks area or relocated to an unused base building. This separated the troops from the rest of the garrison personnel, effectively isolating specific talk of departure time (to anyone else who might be interested).

Departure times were varied throughout the day and night. Busses, with windows tinted to lower the visibility of departing troops, were used to transport units from Fort Stewart to Hunter Army Air Field for departure to the Gulf. The same busses were also used for general base transport so that their use in moving troops to the departure point wouldn't stand out from other bus traffic.

The Garrison

Along with the departing troops, the CI office also provided base personnel and dependents OPSEC-related briefings. Garrison personnel; the military left behind; and civilians in administration, logistics, operations, the post exchange (PX), the commissary, and other smaller elements were included. The garrison command received weekly briefings, in addition to specialized 'in-office' presentations to keep the post commander abreast of potential concerns.

The garrison Public Affairs Office (PAO) became a focal point for the news media, for which reason we needed to coordinate closely with them. PAO personnel were attuned to OPSEC, and escorted news media personnel for all interviews and picture taking while on post. In some instances, the PAO took pictures, then allowed news personnel to use them. This cut down on the possibility of sensitive mission-related—though wholly unclassified—information becoming available to the public.

The CI office also reviewed pictures taken by PAO personnel in the Gulf region. Any picture that might prove detrimental in any way was kept from publication in the post newspaper or release to the local press.

Family support groups, the family members of deployed personnel, were provided low-keyed briefings within weeks after my arrival. The briefings were not presented as "security" or "OPSEC," but rather on areas of concern which all of them needed to be aware of. The knowledge that sons and daughters, brothers and sisters, and mothers and fathers were "in harm's way" did a great deal to help promote an understanding of why the elimination of "loose talk" was so vitally important, even at home station. The spouses and family members I spoke to were very concerned, and took the information to heart. Early on, I overheard support group spouses and others "correcting" other people for talking about certain information they may have heard through the grapevine, or from letters and/or telephone calls received from someone in Saudi Arabia.

My briefings were generic but included some specifics that could affect family members in the Gulf region. As an additional monitoring effort, I attended the weekly spouse meetings for both Fort Stewart and Hunter Army Air Field. In this manner, if a question or comment were posed that might have OPSEC ramifications or touch on a sensitive subject area, I could step in. [In retrospect, the monitoring effort helped, especially just before and during the crucial days of the war. The fact that news media had access to spouse meetings meant that any word spoken could end up in the daily paper.]

One element on the military installation that some security and intelligence people tend to overlook is the base Military Police (MPs). The assumption that, as MPs, they are always aware of the situation, is not necessarily the case. I received weekly calls from MP units asking for pertinent and up-to-date security briefings, not only in OPSEC, but other areas as well.

Because of the publicity which the 24th ID received upon its departure [CNN television headquarters being only an hour away], Fort Stewart (and to a lesser extent, Hunter Army Air Field) was nationally known. Potentially, anything that could go wrong would adversely affect morale of the people living in, on and around the bases, and would also be spread across the national news that day. Thus, we provided the MPs with regular training, and gave them weekly updates, ensuring they were kept apprised of all areas of OPSEC and security concern.

Liaison

At any facility, whether a military installation or an office building, people cannot be concerned only with what happens within the facility. There is a need to know what happens outside. What other forces are out there that can affect daily, short- and long-range activities? Where does security awareness and training need to be increased, and in what areas? Liaison greatly assists in providing answers.

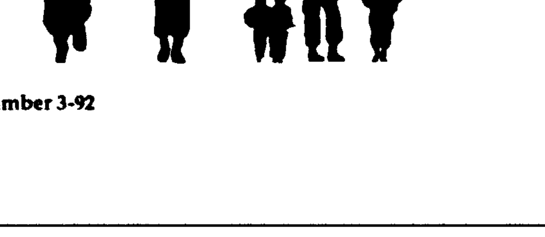
Liaison was an important tool for OPSEC awareness. Our CI office developed and maintained contacts with over 40 federal, state, and local agencies at some 70 different locations throughout Georgia and North Florida. Weekly contact proved an effective means of exchanging information with our counterparts outside the base proper. What affected them could, directly or indirectly, affect Fort Stewart also.

