DNA-TR-83-05

(10)

Proceedings of the
8th Annual Symposium
on the Role of Behavioral
Science in Physical Security

# Conflict & Confrontation in a Civilized Society

7-8 June 1983
Springfield, Virginia

Sponsored by:
Defense Nuclear Agency
Nuclear Security Division
Washington, D.C. 20305

dna

Approved for public release:
distribution unlimited.

## DISPOSITION

Destroy this report when no longer needed. Do not return it to the originator.

## DISCLAIMER

The findings in this report are not to be construed as an official Department of Defense position unless so specified by other official documentation.

## WARNING

Information and data contained in this document are based on the papers available at the time of preparation. No attempt has been made to edit papers. The views expressed in them are those of their authors and should not be construed as representing the Defense Nuclear Agency. Correctness is the sole reponsibility of the authors.

## TRADE NAMES

The use of trade names in this report does not constitute an official endorsement or approval of the use of such commercial hardware or software. The report may not be cited for purposes of advertisement.

# COMPONENT PART NOTICE

THIS PAPER IS A COMPONENT PART OF THE FOLLOWING COMPILATION REPORT:

(TITLE): Proceedings of the Annual Symposium on the Role of Behavioral Science in Physical Security (8th), Conflict & Confrontation in a Civilized Society Held at Springfield, Virginia on 7-8 June 1983.

(SOURCE): Defense Nuclear Agency, Washington, DC.

TO ORDER THE COMPLETE COMPILATION REPORT USE AD-A137 213.

THE COMPONENT PART IS PROVIDED HERE TO ALLOW USERS ACCESS TO INDIVIDUALLY AUTHORED SECTIONS OF PROCEEDINGS, ANNALS, SYMPOSIA, ETC. HOWEVER, THE COMPONENT SHOULD BE CONSIDERED WITHIN THE CONTEXT OF THE OVERALL COMPILATION REPORT AND NOT AS A STAND-ALONE TECHNICAL REPORT.

THE FOLLOWING COMPONENT PART NUMBERS COMPRISE THE COMPILATION REPORT:

| AD#: | TITLE: |
|---|---|
| P002 667 | Some Observations on the Terrorist Adversary. |
| P002 668 | Social Psychology of Selective Violence in Society: Terrorism. |
| P002 669 | Evolution of Behavioral Science in Security Management. |
| P002 670 | Security Vulnerability and Security Awareness. |
| P002 671 | The 1984 Olympic Games: A Challenge and an Opportunity for Law Enforcement. |
| P002 672 | Operational Utility of Psychology Instruments to Law Enforcement and Security. |

COMPONENT PART NOTICE (CON'T)

AD#: TITLE:

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

| REPORT DOCUMENTATION PAGE | | READ INSTRUCTIONS BEFORE COMPLETING FORM |
|---|---|---|
| 1. REPORT NUMBER<br>DNA-TR-83-05 | 2. GOVT ACCESSION NO.<br>AD-A137 213 | 3. RECIPIENT'S CATALOG NUMBER |
| 4. TITLE (and Subtitle)<br>PROCEEDINGS OF THE 8TH ANNUAL SYMPOSIUM ON THE ROLE OF BEHAVIORAL SCIENCE IN PHYSICAL SECURITY: CONFLICT AND CONFRONTATION IN A CIVILIZED SOCIETY | | 5. TYPE OF REPORT & PERIOD COVERED<br>Technical Report<br>6. PERFORMING ORG. REPORT NUMBER |
| 7. AUTHOR(s)<br>Compiled by Major Barbara G. Curtis, USA | | 8. CONTRACT OR GRANT NUMBER(s) |
| 9. PERFORMING ORGANIZATION NAME AND ADDRESS | | 10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS |
| 11. CONTROLLING OFFICE NAME AND ADDRESS | | 12. REPORT DATE<br>31 October 1983<br>13. NUMBER OF PAGES<br>90 |
| 14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) | | 15. SECURITY CLASS. (of this report)<br>UNCLASSIFIED<br>15a. DECLASSIFICATION/DOWNGRADING SCHEDULE<br>N/A since UNCLASSIFIED |

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Physical Security
Human Performance
Terrorism
Nuclear Weapons Security
Law Enforcement

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

These proceedings include all papers submitted for publication that were presented at the 8th Annual Symposium on the Role of Behavioral Science in Physical Security: Conflict and Confrontation in a Civilized Society which was held in Springfield, Virginia on 7 and 8 June 1983.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

TABLE OF CONTENTS


Page

Agenda . . . . . 3

Axiomatic Impact of Adversary Behavior . . . . . 5
Brian Michael Jenkins, Rand Corporation

Social Psychology of Selective Violence in Society: Terrorism . . . . 15
D. G. Macnair, Gulf Refining & Marketing Co.

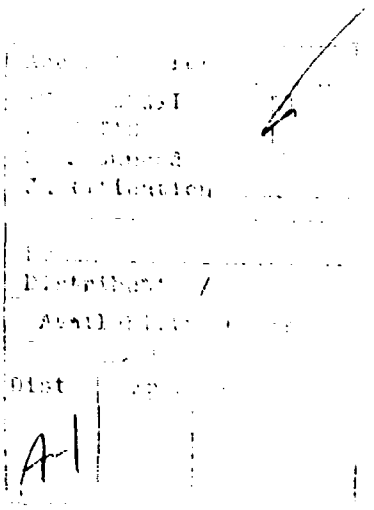
Evolution of Behavioral Science in Security Management . . . . . 25
Richard Healey, CPP, Professional Protection Enterprises, Inc.

Security Vulnerability and Security Awareness . . . . . 37
Timothy J. Walsh, CPP, Harris & Walsh Management Consultants

Correlation of Values in Planning the Security of a Multi-National Sports Event Attracting Significant Media Attention . . . . . 55
Commander William Rathburn, Los Angeles Police Department

Operational Utility of Psychology Instruments to Law Enforcement and Security . . . . . 67
Dr. Ira Berstein, Professor of Psychology,
University of Texas at Arlington

Roster of Participants . . . . . 83

## AGENDA

8th Annual Symposium on the Role of Behavioral Science in Physical Security

CONFLICT AND CONFRONTATION IN A CIVILIZED SOCIETY

Tuesday, 7 June 1983

| | | |
|---|---|---|
| 0830-0915 | Registration | |
| 0915 | Opening Remarks | Lieutenant General Harry A. Griffith, USA<br>Director, Defense Nuclear Agency |
| | Adminstrative Announcements | |
| | "Axiomatic Impact of Adversary Behavior"<br>Brian Michael Jenkins, Rand Corporation | |
| | "Social Psychology of Selective Violence in Society: Terrorism"<br>D.G. Macnair, Gulf Refining & Marketing Co. | |
| 1145-1300 | Lunch | |
| 1300 | "Evolution of Behavioral Science in Security Management"<br>Richard Healey, CPP, Professional Protection Enterprises, Inc. | |
| | "Security Vulnerability and Security Awareness"<br>Timothy J. Walsh, CPP, Harris & Walsh Management Consultants | |
| | "Legitimacy of the Nuclear Arsenal--A Behavioral Interrogatory"<br>S. D. Vestermark, Jr., Fellow, Inter-University Seminar on Armed Forces and Society | |
| 1700-1800 | Social Hour | |
| 1800-1900 | Buffet | |
| 1900-2000 | "Correlation of Values in Planning the Security of a Multi-National Sports Event Attracting Significant Media Attention"<br>Commander William Rathburn, Los Angeles Police Department | |

Wednesday, 8 June 1983

0900 Administrative Announcements

"Operational Utility of Psychology Instruments to Law Enforcement and Security"
Dr. Ira Bernstein, Professor of Psychology, University of Texas at Arlington

"Changing Assessment Methodology of the Adversary View of Security"
James L. Stinson, CACI, Inc.-Federal

Closing Remarks — Colonel Charles R. Linton, USAF
Director for Operations, Defense Nuclear Agency

1200 End of Symposium

# SOME OBSERVATIONS ON THE BEHAVIOR OF THE TERRORIST ADVERSARY

Brian Michael Jenkins

The Rand Corporation*

July 1983

This meeting focuses on the behavioral aspects of physical security. Our research at The Rand Corporation has for the past ten years focused on the opposite side of that issue--the behavior of the potential adversary. Although our research has addressed the possible motivations, capabilities, and *modus operandi* of a wide spectrum of adversaries including those who might be motivated by ideological, economic, or idiosyncratic reasons, one particular category of adversary--the political terrorist--has dominated our attention.

In the course of that research we have addressed such questions as:

- Will terrorists attack a particular type of target?
- How do terrorists measure their own success?
- Will terrorists ever employ weapons of mass destruction?
- Will terrorists go nuclear?

Answers to these questions depend on presumptions about the behavior of terrorists and terrorist groups. This is a realm of few axioms. Little systematic research has been done. Government agencies are concerned more with the pragmatic problems of defense against terrorism--How do we protect our embassies against takeover by terrorists?--and generally have been reluctant to support basic behavioral research. Data is hard to get; until recently, few terrorists talked. Indeed, what we know about the terrorist mind today may be compared to what the outside world

*Views expressed in this paper are the author's own and are not necessarily shared by Rand or its research sponsors.

knew about Africa in the middle of the nineteenth century. A person in London, Paris, or Berlin knew the general shape of the continent, and a few explorers had traveled up the African rivers and returned with their observations. But for the most part, it remained *terra incognita* for Europeans, a dark continent. So it is with the terrorist mindset today. We have a handful of observations, a few notions, some assumptions, and some assertions, but some of the ideas seem as fanciful as those demons and sea monsters that ancient cartographers put at the far edge of what they knew.

Today I would like to share with you some of the things we have learned about terrorism in general and the terrorist adversary in particular, and identify a few of the many questions that remain. We begin with a paradox!

Despite increasing government success in combating terrorists, the total volume of terrorist activity worldwide has increased during the last ten years. It is a paradox that frustrates governments and confounds analysts.

Governments have become tougher in dealing with terrorists. More and more governments have adopted hard-line, no concessions, no negotiations policies--a marked change from the situation in the early 1970s when governments often gave in to the demands of terrorists holding hostages. Terrorists who seize embassies, a popular tactic in the 1970s, now face arrest and prosecution.

They also risk being killed as more and more governments have demonstrated their willingness to use force wherever possible to end hostage episodes at home and abroad. When Arab separatists seized the Iranian embassy in London in April 1980, the British government refused to meet any of their demands and later sent in SAS commandos to rescue the hostages. All but one of the terrorists were killed in the assault. Terrorists who seek worldwide publicity and political concessions by by barricading themselves with hostages now must also contemplate being shot.

Governments sometimes still make secret deals with international terrorist groups, offering freedom of movement in return for immunity from attack; but with some exceptions, governments appear less inclined

to "parole" imprisoned foreign terrorists simply to avoid further attacks.

At the technical level, governments have become more proficient in combating terrorism. They have skillfully used offers of reduced sentences, conditional pardons, new identities to key witnesses and other inducements to persuade at least some terrorists to provide information about their organizations. Italy has been particularly successful in exploiting the so-called "repentants," as they call apprehended terrorists who have taken advantage of a new law providing reduced sentences in return for information. The willingness of captured Red Brigades members to talk was one of the key factors in the rescue of General Dozier in 1982. The collection and analysis of intelligence have improved. International cooperation has increased.

Physical security around likely terrorist targets also has greatly increased. It is harder now, though still possible, to smuggle weapons aboard airliners. Embassies have become fortresses. Diplomats and top executives often travel in armored limousines with armed bodyguards. Specialized tactics and skills have been developed for use in hostage situations.

Worldwide, thousands of terrorists have been arrested or compelled to go deeper underground. Some groups have been virtually destroyed. Others are hard-pressed by authorities.

Most of the Red Brigades now reside in prison. German police captured the operational heads of the Red Army Faction in December of last year. Eleven members of the FALN, a Puerto Rican separatist group, were apprehended in Illinois three years ago. One of the most wanted Puerto Rican separatist bombers was recently captured in Mexico.

But despite these undeniable achievements, the total volume of terrorist activity in the world has not diminished. Like the Hydra--the mythical many-headed monster that grew two heads each time one was severed--terrorism persists, even grows, despite defeats. Authorities are able to suppress terrorists at least temporarily, but thus far have been unable to reduce terrorism at least not easily, without resorting to unacceptable methods of repression.

Old groups survive. New groups appear. They are generally smaller, more tightly organized at the operational level and harder to penetrate, sometimes less structured at the national level and harder to predict, always more violent.

Exact figures vary according to the source of information, collection criteria and procedures, but the trajectory of terrorism continues upward. While in some countries terrorist activity has declined, it has increased in others. Terrorism declined sharply in Italy last year but exploded in France. The number of terrorist incidents in Israel dropped sharply after Israel's invasion of Lebanon, but the number of terrorist attacks on Israeli and Jewish targets abroad went up.

Governments may be able--and more willing--to pursue local terrorists than those who cross borders to carry out their attacks or who attack targets connected to foreign governments. Counting local and international terrorism together, we see a slight decline in the total number of incidents since 1980 but a 13 percent annual increase in the number of deaths caused by terrorists. Looking at international terrorism by itself, the picture is worse. The first three years of the eighties have shown an annual increase in international terrorism of approximately 30 percent--twice the rate of increase in the 1970s. Overall, terrorist activity has increased four-fold in the decade since the Munich incident.

This is not to say that terrorism has been a success. Nowhere, this side of the colonial era, have terrorists yet achieved their own stated long-range goals. Terrorists are able to attract publicity to themselves and their causes. They cause worldwide alarm. They create crises that governments are compelled to deal with. They make governments and corporations divert vast resources to security measures. Occasionally they win concessions. In several instances they have provoked the overthrow of governments, usually by elements willing to use repressive tactics with less constraint.