The Directorate of Security's CI office hosted a one-week crisis management course in December 1990, which was conducted by the Federal Law Enforcement Training Center, from Glynco, Georgia. Representatives from all garrison activities and local law enforcement were invited. Law enforcement personnel came at no cost to their agencies. This was a tremendous effort on our part, having the crisis management training in addition to other requirements. But the informal rapport that developed between these numerous representatives and the CI office personnel became the basis for a better cooperation which stood up well in the months to come.

What Should We Be Doing Now?

The troops are home, but the mission of the military continues . . . and so does OPSEC. We can't afford to wait until the next world problem is addressed; we must start now. We know that changes at the local level are required to make the program work effectively. In essence, effective OPSEC educational training—tailored to the facility and its mission, with emphasis on each individual contributing and supporting the program—is a "must" that can never be emphasized enough. If you are a security professional who has briefing or training responsibilities, I strongly recommend that you use current examples within the unit, facility or installation, to bring the point home. OPSEC can work in the real-world environment where the lives of friends, co-workers and fellow Americans are at stake. It can work, but only with your drive, determination, and persistence to make it work!

In summary, the informal approach applied by people responsible for OPSEC training worked extremely well at Fort Stewart, Georgia. Discussion with returning troops indicated the DSEC CI presentations were very effective, superior to what was given to many troops while in the war zone, and truly "on the mark." These kinds of comments made the entire office feel justifiably proud of our efforts in supporting our fellow soldiers in the operational theater.



About the Author: An Army Reservist, Mr. Roper was assigned to the Fort Stewart, Georgia, Directorate of Security's Counterintelligence Office during Operation Desert Shield/Storm. He provided OPSEC and other security training support, in addition to other duties, to the Fort Stewart and Hunter Army Air Field garrisons. In his civilian job, he is an instructor with the Department of Defense Security Institute.

Aiding the Enemy: The Case of Albert T. Sombolay

SFC Albert T. Sombolay

We normally think of espionage which results in damage to national security or places the lives of our combat personnel at risk as associated with the sale or passing of classified information. This is not always the case. What follows is an account of espionage and betrayal by one of our own service members who was recently convicted of attempting to sell unclassified information that might have been very damaging to US operations in the recent Gulf War. This is the same type of information, by the way, that normally deserves protection through the application of OPSEC countermeasures.

Army artillery specialist Albert Sombolay was born in the central African nation of Zaire, became a naturalized US citizen in 1978, and joined the army in 1985. By the time of the Gulf Crisis, he was stationed at Bad Kreuznach Germany with the 8th Infantry Division. In December 1990, whether because of money or dissatisfaction with the service—his motives are yet to be explored—Sombolay began to contact the embassies of Iraq, Jordan and Libya, offering to market information and equipment that could compromise anticipated allied operations in the Persian Gulf theater. This took place a few weeks before our air attack on Iraq and combat operations in Kuwait.

An important fact in this case is that Somoolay did not possess a security clearance and consequently had no access to classified information—no secret documents, no encryption devices, no knowledge of intelligence sources and methods; none of the high-priority items that we normally associate with damage done by classic espionage activities. But as is usually the case, the culprit's attempts to sell information soon came to the attention of Army Military Intelligence. He was arrested, convicted, and sentenced to serve for 34 years at hard labor, forfeited all pay and allowances and was dishonorably discharged. Specifically, Albert Sombolay was convicted by a military judge of committing two acts of espionage, two attempts of espionage, and of aiding the enemy.

Yes, four counts of espionage or attempted espionage and no classified information or material involved in the case! This is where the OPSEC connection becomes clear. Sombolay had offered the following to his potential clients:

- troop deployment information related to Desert Storm
- samples of chemical warfare protection gear
- photographs of his unit's activities in Saudi Arabia after his arrival in the theater
- identification information (how to recognize US units in the field

According to an Army statement issued at the time of Sombolay's arrest, he had in fact "admitted to providing Desert Shield-Desert Storm deployment information, identification documents, and samples of US Army chemical protection equipment to a foreign intelligence officer from Jordan." Disclosure of his conviction was delayed for four months until Army Intelligence could determine that Sombolay had acted alone. He is reported to have been paid about $1,300 for his activities. A paltry sum when compared to a ruined life, a lost career, and to the despair inflicted on a wife and family.

The message is obvious: all of the above information offered for sale by Sombolay was or should have been protected under an OPSEC countermeasures program because its inadvertent or careless disclosure could have hurt us badly. In this instance there is no indication that OPSEC procedures failed; *the compromise was deliberate.* But whether we lose sensitive information through negligence, ignorance, or espionage, the effect is potentially the same. You don't have to be a West Point graduate to realize that the use of any of this information (although unclassified) by a potential adversary might have resulted in the loss of life and resources in the field of battle. This is precisely why the military court in sentencing Sombolay took very strong exception to this crime. And, this also is why the United States Government has mandated that "each Executive Department or Agency, assigned or supporting national security missions with classified or sensitive activities, establish an OPSEC program."

Security Awareness Publications Available From The Institute

Postage Requirement: We ask that you provide postage, but the publications are free of charge. Instructions for figuring postage are provided on the next page. See ordering instructions below.

To Order:

1. Check publications on the list below.
2. Add total weight. Include 1 oz. for envelope.
3. Figure the postage using information on the next page.
4. Choose envelope size (see chart 4, next page); affix postage and mailing label.
5. Send this page with **stamped** (no checks, please), self-addressed envelope to:

DoD Security Institute
Attn: EPD
c/o DGSC
Richmond, VA 23297-5091
(804) 279-5314/4223 or DSN 695-5314/4223

(TAS) Training Aids for Security Education. February 1992. Catalog of audiovisual and printed material of interest to security educators. Instructions for ordering. . . . . ____ 3.5 oz.

(REC) Recent Espionage Cases: Summaries and Sources. September 1991. Seventy-eight cases, 1975 through 1989. "Thumb-nail" summaries and open-source citations. . . . . ____ 3.5 oz.

(FIT) The Foreign Intelligence Threat to U.S. Defense Industry. By Defense Security Institute staff. January 1991. . . . . ____ 3.0 oz.

(FTB) Foreign Travel Briefing. 1981. Script of briefing designed for cleared employees traveling to designated countries. Outlines methods used by hostile intelligence services and precautions against them. (For 14-minute tape/slide briefing, see "Training Aids for Security Education.") . . . . ____ 2.5 oz.

(SIT) Soviet Intelligence Targeting of the US Scientific Community, August 1990. A basic tutorial for those in contact with the Soviet scientific community. . . . . ____ 3.0 oz.

(CUT) Control of Unclassified Technical Data with Military or Space Application, May 1985. DoD 5230.25-PH. 20-page booklet prepared by the Office of Secretary of Defense explaining the DoD program to limit public disclosure of export-controlled technical data and the special markings for technical documents. . . . . ____ 1.5 oz.

(SAM) Soviet Acquisition of Militarily Significant Western Technology: An Update, September 1985. Western products and technology secrets are being systematically acquired by intricately organized, highly effective collection programs. . . . . ____ 5.5 oz.

Individual back issues of the *Security Awareness Bulletin* up through #2-89 are no longer available from the Institute. Reprints of past feature articles have been brought together under a single cover in a publication, *Security Awareness in the 1980s*. Available from the Government Printing Office, stock number 008-047-00394-3. Price is $11.00. To order call (202) 783-3238.