Terrorists have been unable to translate the consequences of terrorism into concrete political gains. Nor have they yet revealed a convincingly workable strategy that relates terrorist violence to

positive political power. In that sense terrorism has failed. It is a fundamental failure, ironically one recognized by early Marxist revolutionaries.

The paradox works on both sides. Despite their failure, terrorists persist in their struggles. Why? Are terrorists irrational or simply slow learners? Probably neither, but they are capable of self delusion. Professor Franco Ferracuti, a noted psychiatrist who has studied Italy's terrorists, suggests that terrorists wage fantasy wars. The presumption of war permits violence that would otherwise be unacceptable. It is, however, fantasy because the rest of society does not share the presumption.

In fact, cut off from most normal contacts with society, having only each other to talk to, terrorists live in a fantasy world. Their organizations are extravagant assertions. They imagine themselves to be armies and brigades. They believe themselves to have legions of supporters or potential supporters on whose behalf they claim to fight, but their constituencies, like their military formations, are largely imaginary.

Terrorists carry out operations they believe are likely to win widespread approval from these perceived constituents. But they do not always seem able to distinguish between a climate that is favorable to them because of what they do and a climate that just happens to be favorable to them. Terrorists, like the Weather Underground Organization, who were active during the height of the protests against the Vietnam War mistook anti-war sentiments for pro-revolutionary sentiments.

Terrorists fall prey to their own propaganda. They overestimate their own strength, their appeal, the weakness of their enemies, the imminence of victory. And they continue to fight, for to quit is not simply to admit defeat. It requires an admission of irrelevancy. It removes the justification for violence.

Some terrorists may be less concerned with progress toward distant goals, or the lack of it. It's not winning or losing, it's playing the game. They are action oriented rather than goal oriented. Terrorism becomes an end in itself, for some because living a dangerous life underground, oiling weapons, building bombs, endlessly planning and

occasionally carrying out acts of violence fulfill some inner psychological need; for others perhaps because membership in a terrorist organization gives them status and offers them opportunities for the continued application of criminal skills which they have developed as terrorists.

This suggests another reason why terrorist groups go on. Terrorist groups are collections of persons with otherwise unsalable skills. They have membership, hierarchy, management, specialized functions, a cash flow. Organizations are dedicated to survival. They do not voluntarily go out of business. Right now the immediate objective of many of the world's hard-pressed terrorist groups is the same as the immediate objective of many of the world's hard-pressed corporations, that is, to continue operations.

They may restructure themselves to do so. They may revise their goals. They may alter their operations. But they will struggle to stay in business. It is an organizational imperative.

In the process of long-term survival, some terrorist groups are changing their character. It costs a great deal of money to maintain a terrorist group. Terrorists who do not receive financial support from foreign patrons must earn it through bank robberies, ransom kidnappings, extortion, smuggling, participation in the narcotics traffic, all of which require criminal skills. Gradually, the criminal activities in support of terrorism become ends in themselves as terrorist groups come to resemble ordinary criminal organizations with a thin political veneer.

If the world's major terrorist groups sank into common criminality, the problem of terrorism might diminish, but the lack of progress and the methods necessary to achieve it remain issues within the terrorist ranks. As in war when neither side prevails, there is a tendency toward escalation, and we see evidence of escalation in terrorism. At the beginning of the 1970s, 80 percent of terrorist operations were directed against things, 20 percent against people. By the 1980s, approximately half of all terrorists attack were directed against people. Incidents with fatalities have increased by roughly 20 percent a year. Large-scale indiscriminate attacks like the bombing of the American embassy in Beirut have become more common. In 1982, six terrorist bombings

alone killed over 80 persons and injured more than 400. 1983 is likely to be the year of the car bomb; 5 car bombs this year have already killed 135 and injured nearly 600 persons. Civilian bystanders--those who just happen to be in the wrong place at the wrong time--are increasingly victims of terrorist operations, further evidence of growing indiscriminate violence.

There are several explanations why terrorism has grown bloodier. Terrorists have been brutalized by long struggles, the public numbed. Staying in the headlines in a world in which incidents of terrorism have become increasingly common and recovering the coercive power terrorists once exercised over governments who have since become more resistant, require acts of greater violence. Terrorists also have become more proficient; they can now build bigger bombs. At the same time, the composition of terrorist groups has changed as harder men have replaced the older generations of terrorists who debated the morality and utility of actions against selected individuals.

Although international terrorism has increased in volume, the patterns have remained steady. Terrorists operate with a very limited tactical repertoire. Bombings alone account for roughly half of all terrorist incidents. Six basic tactics comprise 95 percent of the total; bombings, assassinations, armed assaults, kidnappings, barricade and hostage situations, and hijackings. No terrorist group uses all of them.

The terrorists' tactical repertoire has changed little over time. Hijacking airliners and seizing embassies to make political demands are two significant terrorist inventions, along with kidnapping and leg-shooting. Some terrorist groups have experimented with other forms of attack but most groups stick to familiar tactics. Terrorists appear more imitative than innovative. New tactics, once they are introduced, are likely to be widely imitated.

One notable change has been the marked decline in barricade and hostage incidents. Seizing embassies and consulates and holding their occupants hostage became a popular terrorist tactic in the 1970s. Since the seizure of the American embassy in Teheran in November 1979, the use of the tactic has declined. Increased physical security has made it more difficult to seize government buildings. At the same time, the

odds against the terrorists having their demands met have decreased while the chances of being killed or captured have increased. There were 20 terrorist barricade and hostage situations in 1980, 10 in 1981, and six in 1982.

It seems a success story? A combination of better security, hardline policies, and greater willingness to use force have dissuaded terrorists from seizing embassies, but not from attacking diplomats. As embassy takeovers declined, assassinations and bombings increased. Overall, attacks on diplomats went up.

The point was made in the devastating bombing at the American embassy in Beirut in which 57 people were killed. Security of the embassy had been improved to prevent takeover by terrorists, the embassy had few defenses against several hundred pounds of explosives.

The dilemma is that terrorists can attack anything while governments cannot protect every conceivable target against every possible kind of attack. If embassies cannot be seized, embassies can be blown up. And if terrorists cannot blow up embassies they can blow up railroad stations, hotel lobbies, restaurants, or Horse Guard parades.

Just how far terrorists will escalate remains a matter of debate within the inner circles of terrorist leaders and conjecture by outside observers. We could see more of more of the same, no great change in tactics or targets, the continued ragged increase of terrorism as we know it today. Or we could see escalation in the form of increasing events of large-scale violence. At the far edge of plausibility are the scenarios that fascinate newspapers and novelists in which terrorists acquire and use or threaten to use chemical or nuclear weapons to hold cities hostage. Almost every terrorist group probably has contemplated the utility of violence on a larger scale. And, for the most part, they have rejected it. Unless we are talking about high technology terrorism, the constraints on terrorists are not technical but rather are self-imposed and political.

Occasionally intelligence sources, terrorist publications, or the testimony of defectors give us a glimmer of the arguments for and against such operations. The more moderate among the extremists argue that apart from being immoral, indiscriminate violence is

counterproductive. It alienates perceived constituents (even if they are largely imaginary), causes public revulsion, provokes extreme countermeasures that the organization might not survive, and exposes the operation and the organization itself to betrayal by terrorists who have no stomach for slaughter. Harder men and women counter that wars (even fantasy wars) are won by the ruthless application of violence.

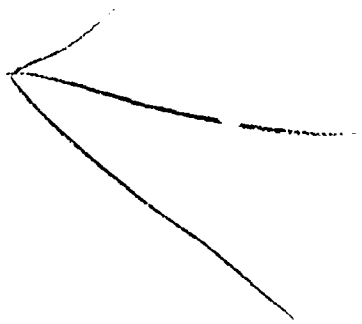
If recent bombings in London, Paris, Beirut, and Pretoria are any indication, the hardliners are prevailing. In hideouts of the Red Brigades, Italian police last year discovered a frightening terrorist plan to attack the Christian Democrats political convention--an operation that if realized would have resulted in the deaths of dozens of people. Smarting from their defeat and withdrawal from Beirut, PLO chief Yasir Arafat reportedly is under pressure from hardliners to abandon his current "moderate" course and permit the creation of a new Black September organization to wage a worldwide campaign of terrorism. The recent car bombing in Pretoria represents a new and likely to be bloodier phase in the struggle of African National Congress guerrillas against white rule in South Africa.

It is difficult to argue for constraint in an organization comprised of extremists who have already taken up arms, especially if things are not going well. Terrorists are by nature not easily disciplined. Terrorists with too many scruples drop out, are removed, or go along with hardliners to maintain their position of leadership.

Governments grow tougher and more efficient. Terrorists persist and grow more savage. And terrorism increases.

BRIAN MICHAEL JENKINS

Brian Jenkins has served as Director of Rand's Security and Subnational Conflict Program since its inception in 1979. He joined Rand as a consultant in 1968 while he was a member of the Long-Range Planning Task Group, MACV, Headquarters, Saigon. Since 1972, when he became a Rand employee, he has directed research projects on civil violence, international terrorism and other forms of low-level conflict that may threaten national security and international stability. In addition to directing this research at Rand, he has frequently been called upon by government agencies to consult on specific programs pertaining to intelligence, security measures, governmental organization, and policy.



# "SOCIAL PSYCHOLOGY OF SELECTIVE VIOLENCE IN SOCIETY: TERRORISM"

BY
DOUGLAS G. MACNAIR

AN ADDRESS PRESENTED BEFORE THE
8TH ANNUAL SYMPOSIUM ON THE ROLE
OF BEHAVIORAL SCIENCE IN PHYSICAL SECURITY

"CONFLICT AND CONFRONTATION IN SOCIETY"

SPONSORED BY
THE DEFENSE NUCLEAR AGENCY

AT
SPRINGFIELD, VIRGINIA

JUNE 7, 1983

A primary reason that selective violence - terrorism - remains a mystery is that those who orchestrate the strategy know about us. about our society, about our way of life, about how we think and what we believe, they know our frame of reference, our contradictions, our confusion, our vulnerabilities; in short, they know more about us than we know about ourselves. While we seem to have internalized little from Socrates' "Know Thyself," it seems apparent that terrorists have paid heed to an equally important axiom, "Know Thine Enemy."

We have a great capacity to be well read and informed but not necessarily knowledgeable. I am amazed each time I visit a bookstand with the proliferation of "Me, Me, Me" books selling like hotcakes and making their respective authors wealthy. Their theme is all too familiar. "My diet; You too can do it; Get rich like I did." To quote the title of Dr. Wayne Dyer's book, "The Sky Is The Limit." The various cults abound as do their devotees.

There is an array of evidence that suggests we are more self-oriented today than ever before; at the same time, we may know less about what is happening than anytime in history. Have you taken notice of the dexterity with which individuals project blame for error, when self is threatened by error or mistake, to the nearest thing available, other than themselves? When was the last time your mechanic said, "It's my fault; I didn't fix it." And while the tendency to project responsibility for fault has always been a part of human kind, I would submit never on the order of magnitude found today. Nothing is ever anybody's fault. The essence of the dilemma faced by management may well be that nobody is responsible for anything.

To a great degree you and I are the products of hundreds of thousands of stimuli bombarding us since early childhood -- a bombardment with the precise effect of shaping the tastes, attitudes and values we hold today. It is this hierarchy of the value system that comprises the little discussed nor fully understood affective domain of the mind. I suggest change has been at work.

Ariel Merari was recently quoted as saying, "If terrorism stops terrorizing -- if it ceases to have an explosive impact on public opinion -- then terrorists have an innate tendency to escalate in order to recapture headlines." I agree. But, the day I read this I could not help but ponder the notional reversal to this statement. Suppose for just a moment that terrorists know that when their acts fail to capture headlines, the balance theory of acceptable behavior has been altered and they are free to intensify the violence of their deeds. Remember the old joke from the psychology lab? One rat said to the other, as he saw his researcher approaching, "I've got this guy well trained. Everytime I turn right at the end of the maze, he has to give me a jelly bean."

I believe in the hierarchy of tastes, attitudes and values. Tastes are shallow and the easiest to alter; attitudes are deeper and more difficult to sway; values are deep and changed only by altering the more shallow parts of the hierarchy and then over some extended period of time. Have yours and mine

been altered? The absolute answer is -- Yes! But, the degree of change is extremely difficult to gauge. The old argument that we hold certain universal values - constant values shared commonly and to the same degree by all people - was disproved. Neither power nor wealth could withstand the test. Just as tastes and attitudes are ever changing and vary among people, values are too. Change a person's value system and you change his behavior.

How change is brought about is an interesting phenomenon. It can result from either a random number of stimuli received by the individual through happenstance or it can be achieved through a cognitively developed methodology where control is exercised over the stimuli to which the individual is exposed. Understand, of course, that perfect control can never be achieved. Stray inputs will always occur. The world of advertising is all too familiar with this facet of psychology. In fact, it is their bread and butter. Some do better than others; but, all have some effect. But, the most fascinating aspect in advertising must be the willingness we evidence to cognitively allow mind play in shaping our tastes, attitudes and values. We know what they are doing. Each day in our lives is an interesting snapshot in time. We allow our minds to be focused hundreds of times between dawn and dusk. We read papers; we watch television; we listen to radio. Our awareness is peaked on the thrust of today. Peaks and valleys occur as the days change one to next; but always left in the passage of each is some small residue that awaits reinforcement or refutation. Tastes can change; attitudes can alter; values may sway.

For just a moment, I would like to take you back two decades to this same time in the year 1963. Remember? Vietnam was a place no one had heard much about. We had finished putting Cuba and the Soviet Union in their place. President Kennedy was alive and well. And narcotics? Narcotics were evil. Assuming a legal search and seizure, a trooper caught with an ounce of marijuana was all but guaranteed of being sent to the slammer, a convicted felon.

Here we are in 1983. Without dwelling on the other three issues then current, the war on drugs goes on. While we may share the same tastes, attitudes and values we did twenty years ago, the size of the drug market clearly indicates that a "whole bunch" of people do not. Apparently they "like" drugs. In fact, the balance theory of acceptable/unacceptable behavior has been drastically altered.

As those same twenty years passed, much was written about the decline of our social foundation -- the church, the home, the family -- and the resultant effect. Similarly, books like The Ugly American, Street Without Joy, Future Shock, and A Nation of Strangers came and went, their apparent implications missed by the multitude. Instead we witnessed an amazing phenomenon, the emergence of the "single interest" group as a means of accelerating change. In far too many instances, change seemed to serve the sake of the individual and not that of the nation, at least in my view. Were we growing apart of together? There is, of course, some good or bad to almost any change wrought by man; but, whether good or bad is not the issue. The issue is simply that many of our former assumptions, our

constructs, about society may now be invalid. Many of us tend to be fixated day-to-day on specific tasks or problems as opposed to interrelationships. Most frequently our jobs require focused thought. I know, for example, that this nation has undergone drastic social and psychological changes in only twenty years. That is cognitive thought, easy to grasp and support with fact. But, what about the true meaning of these words? What are their implications?

In preparing for these remarks, I gave this issue a great deal of thought. I had to, simply because social psychology is all about interrelationships between the individual and the group; about membership and reference groups; about formal and informal power; about structure, anchorages, value systems and change. The example I chose was that "group" we often refer to as the "silent majority." I set to paper those tidbits I would attribute to this value system. A subsequent sampling of a few people through discussion and open-end interview leads me to speculate that the silent majority has either undergone change or they do not really exist.

I found attitudes and values I did not anticipate. On narcotics I heard such things as: "Drugs aren't too bad; maybe heroin is, but not Marijuana or Coke."; "The drug war is a waste of time: nobody goes to jail anyway."; "It's sort of like prohibition, we ought to make it legal and tax it. If you want to use it, pay for it."; "If being a homo is O.K., so are drugs."; "Most people use it, they just don't say they do." And on terrorism: "Terrorism is here to stay; there's nothing we can do about it."; "A lot of it is our fault; we always back the wrong guy."; "It's too bad; but, that's the way things are." On the embassy in Beirut one said, "I don't see how we can act surprised; we're pretty dumb; we ask for it and we get it." Another commented, "Those guys (in Washington) can't get their act together; they just do the same thing over and over again." One even said, "I find it interesting; the boob tube makes it a program that beats all of the other stuff that's on; it's interesting."

I guess that statement is true; through the medium of TV, a terrorist event is sort of like being seated at the arena to witness the latest spectacle of the Lions vs. the Christians. After all, we can always hope the Christians will get in a lick or two.

I conclude that terrorism is now an acceptable form of behavior, as long as the acts are not too outrageous. To paraphrase Starkist, the only caveat seems to be, "We want terrorists in good taste, not terrorists who taste good." Good taste in this context relates to such things as nuclear terrorism. From the responses elicited, it seems that balance theory has not yet had time to make this form of terrorist behavior even moderately acceptable. Nuclear terrorism is going too far; it would not be in good taste. In fact, I would hazard that such an act would constitute a blunder on the highest order of magnitude analogous only to Napoleon's Waterloo or Hitler's opening of the Eastern Front.

Interestingly enough, not one person interviewed felt "touched" by terrorism. What they seemed to be transmitting sounded remarkably like, "If I don't

bother them, they won't bother me." When the issue of attacks on U.S. businesses abroad was mentioned, responses varied: "That's our government's fault."; "They probably are meddling around."; They shouldn't do business over there." Psychologically, the use of the word "they" and not "we" is extremely interesting. It indicates a total separation in self identification with the membership group to which they obviously belong. All the persons interviewed represent business and, beyond that, management. They are mature, educated, traveled, and at least moderately intelligent; they go to church, raise children, and are, to some degree, affluent. All admit they have changed in some way.

Each of us belong to a wide array of membership groups. Some are recognized entities such as our agency, company, or, for that matter, an association. Others may be more generic or vague, such as those relating to our speciality or avocation. We may or may not have much in common with other group members. We usually join a membership group because it is something we have to, want to, or should do.

Reference groups are different. We belong to a reference group because of some inner drive or commitment. What moves the group moves us. We believe in our reference groups -- both the bitter and the sweet. We join because we "need" to. In a reference group you never hear the word "they," only "we." The notion of ideas is important; after all, everbody should have at least one or two.

The interplay betwen individuals and groups grows in significance. My reference group - my life if you will - may be your membership group. What affects the group and, by definition, me, may not touch you at all. As an example I offer the words, "Duty, Honor, Country." Internalized by some, they represent a reference group in which many take pride; to others they are merely words representative of a group in which they hold membership. And, of course, there are those who could not care one way or the other -- who find the words meaningless.

Our environment is complex. To describe it accurately is difficult. I frequently use the Organizational Systems Model as a means of communication because the major variables can be lumped in four convenient groupings. Man's environment is nothing more than an organization: whether the world, nation, agency, or company makes little difference.

- There is structure - everyone accountable to someone - to provide stability.
- There is technology - man's developments - to provide livelihood and further growth.
- There is society - interrelationships between man and his fellows - where he works and resides.

- There are goals and values - man's mechnanism for self motivation - that Maslow contended were dependent on a hierarchy of needs.

Superimposed over these four intertwined and interdependent subsystems is management - the method and process through which we exercise control over the environment and this thing we call civilization.

From a social psychological frame of reference, I believe this model is useful in viewing terrorism. As most of you may know, I contend that terrorism is both a process and an adjunct to strategy as opposed to a tactic. Terrorism is a form of war, using many things as its tools and tactics: murder, extortion, piracy, arson, assassination are but a few.

Having long argued this position, I am pleased to see others now voicing this opinion. Hopefully this insight, this perception, will spread, enabling the formulation of an anti-terrorist strategy capable of stopping what has been called, "A Spreading Disease." (U.S. News and World Report, May 16, 1983.)

As a process and a strategy, terrorism is of the offense and not the defense. Terrorism is an attack on our environment. It is an extension of power, free to adopt all of the tools in man's array ranging from rhetoric to the threat or commission of abhorrent acts. It is a strategy designed to dominate and direct the actions and choice by nullifying the will of those who constitute the target. It is a strategy designed to insidiously and incrementally alter or change behavior.

If this thesis is accepted, then reflective thought will show that we have done a good job in countering but two of the four subsystems offered in the Organizational Systems Model. We have countered in both structure and technology. The state of the art today deals with "things" that, for the most, are tangibly related to both: executive protection; site hardening; historical analysis; intelligence gathering on terrorist groups, their organization, methods of operation and intentions; innovative hardware; and hostage negotiations. Left effectively unanswered is the terrorist challenge in the remaining two arenas of our environment: the psychosocial and the goals and values subsystems. Less tangible because they relate to the inner nature of man, they nevertheless are critical to success or failure. If the model is valid, management's answer - management being the government of the United States - must appreciate and account for this void.

Is the notion of membership and reference groups important? Are attitudes and values critical to our vulnerability? I believe they are. After all, the bombing attack in Beirut attacked someone's reference group. This point hit home when I read The Wall Street Journal, April 21, 1983.

> ". . . perhaps even more troubling is the psychological impact of such acts as this week's bombing of the Beirut Embassy or the 1979 seizure of the U.S. Embassy in Iran. U.S. officials fear that such attacks can

induce diplomats and their families to shy away from or leave assignments in high-risk areas."

Hopefully, as The Great Seal of the United States reflects, "God has smiled on our undertakings." The "green back" of our one dollar bill depicts the great pyramid that stands as our society. The foundation - our goals and ideals - is the building blocks that were carefully laid by our forefathers and their childrens' children. The top of the pyramid - management - is the home of wisdom; the ability to see with clarity pressures from without, the place of cognition. Upon these precepts our nation depends. Without them, erosion will occur; the structure will crumble.

I suggest that the time is at hand to re-examine terrorism from the aspect of the behavioral sciences widely applying known techniques to both the cause and the effect. I suggest that we focus on the process of terrorism rather than the products or events. I suggest in this more generic application of the disciplines, we may develop the insight to a strategy that effectively meets the challenge. The mandates of such a strategy may be axiomatic to those precepts of Organizational Development.

- Long term
- Systematic effort
- Include whole organization
- Manage change
- Specified outcomes

Regardless of the model, Organizational Development or others used in combating terrorism, let there be no doubt that the strategy must include consideration of the psychological dimension of social behavior.

If the selective violence we face is founded in an offensive strategy, then an appropriate counter-strategy is required. A counter-strategy that is also offensive. A counter-strategy that first reaffirms our society's value system and highlights the advantages and responsibilities inherent in our republican form of democracy. A counter-strategy that projects our values and seeks to influence the psychological subsystem of those emerging political entities that are seeking constructive change.

In reviewing the transcripts of the 1982 hearings before the Senate Subcommittee on Security and Terrorism, it was interesting to note that in all the Eastern block's insurgency training camps, whether in Russia, Libya, Angola, or Cuba, the focus upon forming a Marxist - Leninist value system was uniformly consistent. The Eastern block appears to appreciate the need for establishing common values.

I cannot help but wonder if we have lost sight of our national need to educate our citizens concerning our fundamental values. In our desire to

train our youth in technical disciplines, have we bypassed the need for education -- for reaffirming our national values? What implications can be derived from a statistic which depicts a decline in liberal arts degrees from 20.4 percent of all college graduates in 1966 to 7.4 percent of the 1981 graduating classes? Where are our trained specialists going to attain an orientation to our national values -- in their trade journals, from their narrow reference groups, from the "Me, Me" "How to" best sellers?

I would submit that there is a crucial need for our behavioral scientists to recognize the requirement for their input into an emerging national counter-terrorism strategy. To take the lead in developing a program that will, at least, expose our citizens to the fundamentals of our national value system. The challenge is ours.

Admittedly, we are an open society; but, this should be our strength, not our weakness. The problem transcends political boundaries, administrations, agencies of government and the differences between government and industry. It is, in fact, a problem to be shared through the whole organization, which in this context is the entire nation. History shows we can achieve any goal that we as a people care to achieve. But, we must be of one mind, one purpose, and most important -- committed.

## ABOUT THE AUTHOR

Colonel Macnair is a graduate of the Naval War College and the Army's Command and General Staff College, where he also served on the faculty. His diversified career has included assignments ranging the spectrum of command and staff, with occupational interests in strategy, strategic mobility, counter-terrorism, and intelligence. He is currently affiliated with a multinational corporation.

# EVOLUTION OF BEHAVIORAL SCIENCE IN SECURITY MANAGEMENT

by

RICHARD J. HEALY, CPP
President
Professional Protection Enterprises, Inc.
Suite 30, 4401 Atlantic Avenue
Long Beach, California 90807

Prepared for presentation at the 8th
Annual Defense Nuclear Agency Behavioral
Science Symposium--"Conflict and Confrontation
in a Civilized Society".

Springfield Inn
Springfield, Virginia

7-8 June 1983

## EVOLUTION OF BEHAVIORAL SCIENCE IN SECURITY MANAGEMENT*

Next to his life and the lives of loved ones, man has valued his property through out history. Many techniques have been developed over the centuries to protect property against invaders or aggressors who threatened to take or destroy it. As the factories and the use of hired labor expanded during the Industrial Revolution, protective efforts developed from simple, individual, proprietary practices to more organized programs by larger employers. As a result, watchmen or guards, who were considered "private police", were hired and dressed in uniforms similiar to those worn by municipal police. They were also provided with similiar equipment and were expected to discourage crime, particulary theft, on the protected premises. The use of guards or watchmen generally represented the only security effort.

As such security programs were usually patterned after law enforcement operations, their effectiveness depended to a great extent on the psychological impact made by the watchmen or guards. Uniforms, badges, guns and other such tokens of authority were used to promote the enforcement image and the uniformed personnel typically carried out police-type duties. Following commonly accepted police practice at that time, the uniformed personnel were organized and trained to react only after an incident had occurred. Prevention or avoidance was not the objective and the focus, instead, was on investigations, apprehension and other police related activities. Further, there was a tendency of management to often regard the uniformed security activity as a low grade, unimportant activity in the organizational structure.

Personnel in security organizations of this type had a tendency to view everyone with suspicion and they usually dominated those with whom they came in contact. There was also a tendency to disregard the rights of individuals; the personnel in the protection organization were at times discourteous, arbitrary, arrogant, and even stupid in their handling of individuals and their problems. This type of protection organization represented protection in and by itself in the enterprise and could best be characterized as "carrying a big stick." As a result, individuals who came in contact with such an organization had a tendency to view it with hostility, fear, and distrust. This type of protection organization usually operated as a mysterious entity, generally in what might best be described as a vacuum, and attempted to give the appearance that it had authority. In reality, an organization of this type did not have any authority and was really not effective in protecting the assets and personnel of the enterprise, because the impact of the operation was limited to the psychological effect it had on people and depended on fear alone to motivate results.

* The information in this discussion has been extracted from the Protection of Assets Manual by Timothy J. Walsh and Richard J. Healy and published and copyrighted by The Merritt Company, Santa Monica, CA

Security over the years developed a poor image because of the conduct of personnel in security organizations and because of many examples reported internationally in the news media of a disregard for human rights in the name of security involving electronic surveillance, spying on individuals and the improper use of money and sex. The distasteful and clumsy conduct of those involved in the Watergate incident identified as security personnel is just one example. Going back further in history, the abuses perpetrated by the late Senator Joseph McCarthy in the early 1950's under the guise of security are generally recalled as a national disgrace.* The publicized poor performance of contract guards has also made an unfavorable contribution.** As a result, it can generally be concluded that the poor image of security that had developed over the years resulted in large measure because of a past disregard for human relationships and for the rights of individuals.