Security Awareness Bulletin. Back issues available from the Institute:

(1-90)	Oct 89	Foreign Travel. FOR OFFICIAL USE ONLY.	____	3.0 oz.
(2-90)	Jan 90	The Case of Randy Miles Jeffries	____	3.0 oz.
(3-90)	Apr 90	Beyond Compliance – Achieving Excellence in Industrial Security	____	5.5 oz.
(4-90)	Aug 90	Foreign Intelligence Threat for the 1990s	____	3.5 oz.
(1-91)	Jan 91	Regional Cooperation for Security Education	____	3.5 oz.
(2-91)	Sep 91	AIS Security	____	3.5 oz.
(1-92)	Oct 91	Economic Espionage	____	3.5 oz.
(2-92)	Feb 92	Self-Inspection Handbook	____	4.0 oz.
(#-92)	Mar 92	OPSEC	____	2.5 oz.
		Allow for envelope	✓	1.0 oz.
		Total weight	____	
		Send postage in the amount of	$________	

Postage Information

If total weight is **11 ounces or less**:

Chart 1: find the amount of postage

Example: If total weight is 4.5 oz., postage is $1.21.

Chart 1

Weight not exceeding:	First Class Rate
1 oz.	$0.29
2 oz.	0.52
3 oz.	0.75
4 oz.	0.98
5 oz.	1.21
6 oz.	1.44
7 oz.	1.67
8 oz.	1.90
9 oz.	2.13
10 oz.	2.36
11 oz.	2.59

Chart 4 Envelope Size

Publications measure 8 1/2 x 11"

No. of pubs	envelope
1-9	9 1/2 x 12"
10-18	10 x 15"

If total weight is **greater than 11 ounces:**

Chart 2: find postal zone using first 3 digits of your ZIP code

Chart 3: determine amount of postage using weight and zone

Chart 2 Postal Zone Chart

ZIP Code Prefixes	Zone	ZIP Code Prefixes	Zone	ZIP Code Prefixes	Zone
004-005	3	295	3	513-560	5
006-009	7	296	4	561-576	6
010-043	4	297	3	577	7
044	5	298-322	4	580-585	6
045	4	323-325	5	586	7
046-047	5	326	4	587	6
048-065	4	327-349	5	588-593	7
066	3	350-353	4	594	8
067	4	354-355	5	595	7
068-119	3	356-359	4	596-599	8
120-126	4	360-361	5	600-608	5
127	3	362	4	609	4
128-147	4	363-367	5	610-617	5
148-163	3	368	4	618-619	4
164-165	4	369	5	620-667	5
166-172	3	370-374	4	668-672	6
173-174	2	375	5	673	5
175-196	3	376	3	674-693	6
197-223	2	377-379	4	700-705	5
224-225	1	380-383	5	706	6
226	2	384-385	4	707-729	5
227	1	386-397	5	730-742	6
228-229	2	399-410	4	743-744	5
230-232	1	411-412	3	745-748	6
233-237	2	413-414	4	749	5
238-239	1	415-416	3	750-754	6
240-241	2	417-418	4	755	5
242-243	3	420	5	756-784	6
244-245	2	421-436	4	785	7
246-253	3	437-439	3	786-796	6
254	2	440-443	4	797-831	7
255-266	3	444-447	3	832-844	8
267-268	2	448-455	4	845	7
270-274	3	456-457	3	846-864	8
275-279	2	458-496	4	865-885	7
280-286	3	497-509	5	889-999	8
287-294	4	510-512	6		

Chart 3 Priority Mailing Rates by Zone

Weight, up to –	*1, 2, 3*	*4*	*5*	*6*	*7*	*8*
2 lbs.	$2.90	$2.90	$2.90	$2.90	$2.90	$2.90
3 lbs.	4.10	4.10	4.10	4.10	4.10	4.10
4 lbs.	4.65	4.65	4.65	4.65	4.65	4.65