## FACTORS INFLUENCING HUMAN RELATIONSHIPS

The situation changed in recent years because top management in progressive enterprises began to recognize that security programs based on the uniformed security operation were not effective. It was recognized that the constantly changing fabric of society required that human relationships, modern management techniques and behavioral science concepts had to be given emphasis in the development and implementation of effective security programs. Also, that there was a need to give attention to loss prevention or the avoidance of problems. Some of the more significant factors that motivated this change in management thinking are discussed in the paragraphs to follow.

### The Knowledge Worker

Peter Drucker utilized the designation "knowledge worker" to describe a new breed of worker who is more skilled and educated because of automation and new technology.*** According to Mr. Drucker, this type of worker now dominates the work force instead of the less skilled and poorly educated manual worker who previously made up the bulk of the work force. According to Mr. Drucker, "For the weapon of fear -- fear of economic suffering, fear of job security, physical fear of company guards or the states police power -- which for so long substituted for managing manual work and the manual worker, is simply not operative at all in the context of knowledge work and knowledge worker. The knowledge worker, except on the very lowest of levels of knowledge work, is not productive under the spur of fear; only self-motivation and self-direction can make him productive. He has to be achieving to produce at all."

* Thomas C. Reeves, "The Life and Times of Joe McCarthy." Briarcliff Manor, New York: Stein and Day, Scarborough House, 1982.

** For a discussion of contract guards, please see James S. Kakalik and Sorrell Wildhorn, a study of private police in five volumes. Santa Monica, California: The Rand Corporation, 1971.

***Peter F. Drucker, Management: Tasks, Responsibilities, Practices. New York: Harper and Row, 1974, pp. 30 and 176-179.

Because of the change in the characteristics of the present day worker described by Mr. Drucker, the development and management of an effective assets program is now more difficult and requires more imagination, innovativeness, and a real appreciation for a more humane approach. Even with the manual worker it might be questioned as to whether an authoritarian type of protection program operated on the basis of fear was ever effective. A clever worker might display the proper servile attitude expected of him while taking advantage of the situation by developing a means of circumventing the protective controls designed mainly to insure his compliance through fear.

The knowledge worker will be just as quick to understand that an authoritarian program is neither realistic nor effective. The only difference between the manual worker and the knowledge worker is that more of the latter will probably discover the deficiencies of the program. Those who do not conspire to circumvent it for their own benefit may react negatively toward the enterprise for allowing such a condition to exist. The result could be that the morale of the entire work force might be adversely influenced. A large enough loss of assets can certainly destroy an organization, but an enterprise may be destroyed just as quickly because of the reactions a demoralized work force may have toward a poor protection program not geared to the needs of the present day worker.

## The New Generation

Another area that requires attention and understanding is what has been described as the "now generation." Management executives at all levels, including those in the protection organization, are being confronted by young men and women who are becoming an ever-increasing proportion of the work force. As a result, it is becoming essential that every effort be made to bridge the generation gap so that the members of this current work force can be understood and dealt with on an intelligent level.

Unlike workers of past generations, this new breed of worker is not willing to accept requirements that appear to be arbitrary or those that do not seem to be reasonable. Also, they are unwilling to accept incomplete answers to questions but will have a tendency to question every restraint, and demand full explanations as to the need for certain protection requirements. In short, they can be expected to reject an authoritarian type of protection program and will not be motivated by fear.

In attempting to understand this new generation, it may be helpful to remind ourselves that many elements of the lifestyle now regarded as new are really as old as the history of civilization. Some examples may serve to illustrate this. Long hair and beards for men were traditional in earlier times; drugs have been utilized as long as history has been recorded; belief in nonviolence was an early basic Christian doctrine; young people throughout history have rejected what they have regarded as arbitrary authority; and they have over the years proclaimed that individuals should be guided by their own individual ethical standards.

It cannot be assumed that freedom of sexual expression, long hair, beards, beads, tattered or well-worn casual clothing, bizarre accessories, a lack of cleanliness, or any of the other elements discussed above will adversely influence work performance.

It may be natural for security personnel to overreact when confronted with the uninhibited behavior of this new generation of worker or reject them as "kooks." Those who adopt such an attitude and attempt to administer an authoritarian type of protection program while refusing to understand the needs of the new generation may find they are constantly having problems with the work force in the enterprise because they are out of step with current requirements.

## Women Workers

The impact of the ever-increasing number of women entering the work force at all levels must also be considered. Until relatively recent times, women employees were either temporary--working until they could get married--or those performing permanent but what might be described as menial tasks in the organization. Wives of those who were defined as being in the middle or upper economic classes usually did not work outside of the home.

This situation is now changing drastically as more and more college-educated wives from middle class families are now career oriented and are beginning to compete with men for more responsible positions. This is now possible because family sizes are limited and housework is easier to complete because of the availability of labor saving appliances. Although women's liberation may be a factor in this evolution, the more driving forces probably are economic, social, and psychological. The efforts of the federal government taken to insure equal opportunity for women have also most certainly been a big factor.

Security personnel must realize that the movement for equal rights and the influence women are having on every organization at all levels is real, and that they must give consideration to this relatively new development while planning a protection program. The movement cannot be dismissed as only a reflection of women's liberation--often characterized by the "braless look" practiced by a limited number and by exaggerated demands made by small militant groups. The women's liberation movement, of course, is also real; and, although it is a small part of the overall movement of women to enter the work force, it must also be given consideration in any protection plan.

## Minorities

Another relationship problem requiring attention involves the constantly increasing number of minority employees entering the work force. Individuals in this group range from the highly intelligent college-educated to the illiterate. Because jobs are regarded today as a significant factor in the rehabilitation of socially maladjusted individuals, minority workers--many of whom are defined as the hard-core unemployable who have no skills and have criminal records--may be encountered in increasingly large numbers. These workers, because they generally lack a feeling of social responsibility, cannot

be dealt with in the same way as the more educated minority employee.

Many minority workers will not be motivated by fear because they have had a lifelong experience with discrimination and law enforcement official harassment. They will have learned to disregard any fear-producing motivation. Consequently, an authoritarian type of protection program will usually not be effective in dealing with this class of worker. Also, the minority employee may have a tendency to be angry because of the mistreatment experienced in the past. As a result, any violation of rights or any mishandling of incidents by representatives of the protection organization may result in violence. A strike, work stoppage, or riot could easily be the result.

### Automation and Computers

Automation and computers, as well as data processing, can be utilized in security programs to improve protection and reduce costs. However, the need for personal relationship between the security organization and those affected by automation and computer techniques must not be overlooked. Unless consideration is given to this element, personnel interfacing with the protection organization may begin to regard it as an impersonal machine. For instance, it is a common experience for an individual to have a problem with a bill or record resulting from a computer error. An exasperating experience usually follows as an attempt is made to have the necessary correction made. When an individual is finally found with whom the problem can be discussed, the usual explanation for the error is that it is the computer's fault. Such an answer is no longer acceptable to most people because the average person now knows enough about computers to understand that the computer is only a machine that does what it is told and that any error was therefore created by a human being.

As a result, it must be recognized that many people dislike automation and computers because computer-using organizations with which they have dealt have appeared to them to be machine-like, faceless monsters. People resent having their lives controlled by impersonal machines. However, the use of automation and computers should not be avoided for this reason. Instead, the problem of relationships with users should be recognized and compensated for.

### Alcohol and Drugs

The new generation of workers already discussed in this section has created what is regarded as a serious and growing problem area--alcoholism and drug addiction. Since the alcoholic and the drug addict represent a serious threat to the safety and security of the enterprise, protection executives must give serious attention to this problem area and be prepared to deal with it. Since human relationships are extremely important in dealing with this area, it is mentioned here as one additional item that should be considered.

## APPLICATION OF CONCEPTS--THE SYSTEMS APPROACH

The discussion up to this point has involved a general outline discussion of concepts relating to human relationships and some problem areas that should be given attention in the implementation and management of a security program.

Two questions that might be asked now are, "How can the concepts mentioned be applied in a practical manner and how can the problems mentioned be overcome?" One method of applying the principles outlined to insure that a complete, effective security program is adopted is to utilize the systems approach. The systems approach has been defined as "a comprehensive solution to a total problem." It is an orderly and rational method of problem solving. The following are three general steps in the implementation of the systems approach: (1) a vulnerability analysis, (2) installation of countermeasures, and (3) a test of the operating program to insure its effectiveness. As the next presentation will deal with the first step, vulnerability analysis, it will not be discussed further here.

Countermeasures

Countermeasures can be divided into the following three general catagories: software, people, and hardware. All three must be interrelated in the system design to insure an effective, integrated protection program.

Software-- The term software arrived with the electronic processing age and was originally used to describe instructions in the form of programming needed to make computers perform. For the purpose of this discussion, the term will refer to all directives and instructional or training material, written as well as verbal, needed to make an assets protection program operate effectively and efficiently.

A basic software item needed in the development of a protection system is a policy statement issued by the top management of the enterprise establishing the assets protection program. That statement, as well as other policy statements that may be issued, is important because it will set the tone of the complete program, will indicate the interest of top management, and will be the basis for detailed implementing material.

Software material issued to implement policies, such as procedures, practices, and directives, will usually define in detail the controls that are being established throughout the enterprise, as well as the responsibilities all employees must assume. Such material should be designed so that it can be easily understood and followed by employees at all levels in the organization. It will usually not be adequate simply to issue directives or procedures and expect them to be followed without further explanation.

The material should take into consideration that all employees in the organization must participate and assist in the program to make it operate. Also, it should be stressed with supervisors at all levels that they must insure the compliance of all employees under their supervision. The cooperation and assistance of employees is necessary, because employees assigned to the protection organization, regardless of the number, cannot protect the enterprise alone. They need the cooperation and assistance of all other employees. Therefore, general employee reaction and attitude are important.

If it is to be effective, any protection program will necessarily control and limit people and their activities. A natural antagonism may develop if the program is not implemented properly. Employees will naturally resent controls that seem arbitrary. However, if the need for controls and the method of operation of the protection program are reasonably explained, most employees will accept the program and will help to make it work.

For these reasons, an educational program, as one software element, will effectively counter resistance and enhance cooperation. For example, employees are often not aware that losses must be deducted directly from the profits of the organization. Also, losses that might at first appear to be very small could have far-reaching effects on the profitability of the enterprise and might even have an adverse effect on employees. Employees can be informed that prevention of a loss will avoid decrease in net profit, and that the success of the organization, largely measured in profit, will insure personal security for them in terms of employment and a better future.

Methods of dealing with employees who violate or ignore procedures need also to be established. Violation of an assets protection practice should be handled in the same way that the infraction of any other major company rule is handled. The problem should be referred to the appropriate level of supervision for corrective action. As a part of the educational program, employees and supervisors should be informed of the standards and procedures that have been established for handling instances of non-conformance.

A different type of educational software, but equally important, is training material for those employees and supervisors who operate the protection organization, such as uniformed security officers, investigators, and clerks. Once procedures or practices for use within the protection organization are developed, arrangements should be made to give the protection employees appropriate instruction so they are familiar with the detailed operation of the program.

People--The use of people was the second element listed earlier under countermeasures. The effective use of personnel assigned to the protection unit is important, because manpower is normally the most costly item in any protection program. During the system design, particular attention should be given to the substitution of software and hardware for people wherever possible.

Protection system personnel may be employees of the enterprise or contract employees or a combination of both. Organizations of sufficient size will normally assign to a full-time executive the responsibility for the administration of the program. The executive will usually have a sufficient number of employees to administer the program. In addition, contract personnel, such as guards, may be used. Smaller organizations, not able to afford a full-time executive for the protection function, may rely upon other employees to administer the program on a part-time or added-duty basis. In such situations contract personnel may be utilized extensively.

A program to orient and educate the workers in the enterprise will be of little value if the members of the protection organization do not practice what is being advertised. As a result, a training program in which human relations concepts are stressed should be designed and presented to the protection staff. Such a program should train members of the protection organization to conduct themselves in such a way as to insure that an environment is provided which will stimulate the cooperation of all those with whom they come in contact.

Hardware--Some examples of hardware items, the third element listed under countermeasures, are locks, fencing, bars, and screens to protect openings, safes, vaults, lights, turnstiles, and electronic devices. When properly utilized, these can make a significant contribution to the protection of a facility. As with the other two countermeasures categories, software and people, each item of hardware must be carefully planned to insure that it interrelates with the system and economically increases the protection of the facility.

A lock, for instance, is traditionally regarded as an effective security measure. However, it could be a mistake to install a lock expecting it to provide complete protection. A door or barrier secured by a lock can be penetrated in a wide variety of ways. To make a lock effective, procedures should be established defining how and when it is to be used, arranging for a periodic inspection by a guard or other individual, and providing for an alarm detector and adequate response in case of a penetration. So planned, all three countermeasure categories are involved. A lock is the hardware element. Software is represented by procedures providing for the activation, inspection, and response to an alarm. And the third element--people--is required to inspect and respond in case a penetration is signaled.

Electronic detectors and components can also be utilized effectively to raise the level of protection and reduce costs at the same time. They may be used for a variety of command and control functions involving security, fire, safety, and utilities.

## The System Test

A test of the operating program is the essential third step in the system implementation for two reasons. First, risks or hazards still existing will be identified, and system deficiencies will be revealed. Second, system changes required to accommodate facility or organization revisions will become apparent. Checks or tests can be performed by the regular work force as part of their normal work assignments, as well as by the special employees operating the protection system. Arrangements should be made to test the system frequently.

Regular employees can be asked to make suggestions for the improvement of the protection program. Usually they will respond positively if the education program mentioned earlier is effective. Employees' comments and suggestions

will give some indication of how well the protection system is operating and what changes, if any, should be made. Procedures can be established requiring supervisors at all levels to make regular checks to insure that employees are complying with system requirements. Supervisory personnel can also be prepared to perform other tasks, such as inspections of areas and periodic audits of invoices, negotiable instruments, and so forth, and to report any discrepancies to the executive responsible for the operation of the system. All members of the protection organization can be required to be constantly alert to any deficiencies in the system operation. In addition, they can be assigned specific inspection responsibilities to be performed periodically.

Errors can be purposely inserted into the system to determine if they are noted and reported. Test exercises can also be designed and conducted to determine how the system reacts. For example, a controlled test might involve the report of a bomb in the facility to check the reaction of everyone responsible for taking action in such a situation. Of course, such exercises must be carefully supervised by trained personnel so that undesirable reactions and results are prevented.

## BIOGRAPHICAL SKETCH--RICHARD J. HEALY

Richard J. Healy, CPP, is President of Professional Protection Enterprises, Inc., Long Beach, California. He previously was Director of Security and Safety at The Aerospace Corporation in Los Angeles.

Certified as a Protection Professional (CPP) by the American Society for Industrial Security, Mr. Healy has an international reputation as a consultant, writer, lecturer, and administrator in the security field. He is also listed in the current issue of Who's Who in The West.

Born and raised in Iowa, Mr. Healy received his B.A. from the University of Iowa and attended law school at the University of Maryland.

He served in the European Theater of Operations during World War II as an Intelligence and Tank Officer in General Patton's Third Army. After 5½ years in the army, he was released as a major and joined the FBI as a special agent. He served in Washington, Dallas, Cincinnati, and Dayton in the FBI and later served as assistant to the Inspector General, Air Research and Development Command (now Air Force Systems Command, U.S. Air Force).

Mr. Healy is a charter member and past president of the American Society for Industrial Security, he is active in the Society of Former Special Agents of the FBI, and the National Panel of Arbitrators of the American Arbitration Association. He has chaired and participated in workshops and seminars for a number of professional organizations as well as for colleges and universities in the United States as well as abroad.

Mr. Healy has written two books published by John Wiley & Sons, Inc., New York--"Design for Security" and "Emergency and Disaster Planning." He is also the coauthor of "Protecting Your Business Against Espionage," published by the American Management Association, New York, "Principles of Security Management," published by Professional Publications, Long Beach, California, and a handbook entitled, "Protection of Assets Manual," published by the Merritt Company, Santa Monica, California.

# SECURITY VULNERABILITY

# and SECURITY AWARENESS

A presentation to the 8th Annual Defense Nuclear Agency Behavioural Science Symposium.

June 7 and 8, 1983

by: Dr. Timothy J. Walsh, CPP

# SECURITY VULNERABILITY

## - AND - SECURITY AWARENESS *

### INTRODUCTION

The preceding Chapter addresses itself to training in its many forms. There and elsewhere in the *Manual* repeated reference has been made to a need for "education," "training," and "knowledge of the program" on the part of senior management, workers in general, and members of the security organization. Although the term "education" can be said to suggest a somewhat formal and generalized instruction in the broad area of assets protection, and the term "training" to suggest more particularized attention to acquisition of specific skills or behaviors in regard to the security program, there is still a third concept of critical importance, which is a companion idea to education and training. This third concept is "Awareness."

"Awareness" can be defined as a state of mind or attitude through which the individual is conscious of the existence of the security program, and is persuaded that the program is relevant in one or more ways to his own behavior.

Awareness, then, is a condition precedent to training or education. One must know there is a program before learning specific skills or acquiring particular behavioral patterns in support of it. More important, awareness is a **continuing state**, a prime result of which is the sustained attention of a variety of persons to the assets protection needs of the enterprise. This latter quality of awareness is of signal importance to the ultimate success of the security effort. It might appear self-evident that awareness of a thing is necessary before any intentional conduct in regard to it is possible, but there is ample evidence that surprising numbers of protection professionals neither make useful attempts to determine or measure such awareness as might exist nor do much to establish or extend it. Even in those situations where appreciation of the importance of awareness is apparent, there is often a lack of sustained effort at maintaining it.

Awareness, as we have defined it, is a state of mind and, as with all states of mind, is subject to displacement on an occasional or even permanent basis by the more urgent demands of other stimuli. Yet, if key populations are **unaware** of the security program, or only aware of it in an obscure or hazy way, the likely consequences are program failure for lack of resourcing or lack of participation, or both, depending upon which population group lacks the awareness.

The purposes of this Chapter are: 1) to distinguish security awareness from the more specific concepts of security training and security education; 2) to indicate identifiable groups who must develop and maintain some form of security awareness; 3) to point out at least seven reasons why security awareness must be developed; 4) to outline some techniques with which to achieve and maintain awareness; and 5) to suggest some resources to assist in this important task.

## SECURITY AWARENESS AT VARIOUS LEVELS

Because the security program will have different impacts upon the different functional groups within any enterprise, and because it will require different responses from them, it is relevant to inquire whether awareness is a single concept, the same for everyone, or whether it is dynamic and variable, stressing different characteristics for different groups.

Certainly the **program** itself is the same. That is, if there is a requirement that all persons entering a facility first establish their personal identity, that requirement is a given and does not change. Similarly, if there is a requirement that known or suspected asset losses of a defined type and dollar limit are to be reported in a standard format, the requirement does not change just because it is considered by different persons having a reporting responsibility. However, there is a real relationship between specific, objective program elements and the way in which particular persons will see or be aware of them. Awareness is in part the result of the thing or condition outside the one aware (the environment) and in part the result of the mind-set of the one aware. As will be seen from later comments, much difficulty arising from hostile or disapproving mind-set can be avoided by the style in which the thing required or the security environment is established. But, however established, it is inevitable that the program and its elements will be perceived differently because the status or position of the perceivers varies.

Chapter 23 took notice of the differences among enterprise management, the general employee population and the specific personnel of the security organization in regard to motivation and response. Actually, there are several more specifically different groups whose attention must be secured, and in whom awareness of the security program is necessary. Each group, in itself, will have many variations and its members will by no means be of one mind in their attitudes. However, because the responses desired from these groups generally are the same for all the members of the group, it is useful to consider how best to address the group (no program can deal with all the individual varieties of perception).

## THE SENIOR MANAGEMENT

This group consists of the ultimate decision makers in the enterprise. It will include the Chief Executive and Chief Operating Officers and the most senior personnel in other activities, both staff and line. Such persons often have a group role as members of a Management Committee. Senior management are the risk decision makers for the enterprise and it is they who must be aware of the security program in that light. Among the many competing claims for a share of the enterprise resource dollar, the allocation is usually decided, at the highest decision making level, on the basis of contribution to the fundamental enterprise purpose. For most business organizations this will be stated in terms of margin of profit, return on investment, return on equity or earnings per share. Each of those standards is quantitative and is based upon the idea that each dollar invested or spent should yield the highest possible return. In this sense, anything which does not appear to contribute to that objective is essentially undesirable. If a security program is perceived by senior management as an item of expense for which no compensating return can be identified, or if the return is less than the minimum considered acceptable for allocation of resources, there is a strong likelihood that the program, insofar as it is not unavoidably mandated by statute, regulation or contract, will be de-emphasized or even eliminated. For example, if an enterprise is spending $200,000 annually on personnel and material costs for a security program, and if that program is not yielding (or, much more likely, **has not been shown to yield**) any measurable benefit, the senior management will look at the minimum return level for other investments or the available short-term income opportunities and conclude that, diverted to other purposes, that $200,000 could yield fifteen or twenty percent annually. In this situation, especially if enterprise resources are tight or the economy is in recession or recent enterprise performance has been poor, the **necessary conclusion** for responsible senior managers is to maximize return. The security program may be (and often has been) reduced or eliminated in such a case.

The point is not that the security program was ineffectual or produced no return, but that it was not **perceived** to do so. Of course, it may be that the assets protection effort is not producing benefits because it has been poorly designed or is being ineptly managed. If that is the situation, a much more radical cure than increased or changed awareness is required. But the case would seem to be, based upon wide observation of many programs over a lengthy period, that there are real benefits, in many cases to the extent of multiples of the cost of the program. The benefits, however, may not have been quantified or even clearly identified, and the consequence has been a perception of the security program by senior management as a liability or drag on profitability.

To change this awareness requires: 1) that there be real benefits; 2) that they be commensurate with the resources being consumed; and 3) **that the senior management perceive that relationship.** To the extent that they do, program resourcing may be improved, with the net effect of further enhancing the program results.

Whatever else may be done to bring the specifics of the assets protection program to the attention of senior management, **the effort as a whole must be seen as a justifiable activity in economic terms.** Awareness for this group, then, means principally awareness of the practical contribution to the "bottom line."

## INTERMEDIATE MANAGEMENT

The middle line manager will have a somewhat different and often more parochial view or attitude. While ultimate enterprise success is still a goal, the middle manager cannot achieve it alone, and knows he is not held accountable on that basis. Performance of the department, unit or activity of which he is in charge will determine his personal success. All units do not perform equally in this regard. Indeed, it is evident to any observer that competition among line managers is the rule, and that while good managers do not seek or actively desire poor performance by their peers they are sensitive to relative differences in performance. To the extent that they perceive their personal activity as more successful than that of others they probably will continue that activity. If they perceive themselves as less successful they will probably modify the activities in some way to improve performance. In behavioral terms their "expectancies" will largely determine their "performance." (Further comment will be made on behavioral theories a bit later.)

Thus, if the security program, although possibly contributing to the net good of the enterprise on an overall basis, appears to a given manager to be making disproportionate or counterproductive demands upon him, his attitude will probably be disapproving. If the attitude is negative, response to the program in that manager's area of responsibility may be inappropriate or inadequate. This, in turn, can produce dislocations and strains which may cause program failures elsewhere in the enterprise. For example, if the Laboratory Manager in a sensitive research area perceives the security requirements for application of need-to-know on disclosures to be unnecesarily slowing results in his unit, he may disregard the requirement and permit a general exchange of information. That fact, through the organizational contacts of the lab scientists, may become generally known in other areas, leading to a relaxation there as well. In due course, the widespread internal disclosure of sensitive data may result in an unauthorized external disclosure and the loss of a competitive advantage. If that advantage were a technological trade secret, its development might have involved the expenditure of hundreds of thousands of dollars. In the eyes of one other than the lab manager, the possibility of unauthorized disclosure might be easily perceived as a significant threat to the well being of the enterprise. To the lab manager, however, eager to achieve the technical success, the perceived slowing effect of the need-to-know requirement could easily be seen as more undesirable. **The lab manager's awareness of the security program would have been significantly weighted by his assessment of the impact of some delay on his success.** For the program to be effective in that laboratory the threat of loss of advantage would have to be seen as more critical than delay in achieving the advantage. The key consideration in this case would be to make the laboratory manager aware of the restrictive disclosure requirement in such a way as to assure his agreement. Unless he willingly applied the rule to his operation, the only enforcement avenue would be a negative one — some threat of unfavorable action against the manager for failure to comply. Negative reinforcement of this type seems to be least effective when operating upon persons expected to exercise creative judgement and display innovative independence.[1]

[1] ASPA *Handbook of Personnel and Industrial Relations*, Yoder and Heneman, BNA, Washington, D.C. 1979, page 3-36.

## FIRST-LINE SUPERVISION

Awareness for this group will be related to the ways in which the security program is perceived by them to aid in or detract from their specific performance objectives. Unlike higher levels of management, the first-line supervisor is typicallly concerned with a limited process or activity and not with ultimate performance. So, where a manager of manufacturing would be concerned with final completion in the manufacturing cycle of all scheduled production, a manufacturing foreman might be concerned with the more limited activity of a sub-group, say a drill press department or unit. As long as work in and work out of that unit were timely and met quality standards, the foreman would be considered effective. The semi-finished work out of that unit might be indefinitely delayed for lack of materials or labor or tools at a later stage, with the result that the manufacturing cycle did not finish within standards of time or cost. While that would be an undesirable result, it would not immediately touch the drill press general foreman.

On the other hand, substandard drill press output caused by time lost in meeting property accountability rules for needed manufacturing tools would be viewed as undesirable. If the rules were part of the security program, the program could easily be seen as being in opposition to the supervisor's prime goals, even if machine tool loss were serious and the accountability rules were sensible.

In another context, the head teller in a retail bank might be quite hostile to a security program involving the use of "bait money" at teller positions because of the extended counting time required in reconciling the teller positions at the close of the banking day.

Another aspect of first-line supervisory positions which affects their assessment of the security program is the fact that most employee complaints will be raised, initially at least, with the supervisor. If a large number of complaints are raised in connection with the security program, it can lead to adverse reaction by the supervisor who perceives inordinate time being taken dealing with the security rules.

It is not enough that the rules or requirements have been developed because of a genuine vulnerability and that they are reasonable and responsive. The supervisor must perceive them that way. He or she must be persuaded that the time and attention demanded are **in support of the supervisor's prime task, and not subordinate or irrelevant to it.** The supervisor must not only know the security program as it applies to subordinate personnel, but must see its connection to good performance. An approach that might convince a senior management official that the program was necessary and cost-effective might completely miss the mark with a first-level supervisor.

The differences in perception among the senior executive, intermediate manager and first-line supervisor are in large part due to their **different organizational perspectives** as well as to their individual differences in temperament and personality.

## THE INDIVIDUAL EMPLOYEE

Most modern management approaches to employee motivation assume that the employee is willing and interested, and that while information and instruction may be needed before acceptable work performance can be achieved, coercion and intimidation are not. This was the basis for McGregor's "Theory Y" approach to motivation.[2] But the very least that is required is the basic information and instruction. If certain behavior responses are expected (and their absence noted unfavorably), then employees must know clearly what is expected and that it is reasonably possible to accomplish.

But there are many enterprises in which the only formal exposure an employee gets to the security program may be a cursory reference to it on the first day of work, by a supervisor or personnel specialist who is, at the same time, cramming the employee full of a variety of other information. In addition to inadequate information about his own participation, the employee in that situation may sense that the supervisor or personnel specialist does not consider the security requirements to be important because they are only briefly touched on, or included as an afterthought, or actually portrayed as being of secondary importance. That employee will not only be unaware of the expected behavior, but will not be moved to learn more or even apply the little that may have been absorbed. Initial contact with the security program will have developed an incomplete awareness of the requriements and a sense that they are unimportant to the enterprise or to the employee's role in it.

While incorrect attitudes or understandings of the security program on the part of individual employees can be modified and corrected by interested and informed supervisors and managers, the effect upon the employee of disinterested or disapproving supervisors and managers is certain to worsen what may have been an undesirable initial attitude. Even if the employee was adequately informed, and either approving or at least neutral about the value of the security program, subsequent communication of disinterest or disapproval by supervisors and managers will extinguish any initially favorable attitude.

It seems clear that although the awareness of the security program by employees, supervisors, managers and senior executives will be different, there is a connection among them. The program will fail or falter to the extent it does not address that connection. A security program with poor acceptance by the management group **cannot achieve good acceptance among the workers.**

## PERSONS NOT IN THE ENTERPRISE WORK FORCE

There will be other classes of persons who will have contact with the enterprise, who will not be employees, to whom the security program will also be relevant. Among them will be vendors and suppliers, customers, service personnel and organizations, representatives of government, and members of the general public. Most of these persons will have less opportunity than employees to learn the applicable security requirements; yet it may be quite important that they

[2] *POA Manual*, Chapter 23, Part 1, pages 23-9 and 23-10.

do. For example, if a subcontractor or supplier is to provide elements of a manufacturing process or to do some manufacturing on its own premises, and there is a requirement that the supplier be given access to sensitive proprietary information or entrusted with valuable physical assets, the awareness of that supplier of his responsibilities to protect and account for the information or other assets may be as critical as that of the enterprise's own employees.

With regard to customers or the members of the public, a general impression may be formed of a company or organization from a single contact with its security program. By way of illustration, consider the visitor (potential customer) who visits a company location. After driving fruitlessly for many minutes looking for a parking place (because all the places marked "Visitor" have been filled by employees) the visitor finds one, parks and enters the facility. Upon departure he finds a parking violation notice has been placed on his windshield. Even worse, he and the person he is visiting are interrupted by a guard or other security person in the course of the visit, and he is told to move his car from the space he is unauthorizedly occupying.

Or consider the visitor who is told upon arrival that he must wear a visitor's badge (but not why he must wear it), and then is handed a badge with a pin which he must put through his garment to comply with the requirement. A visitor does not automatically perceive the wearing of a badge as useful or necessary **for him.** However, if the explanation were briefly made that its display would permit immediate recognition by and courteous assistance from employees, and if a little ingenuity in design were displayed to find some alternative to a pin, the security awareness of that visitor would be quite different.

## PURPOSES OF AWARENESS

The preceding discussion has distinguished among five groups, for all of whom security awareness is an important consideration and for each of whom it will be different. It is now appropriate to consider the reasons why security awareness is important for each of these groups. Whether any calculated effort is made or not to make persons in these groups aware of security, they will surely develop some form of awareness merely because there is a program. Given a security program of any kind, security awareness is a certainty. Whether that awareness is positive and supportive or negative and hostile will depend upon the skill with which the assets protection profesional and his management colleagues design and communicate the program elements to the persons in each group. The communication task will be conditioned by the reasons or purposes for which security awareness is developed.

These purposes are to allow a person to:

1. **Understand the relationship between security and successful operations.**

   This purpose will be the prime one for awareness effort directed towards the senior executive management. Although the specific techniques of the program will be of general interest, especially in organizations with fragile personnel or labor relations climates, the

interest will typically be limited. If the program does not cause difficulties with the work force it will normally be acceptable **if the senior management is convinced that it is cost effective.** The assets protection professional will be well advised to devote time and talent to developing persuasive models of the security program's quantifiable value to the enterprise.

The commentary found in other sections of this *Manual* in regard to quantifying security risk and achieving measurable cost benefit ratios are relevant here.[3] It is evident that before useful security awareness work can be done, the program design must be such as to optimize cost effectiveness. In outlining awareness material for senior management it may become apparent that there are areas in the program concerning which there is no demonstrable cost-benefit ratio; that either there is no specific benefit at all or it is not stated in financial terms. This is an indicator that more analysis is needed, either to establish the financial relationships or modify the non-justifiable program elements, or to make absolutely clear the compelling, non-financial reason such elements must be maintained.

2. **Know one's personal obligations under the security program.**

This purpose will, to some degree, affect all awareness efforts. It is, however, the prime purpose of the security awareness material directed to the general employee population. It will require different material and different emphases on common material. It is not of major importance to "cost justify" security measures to the work force. It is of major importance to identify with certainty the obligations all employees have, and to present those as reasonable and necessary.

It is for this purpose that the initial employee briefing and orientation materials are utilized; that periodic refreshers are provided; and that various reminders of the kinds later described in the discussion on techniques of awareness are used. The two key considerations are that **each employee,** in the context of his particular job or assignment, **know precisely** what security requirements apply to him or her. The general tenor of material for this group and purpose is "what to do."

3. **Perceive the connection between security program objectives and selected security measures.**

This slant will be of major concern to the intermediate management. The unit or department head must recognize (and preferably agree) that the security countermeasures which involve or affect his unit are appropriate and that the specific objective of the measures is necessary. This will be particularly true if the requirements are especially onerous for that department or unit. Earlier comments concerning careful development of loss criticality data from other departments of the enterprise should be kept in mind at this point.[4] A unit manager will be more likely to accept sometimes bothersome security requirements if he has participated in the assessment of what the loss impact would be without them.

[3]See especially *POA Manual,* Chapter 2, pages 2-20 through 2-23 and Chapter 23, Part II, pages 23-25 through 23-36.

[4]*POA Manual,* Chapter 2, page 2-15.

4. **Be familiar with sources of help in carrying out personal and departmental responsibilities under the security program.**

This purpose and objective will control the generation of awareness material dealing with specific implementation of the requirements. If there is a security rule that particular spaces or containers be locked, where does the responsible employee or supervisor go to get the lock and key? If a question arises within a unit as to the kind or extent of area and access controls required, who provides definitive guidance?

If the policy and procedure development phase of the program have been adequately dealt with there will be standard answers to these and like questions. However, the persons with the questions may not always be aware of or familiar with the answer sources. As many security professionals have learned, and continue to rediscover, publication of a security manual or policy appendix does not solve the information problem. If persons with legitimate questions or problems do not know to whom they can go for assistance, they may either 1) not go to anyone and improvise an answer, probably the wrong one, or 2) go to the wrong person and be needlessly delayed. If every security policy and procedure in existence at the enterprise is reviewed simply to pinpoint the identity of the person or function responsible for overseeing the accomplishment of particular security requirements, that material could well be simplified and used in awareness activities.

5. **Comply with statutory or common law requirements for notice.**

This will apply as a purpose for both the employee population and for non-employees. Some illustrations will point up what is meant here. Civil trespass to land is generally defined as unauthorized entry into or presence on real property.[5] Although in early law it was not necessary to establish intent to trespass, the rule has now largely become the reverse. To recover civil damages for trespass, the landowner or one in control must prove the trespasser intended to trespass. Clear indications that there is a boundary past which movement is not authorized would be probative in showing intent. Communication (verbal or symbolic) of the existence of the boundary would be relevant. This is a form of awareness.

Taking the same illustration a step further, civil trespass can become criminal trespass if the trespasser can be shown to have been intentionally present without authority on the real property of another, such intent accompanied either by personal communication to the trespasser of his lack of authority to enter or by clear posting of the real estate to the same effect.[6] Anything which the landowner would do to make clear that entry was not authorized, or was authorized only in accordance with established procedures, would fall into the class of awareness activity.

Another highly important illustration of legal notice requirement is found in the area of proprietary information control. The case law in trade secret litigation has clearly established as a majority rule that the proprietor of a trade secret must take positive actions to prevent its unauthorized disclosure. Among these actions are those which would convey

[5] *Black's Law Dictionary*, 5th Edition (St. Paul, Minn: West Publishing Co., 1979).
[6] Ibid

to employees entrusted with the secret that the information was secret and valuable.[7] Although knowledge of its character could be indirectly proved by other facts, the most conclusive evidence would be clear notice to the employee at the time of the disclosure. Developing programs for conveying such notices, and documenting that notification, is a phase of the security awareness effort.

6. **To comply with regulatory requirements.**

Agencies of federal, state and local government often require that specific security-related information be conveyed by employers to employees and others. Cases of general application in this regard are the requirement for orientation and training found in the Bank Protection Act and related regulations of the Federal Reserve System, the Controller of the Currency, and others charged with enforcement of the Act.[8] Other agencies imposing security training and awareness requirements by regulation are the Drug Enforcement Administration,[9] the Department of Transportation,[10] and the Nuclear Regulatory Commission;[11] there are also the Fair Credit Reporting Act notice of investigation requirements and the related rules of the Federal Trade Commission.

In situations where awareness efforts are in direct response to regulatory or statutory requirements, it is essential that the precise requirement be known and that the awareness material in terms of the medium used (written, oral, etc), the form or format, and the particular persons to be given notice, all be those specified in the regulatory source.

7. **To comply with contract obligations.**

The nature of the contract will vary from situation to situation. An example of fairly wide application in the U.S. is the Security Agreement (DD 441) and its attachment (*The Industrial Security Manual*) which control the security obligations of contractors handling classified defense information. The *ISM* imposes numerous requirements for "briefings" and for security education and training, including what we have been describing as "awareness" efforts.

A typical collective bargaining agreement in which there is provision that discharges be for "just cause" will impose the generally applied standard that rules, among other things, be on "due notice." This means either that the employee must know of the rule, or that it was so published that he ought to have known of it. This deals directly with the effort to make employees aware of such rules as they relate to security and assets protection, an area that is a major source of industrial discipline cases and arbitration awards.

---

[7] Milgrim, R., "Trade Secrets," *Business Organizations*, Volume 12 (Albany, NY: Matthew Bender & Co.), pages 5-13 *et seq.*

[8] For commentary on bank security regulations, see Davis, A.S., "The Bank Protection Act After One Year," *Industrial Security*, Vol. 14, No. 2, April 1970, American Society for Industrial Security, Washington, D.C.

[9] 21 CFR 301-72 through 301-76

[10] 49 CFR 95

[11] 10 CFR 70 and 73

Contracts of insurance with commercial carriers may, in some cases, carry requirements that designated employees or officials be made aware of specific requirements. Insuring conditions in some U.S. and British company-written Kidnap and Hostage policies include a requirement that specific procedures be adopted and communicated to designated officials in regard to coverage under the policy.[12]

Other contract obligations to provide security awareness material could arise from an agreement to protect the proprietary information of another organization based upon a trade secret license, or a supply contract, or negotiations preparatory to merger.

## THEORIES OF MOTIVATION[13]

Because awareness material is intended to direct or modify behavior, it should be developed with an informed eye on generally accepted principles of behavior and motivation. This area alone is vast and one of the most profound to be encountered. Psychological in orientation, theories of behavior and motivation have been systematically applied within industrial, government, military and commercial environments, and the results analyzed and evaluated. These assessments have in turn led to further theory modification or development. Training programs used in this business community are usually designed in the light of behavior theory and training staffs, especially in the larger commerical and industrial organizations, can be extremely helpful in awareness effort planning.

It is not the intent of this Chapter to present a detailed discussion of motivation theory. That is beyond the competence of the work and not really necessary. It is the purpose to outline briefly the main currents of present thinking and to point the assets protection professional in the right direction for further research.

### MASLOW'S HIERARCHY

In the 1940's Abraham Maslow published his material on the "Hierarchy of Prepotency." He theorized that the human organism is motivated by an ascending series of needs, and that once the lower (prepotent) needs have been satisfied they will be supplanted by the higher needs as motives for behavior. All the possible human needs Maslow ranked, in ascending order from basic to highest, as follows: 1) **Physiological** (food, drink, shelter); **Safety** (protection from perceived harm); 3) **Love** (affectionate relationships with family and friends); 4) **Esteem** (firm and stable evaluation of the self and respect from others); 5) **Self-actualization** (the desire for self fulfillment, becoming all one is capable of becoming).

The kernel of Maslow's argument is that as long as a human being is preoccupied or concerned with a lower (prepotent) need, there will be no advertence to or concern with any higher need. But that once a lower need has been satisfied it will no longer serve as a motivator, and attention will move up the scale to a higher need. Maslow did **not** insist that behavior would necessarily and in

[12]See *POA Manual*, Chapter 17, Part II.

[13]For further development of the material in this section, see ASPA *Handbook*, cited in preceding note 1, Chapter 3-2 and sources there cited.

every case be dependent upon the scale of needs just noted, or even that any particular need would have to be either conscious or unconscious. He did insist that for the most part, human behavior is organized by the needs and in the indicated rank order.

The significance of Maslow's material in security awareness work is that attempts to motivate or induce persons to specific actions will not even register with them if they are preoccupied with needs lower on the scale. In the kind of setting in which most security awareness efforts will take place it is not likely that the physiological or safety needs will control, but there may be questions of acceptance and esteem. What one's peers will think of one's conduct (acceptance) and the need for one to be approved by others in order to approve himself (esteem) will play a significant role in behavior. Awareness programs which ignore this or which urge behavior likely to create conflict in this area may be unsuccessful.

### McGREGOR'S THEORY X AND THEORY Y

This approach contrasts the worker who is unwilling and requires goading and constant supervision ("X") with the worker who is basically willing and competent but needs guidance and assistance in voluntarily making his own best effort ("Y"). The argument is that worker motivation will be more successful if based on the Theory Y assumptions. (This theory is discussed further in Chapter 9 of this *Manual*. See note 2, ante.)

### HERZBERG'S TWO FACTOR THEORY

This theory maintains that two sets of factors will determine workers' motivation. One set relates to the job content, and in that set the motivators are: **Achievement, Recognition, Satisfaction** from the work itself, **Responsibility** given the worker, and **Advancement.** The other set of factors concern the workplace or environment (job context); and these factors are: The **Company in general** and its administrative and policy framework, the technical **competency of supervisors,** the **salary or compensation,** the **personal relationships** with supervisors, and the **working conditions in general.** Application of this theory has led to the job enrichment efforts of many organizations in which the job content and context have been intentionally modified to respond more favorably to perceptions by workers.

### PROCESS THEORIES OF MOTIVATION

These consider how motivation occurs, not necessarily the specific motivators. One approach, the "Equity Theory," says that a person will compare his effort and related achievement with the effort and achievement of some other, model person and seek for parity or equity. Inequitable achievement (or return) would then tend to reduce motivation to continue or repeat the effort.

Another process theory is the "Expectancy Theory" which holds that beliefs concerning the **Performance** to be achieved by **Effort** will effect the kind and amount of effort made, and that beliefs concerning the attainment of desirable **Outcomes** as a result of **Performance** will determine the performance goals selected. For example, if a promotion is a desirable outcome and the promotion is seen or believed to depend upon increased production or improved quality

production (the performance), then desire to be promoted will result in increased effort to achieve more or better quality production. If "compliance with security objectives and requirements" is substitute for "more" or "better" production in this illustration, the relevance of this theory is apparent.

## BEHAVIORAL THEORY OF MOTIVATION

In this approach, consideration is given to two factors outside the person motivated. One is the environment and stimuli from the environment which produce reflexive or responsive behavior. Termed "Respondent Behavior," this theory holds that, given the appropriate stimulus, the behavior is virtually automatic. It is a consequence of the environment acting on the person.

Another theory, called "Operant Conditioning," says that once desirable consequences are perceived to follow typical behavior, the actor is reinforced to repeat the behavior. In this theory the environment does not produce a reflex or automatic response, but may suggest a setting in which a previous action followed by a favorable result could be repeated. In that regard it "cues" the actor to the particular behavior. The more often the behavior is followed by the favorable or desired result, the more likely will be future similar behavior. Approval in a way meaningful to the worker (or supervisor or manager) for satisfactory performance of security tasks or discharge of security responsibilities could, thus, be considered likely to motivate future compliance-type behavior.

## TECHNIQUES OF AWARENESS

Unlike techniques of security training, which will always require content specifically related to the security tasks required of the trainee, Security Awareness material may — but need not —have specific security task content. If it directs the attention towards security content available elsewhere (e.g., in formal training materials) and generates approval or support of the main security purpose, it will be effective.

The techniques which have been used and are generally available to most security program managers include the following:

1. **Written Material.** This can include instructional or advisory material, agreements and acknowledgements. It also includes written security policies and procedures, posters, and other informal reminders such as coverage in house organs.
2. **Formal Security Briefings.** These can be done pre- and post-hire, at new assignment orientation, and at times of promotion or transfer.
3. **Integration Into Line Operations.** This technique is most useful and can be employed by including specific coverage of security performance in merit and promotional reviews, bonus or incentive compensation distribution, regular or special supervisory and management staff meetings. Inclusion of security tasks in job descriptions is another line integrating technique.

## AWARENESS RESOURCES

To exploit security awareness fully in the sense discussed in this chapter, the security program elements themselves must be designed with a clear idea of patterns of motivation and response. The different interests of the various populations to be dealt with will also affect the materials developed and the skills needed in their development. In addition to the security and assets protection staff, it is likely that substantial assistance both in program element selection and in awareness material generation can be obtained from the following groups:

1. **Training Staff.** Specifically charged with developing effective material to modify or introduce desired behavior.
2. **Communication Staff.** This can include internal communications specialists such as the Public and Community Relations staffs, the editorial staffs of house publications, and external communications staffs to the extent the organization uses them. These could be communications consultants, advertising and public relations agencies.

## CONCLUSION

It should be clear at this point that developing an awareness about the assets protection program is critically important.

"Awareness" is a neutral term, and the awareness generated can be supportive and approving or the very opposite.

Awareness will develop even without planned control, and in that event it could very likely be unfavorable.

Awareness is not synonymous with either "training" or "education," although it is intimately related to both. Training and education materials should be developed with clear ideas about the relevance of awareness and its impact on motivation and ultimate behavior.

Awareness is a state of mind — all facets of the enterprise are useful and relevant to its development.

## SELECTED BIBLIOGRAPHY

Garofalo, J., *Public Opinion About Crime*, U.S. DOJ (LEAA), Washington, D.C., Report No. SD-VAD-1, USGOP 1977. (Correlations between perception of crime and behavior modifications)

Healy, R.J. and Walsh, T.J., *Industrial Security Management: A Cost Effective Approach*, (New York: AMA, 1971) especially pages 48-50.

Leavitt, H. and Pondy, L., eds., *Readings in Management Psychology*, (Chicago, Ill.: Univ. of Chicago Press, 1964).

Paine, D., *Industrial Security*, (Madison, Wisc.: Oak Publications, 1972), especially pages 186-191.

Ursis, H. and Pagano, L., *Security Management Systems*, (Springfield, Ill.: Chas. Thomas, Inc., 1974), especially Chapter 11.

TIMOTHY J. WALSH, CPP

President
Harris & Walsh Management Consultants, Inc.
P.O. Box 698
New Rochelle, New York 10802
(914) 576-0820

With Harris & Walsh since 1966, Walsh developed and directs the firm's international activities in security and assets protection. He was previously Security Manager, Sperry Gyroscope Division of Sperry Rand Corporation and Security Director, Allen B. DuMont Laboratories, Inc. He was also formerly supervisory special agent, U.S. Naval Intelligence Service and Detachment Commander, U.S. Air Force Office of Special Investigations.

He is a member: New York, federal and U.S. Supreme Court bars. AB, Fordham, JD, St. John's Univ. School of Law, LLM(Labor Law), New York University Graduate School of Law; graduate OCDM staff college and diplomate Industrial College of the Armed Forces.

Member: American Bar Association (Section on Torts and Insurance Law); N.Y. State Bar Association; American Arbitration Association (Commercial Panel); National Fire Protection Association; Int'l Assoc. of Chiefs of Police; Institute of Criminalogy, University of South Africa; American Society for Industrial Security, of which last named group Walsh is past President and past board chairman. He was formerly academic director of the A.S.I.S. Security Institute and served on the first A.S.I.S. Professional Certification Board. He is past chairman of the Electronic Industries Association Security Committee. Currently a member of the Protective Lighting Committee, Society of Illuminating Engineers.

Formerly Adjunct Assistant Professor of management, New York University and formerly assistant professor, communications arts, Fordham University.

Co-author: "Industrial Security Management: A Cost-Effective Approach", 1971, AMACOM, and "Protecting Your Business Against Espionage", 1973, AMACOM. Contributing author: Maintenance Engineering Handbook, McGraw-Hill; Designers' Handbook for Building Security, McGraw-Hill; Personnel and Industrial Relations Handbook, American Society for Personnel Administration. Co-editor of "Protection of Assets Manual", a continuing publication of The Merritt Company, Santa Monica. Cal. Co-author with R.J. Healy of "Principles of Security Management", 1982, Professional Publications.

Cited for most significant contributions to professional literature, American Society for Industrial Security, Int'l, 1962, 1966, 1969 and 1974. Award for Distinguished Professional Service, American Society for Indstrial Security, Int'l, 1977.

***

# THE 1984 OLYMPIC GAMES

# A CHALLENGE AND AN OPPORTUNITY

# FOR LAW ENFORCEMENT

Presented by

William M. Rathburn

June 7, 1983

## INTRODUCTION

For only the second time in history the Summer Olympic Games will be staged in the United States. The XXIII Olympiad will be in Los Angeles in 1984 as the X Olympiad was in 1932. Needless to say many changes have occurred in the ensuing 52 years and many of these changes have affected the Games in some way. Changing political environments have affected the Games almost every four years since at least 1936. The effect has varied from overt racism in 1936 to cancellation in 1940 and 1944 to demonstrations in the 50's and 60's to boycotts in 1976 and 1980 and ultimately even to a major terrorist incident in 1972 in Munich.

The law enforcement role has also changed significantly over the years. The official report of the 1932 Olympics does not even mention the word "security", and the only law enforcement involvement mentioned was the nearly 1000 police officers concerned with traffic control.

Since the 11 Israeli Olympians were killed by the Black September group in Munich in 1972, security has perhaps become the major concern in staging the Olympic Games. No government can afford to do less than is necessary to prevent a repeat of Munich. The security posture can never return to what it was before Munich.

## MAGNITUDE OF 1984 OLYMPIC GAMES

To appreciate the magnitude of the security responsibility of the Olympic Games, it is necessary to understand the magnitude of the Games.

- The Games last for 16 days from July 28 through August 12, 1984.
- Between 12,000 and 14,000 athletes representing 152 countries will participate.
- Between 12,000 and 15,000 representatives of all forms of news media will cover the Games.
- Television coverage will be 225 hours - triple the 75 hours of coverage for the 1976 Montreal Olympics.
- Olympic activity will be seen on television by 2 1/2 billion people throughout the world - more people than have ever seen any other event in history.
- 7,000,000 tickets will be available for Olympic events
- 350,000 people per day will be drawn to the Los Angeles area by the Games.

If the shear size of the Games is not enough to cause concern, there are other factors that magnify the potential problems.

- There are 48 agencies at the local, state and federal levels with some security responsibility.

- There is no legal provision for unified command of security resources for the Games.

- For the first time since 1932 no Olympic Village will be built. Althletes will be housed on college campuses.

- The Games are the Los Angeles Olympics in name only as they are spread through 5 counties and 8 cities. In addition, some preliminary soccer games will be played at Harvard, Annapolis and Stanford.

- Local taxpayers are unwilling to bear any of the financial burden of the Games, and voters in the City of Los Angeles have even approved a City Charter amendment prohibiting the expenditure of regular City funds for any Olympics purpose including security.

## LAW ENFORCEMENT RESPONSE TO THE OLYMPICS CHALLENGE

Security planning for the 1984 Olympics began in early 1979, over 5 1/2 years before the Games and several months before the Los Angles Olympic Organizing Committee (LAOOC) was established to stage the Games. The initial learning phase involved just a few major local and federal agencies and included trips to Montreal, the site of the 1976 Olympics, to San Juan, Puerto Rico for the 1979 Pan American Games, and to Lake Placid for the 1980 Winter Olympics. The knowledge gained from these on-site visits combined with extensive research, eventually led to the development of an interagency planning model. The model was designed to provide for necessary but limited involvement; for coordination of effort to insure maximum efficiency with minimum duplication of effort; and for cooperation without unity of command.

The cornerstone of the interagency planning model was the recognition of individual agency autonomy whether functional or geographical.

### Olympic Law Enforcement Coordinating Council (OLECC)

OLECC is the major policy-making body for overall Olympic security planning. The members represent the major entities involved in security planning for the Olympics. By mutual agreement, the Long Beach Chief of Police represents all of the smaller agencies within which Olympics activity occurs. OLECC

currently meets quarterly and receives information from and directs policy decisions to the Security Planning Committee (SPC). Membership is as follows:

Chief of Police, Los Angeles
Sheriff, Los Angeles County
Chief of Police, Long Beach
Special Assistant to the President
Special Agent-in-Charge, FBI
Representative, Governor of California
President, Los Angeles Olympic Organizing Committee

## Security Planning Committee (SPC)

The Security Planning Committee coordinates local, state, federal and international security measures. Currently, the SPC meets every other week. The role of the committee is as follows:

- To coordinate the overall security planning effort.
- To direct the efforts of the subcommittees.
- To direct the work of the Integrated Planning Group.
- To advise agencies and organizations of the Olympic information, circumstances and situations which may impact their responsibilities during the Games.
- To recommend policy positions to the OLECC.

## Integrated Planning Group (IPG)

The Integrated Planning Group (IPG) serves as a common point of contact and as a resource center for the various agencies involved in Olympic security planning. The Integrated Planning Group is comprised of representatives from the LAPD, LASD, CHP and various other agencies at the local, state and federal levels which choose to participate on a voluntary, need-to basis. The basic premise of the integrated planning concept recognizes the importance of local, state and federal agencies working together at the same location to develop the plans necessary for all security tasks associated with the Olympics. The IPG staff, under the direction of the Security Planning Committee, works to coordinate and standardize Olympics security operations to avoid gaps or duplication of effort. The IPG is, in effect, the staff arm of the SPC. The Integrated Planning Group and/or members of the group:

- Advise the Security Planning Committee on matters relating to security planning.
- Act as liaison between the Security Planning Committee and various police and security organizations involved in the Olympics operation.

- Support the planning efforts of all subcommittees involved in security planning.

- Act as a clearinghouse for interagency information and serves as a central repository and reference library for all Olympics security information which is available to subcommittees and their members.

- Act as resource persons to the subcommittees.

The IPG staff also ensures that requests for information on Olympics security matters from the Olympic Law Enforcement Coordinating Council or the Security Planning Committee are channeled to the proper subcommittees or are completed within the Group.

Although the goal of the IPG is to standardize and coordinate Olympic security planning efforts, there is the clear recognition that the sheriff or chief of police in each jurisdiction is, by statute, responsible for providing police service within each respective political subdivision. The IPG members respect the statutory responsibilities of individual agencies while still striving to provide the coordination of effort necessary to provide a safe and peaceful environment for staging the 1984 Olympic Games.

## Subcommittees

The primary function of the subcommittees is to plan all interagency aspects of Olympic security which require uniformity throughout the Olympic activity. The membership of the subcommittees is determined by the Security Planning Committee and is comprised of representatives from all involved agencies. The subcommittees are formed to delve into every aspect of Olympics-related security within specific areas of responsibility.

Each subcommittee is activated, as necessary, by the Security Planning Committee with the approval of a planning precept. The precept designates the chairperson, identifies the membership, states the subject of the subcommittee efforts, and gives instructions and information for courses of action. The subcommittee chairperson has the option of recommending additional subcommittee membership to the concurrence of the Security Planning Committee.

The major detailed planning for the Olympics in areas where there is interagency involvement and concern is done through the subcommittees. Sixteen subcommittees have been established to plan all aspects of Olympic Security. The subcommittees are:

| | |
|---|---|
| Accreditation | Emergency Response |
| Air Support | Intelligence |
| Bombs/EOD | International Entry |
| Communications | In-Transit Security |
| Community Relations | Olympic Village Security |
| Crime Prevention | Traffic Control |
| Criminal Justice System | Training |
| Dignitary Protection | Venue/Vital Point Security |

The subcommittees are comprised of representatives of the various city, county, state, federal, and private agencies involved in the Olympic security effort.

## OPERATIONAL PHASE COORDINATION

### Olympic Security Coordination Center

The model that has been discussed is the coordination mechanism for the planning phase. The operational phase requires a different type of coordination - coordination that is immediate and continuing. Coordination for major unusual events in normally accomplished through an exchange of liaison personnel between the agencies involved or that might become involved. Because of the numerous liaison personnel that would be required if this approach were utilized during the Olympic Games, an operational coordination model was developed. This model, called the Olympic Security Coordination Center (OSCC), will provide the common point of contact between all of the agencies with security or law enforcement related responsibility. The OSCC will be comprised of 50 or more representatives from various agencies and will serve as one medium of communication between all of the agencies - agencies that do not have radio communications compatibility for the most part.

Information from the various agency command centers will flow into the OSCC and will be displayed visually for everyone present. Information relevant to a certain agency, as determined by the agency representative, can then be transmitted to that agency command center. Requests for information, assistance or mutual aid can be personally directed from one agency representative to another. To supplement this in-person coordination, or to substitute for it in the case of smaller agencies, all involved agencies will also be linked by an electronic mail system.

It must be reemphasized that the OSCC is only a coordination mechanism, not a command center since, as was mentioned previously, there is no statutory provision for single agency command.

## Intelligence Coordination

Intelligence Coordination will be accomplished by the Anti-Terrorist Operations Center (ATOC) and the Field Intelligence Coordination Center. Intelligence information will be gathered from a variety of sources - international, national and local. The Anti-Terrorist Operation Center will be located at a remote site while the Field Intelligence Coordination Center will be co-located with the OSCC. ATOC will also be linked to all of the law enforcement agencies that have Olympics responsibility by the electronic mail system that can be used to disseminate information of an emegency nature that becomes known to ATOC.

## Interagency Traffic Command Center

The Traffic Command Center concept deviates from the normal approach that each agency will be autonomous. The agencies with traffic management responsibility will be co-located and will make the broad traffic management decisions. Those decisions will then be communicated to the individual agencies for implementation. Decision making in traffic management cannot be left delegated to the individual agencies because of the ripple effect that a wrong traffic management decision made at a local level might have throughout the entire transportation system. The Traffic Command Center will be housed in the headquarters of the California Department of Transportation and will utilize existing traffic monitoring systems such as CCTV and traffic volume counts, to facilitate traffic management planning.

## Other Functional Coordination Centers

There will be several other functional interagency coordination centers established including the Protected Officials Coordination Center, the Air Support Coordination Center, the Bombs/EOD Coordination Center, the Emergency Response Coordination Center, and the In-transit Security Coordination Center. In addition, there will be a rumor control network that will be linked to the Olympic Security Coordination Center to provide a mechanism to disseminate accurate information of a law enforcement nature to dispel false information that might create law enforcement problems within the communities impacted by the Olympics.

## PERSONNEL REQUIREMENT AND AVAILABILITY

It should be obvious at this point that numerous law enforcement personnel will be required to police the 1984 Olympic Games. In 1976, Montreal deployed 17,000 security personnel for the Olympics. Law enforcement agencies in Southern California cannot match that number. There are fewer than 17,000 sworn law enforcement officers in all of the law enforcement agencies in Los Angeles County combined. Personnel to police the Olympic Games must come from a variety of sources. Los Angeles will utilize the largest number of private security personnel ever used in the Olympic Games. These private security personnel will in effect be

the eyes and ears of the sworn law enforcement personnel. Law enforcement personnel will be generated in a number of ways. These include the assignment of personnel to work 12 hour watches, the cancellation of days off, the deferment of vacation , and the reassignment of personnel from staff assignments. In prior Olympics military personnel and/or National Guard personnel have been utilized in law enforcement roles. In the United States, the posse comitatus laws prohibit the use of regular military personnel for direct law enforcement purposes so regular military involvement will be support only. The National Guard will be utilized but it is planned at this time that they will also be utilized only in a support role.

It is clear that in 1984 we will not be able to match previous cities in terms of the number of security pesonnel deployed. What that means is that the various law enforcement agencies involved must do a better job in planning the Olympics so they can be policed with a smaller number of personnel.

## FINANCING SECURITY FOR THE OLYMPICS

In 1978, the voters of the City of Los Angeles approved a Charter Amendment that prohibits the use of regular City funds for Olympics purposes. The only City funds that can be utilized must come from a special Olympic trust fund. This fund derives revenues from a one-half of one percent tax on bed space within the City and from a future special Olympics ticket distribution tax. In 1982 the Los Angeles City Council approved a contract with the Los Angeles Olympic Organizing Committee which provides that the Olympic Commitee will reimburse the City for all costs incurred by the City to the extent that the costs exceed the revenues that accrue to the Olympics trust fund. The contract also provides for a maximum of $22.1 million dollars for all City services, including all security services outside the competition sites, housing sites, and training sites within the City. The cost for security inside those sites has been accepted as a financial responsibility of the Olympic Committee.

Other law enforcement agencies at the local level are currently negotiating with the Olympic Commitee for reimbursement for Olympics related expenses. These negotiations are necessitated by a pervasive public attitude that no taxpayer money should be spent for the Olympic Games.

## LAW ENFORCEMENT CONCERNS

The first thing most people think about when considering the law enforcement problems associated with the Olympic Games is the possibility of terrorism. That concern is real and certainly foremost in the minds of all of the law enforcement personnel involved. But terrorism is only one of many concerns and many areas that require law enforcment planning and preparation. The greatest role for law enforcement officers may well be pure public service - helping people get from one location to another helping them find their lost children and lost property and protecting the visitors themselves as they go to and from events. Crime is also a major concern as it is the general consenus that the Olympics will serve as a magnet for criminals of every type and description. Obviously, major crimes committed during the Olympics or committed against visitors attending the Olympics will be major news throughout the world. Such negative publicity obviously could tarnish the image of the United States.

Another major concern for law enforcement is that the 1984 Olympics are twelve years after the Munich incident. Unfortunately, too many people do not remember the full impact of the Munich incident and are not as receptive to a high security profile as they should be. Also the fact that there were not major security related problems during the 1979 Pan American Games in Puerto Rico, in the 1980 Winter Olympics in Lake Placid or in the 1980 Summer Olympics in Moscow tends to lull the general population into a false sense of security.

## BENEFITS OF THE OLYMPICS

Perhaps the greatest benefit to law enforcement agencies will be the long term effect of the cooperation and coordination that has been necessitated by the Olympics. This should continue after the Games as agencies recognize the value of such an attitude, and the law enforcement community will be stronger as a result.

Other benefits should include an increased level of law enforcement preparedness, economic impact in the billions and an improvement in the image of law enforcement. Also, crime should go down during the Games as has been the case during recent Olympics.

WILLIAM M. RATHBURN

Bill Rathburn is a Commander with the Los Angeles Police Department. Since 1979 he has been assigned as the Department Olympic Games Planning Coordinator with overall responsibility for planning Police Department activities for the Games. During his 20 years with the Police Department, he has served in a wide variety of assignments in all major police functions including patrol, traffic, investigation, administration and management.

Bill has a Bachelor's Degree in Public Management from Pepperdine University and a Master's Degree in Public Administration from the University of Southern California.

# Operational Utility of Psychology Instruments to Law Enforcement and Security[1]

Ira H. Bernstein, Ph.D.
Department of Psychology
P.O. Box 19528

Since it is well established that people remember what they hear at the beginning and at the end of a talk better than what they hear in the middle, I'm going to state and then restate the major points of my talk. These are:

1. Basically there are two ways to improve the caliber of personnel: (a) Selection of better people to begin with, and (b) Modification of the work environment to optimize the performance of people already on hand. These are not exclusive objectives. The fact that I will dwell only upon the former merely reflects my personal skills and interests and not necessarily the demands of any given situations.

2. For most situations, the two main prerequisites of successful performance that involve selection issues are that people be: (a) sufficiently intelligent and (b) emotionally stable, two traits which both involve flexibility of thought and action. Of these, the intelligence is by far the more important for most positions, especially those without an "emergency" component or without potential harm to others, e.g., clerical positions.

3. There is a vast literature and technology of available tests usable for personnel selection that is cost efficient to employ.

---

[1]The author thanks James Adams of Psychodynamics, Inc. for his comments on a draft of this paper.

4. An important ingredient of any selection process is validation research.

5. If validation research is properly carried out the results may appear disappointing in that correlations between predictions of job performance and actual outcomes are typically fairly low. There are a variety of reasons for this to be the case, some of which are not serious. Among those which are serious include: (a) the failure of supervisors to agree upon what is a good subordinate, (b) the use of the "right" tests for the "wrong" situations, and (c) a poor work atmosphere that offsets good selection practices. Among the less serious are: (a) statistical factors such as "range restriction" to be discussed below and (b) the fact that work on the job itself can, in a beneficial environment, change a person for the better.

## Varieties of Assessment Instruments

The "Bible" of Psychometricians is the Mental Measurements Yearbook, founded and originally edited by the late O.K. Buros and currently in its Eighth Edition. It contains basic information and reviews on any test of practical interest.

The Yearbook lists 1184 tests. Most of these are not relevant to my talk, e.g., tests of reading development for school children. For our purposes, the following categories are most relevant: (a) tests of intellectual ability, (b) tests of maladjustment, and (c) tests of "Normal Personality traits". Other types of tests that can be of some utility but which I will not discuss are: (a) tests of specific knowledge and aptitudes, e.g., clerical ability, and (b) vocational interests. I will

also limit the talk to objectively scorable tests.

Tests of Intellectual Ability: Tests of intellectual ability ("group intelligence tests") used in personnel settings have been constructed in a variety of ways. Some, like the Differential Aptitude Test provide a profile of several intellectual skills such as abstract reasoning and verbal reasoning. Others, like the Ravens' Progressive Matrices and Culture Fair Intelligence Test, yield but a single measure. The latter two, in addition, measure abstract reasoning. In contrast, other tests are oriented towards knowledge and facility with written English. One such test was developed by the U.S. Civil Service Commission specifically for use in the selection of law enforcement personnel, the Basic Occupational Language for Police Officers (BOLPO).

Since whole symposia are given on the topic of the measurement of intelligence, my comments must necessarily be brief. First, correlations between task performance and intelligence measures run far higher, as a rule, than between task measures and other psychological test predictors like maladjustment indices. In other words, stupidity is typically the biggest and most pervasive threat we face.

At the same time, intelligence testing has caused the greatest problems of a legal nature, especially in the private sector, of any pre-employment screening devices. Some of these problems were caused by the misuse of tests, most commonly by setting cutoffs for minimum competency that were far higher than those needed for the job. In other cases, the companies sued by unsuccessful applicants or employees who were passed over for promotion failed to perform the necessary validation research to

document the job relatedness of the test. Those interested in some truly excellent defenses of the need for intelligence testing in pre-employment screening might well profit from the many collaborative writings of John Hunter of Michigan State University and Frank Schmidt of the United States Civil Service Commission.

Since this talk is specifically concerned with the selection of people in law enforcement and security, I might note that in this setting, the particular type of intellectual measure (abstract reasoning vs. reading comprehension, for example) is probably less critical than in settings involving highly developed technical abilities. Typically, all forms of intelligence measures correlate positively among themselves and this fact makes most forms of measures suitable. Such tests can be completed in well under an hour.

Tests of Maladjustment: Tests of maladjustment are usually constructed by selecting items which differentiate normals from selected psychiatric groups. As such, the items tend to involve admissions of psychiatric symptoms or denials of positive mental health. The most widely known of these is the Minnesota Multiphasic Personality Inventory (MMPI). Other suitable instruments include the Institute of Personality Assessment's Clinical Analysis Questionnaire, Part II (CAQ-II) and Richard Lanyon's Psychological Screening Inventory (PSI). The MMPI is easily psychology's most widely cited test. Hence, more is known about its strengths (most noticeably its elaborate and sophisticated controls over attempts to "beat the test") and weaknesses (most noticaably its 566 item length). The CAQ-II and PSI are much shorter but, at the same time, lack the degree of

assessment that can be made as to test takers attitudes.

I'll turn later to some general points that apply to all tests, but there are a couple of important things to note about maladjustment screening devices. One point is that they differ in a fundamental way from intelligence and other personality measures in terms of how they should be used. With a maladjustment screening device, one is primarily interested in screening out those applicants who are the most maladjusted. On many scales, people with extremely good (nonmaladjusted) scores don't out - perform people whose scores are average in the workplace. Conversely, if a task makes any intellectual demands at all, there tends to be a more continuous ("the more, the merrier") relation between test results and performance.

Secondly, maladjustment screening devices are most effective in detecting traits that are reflective of those thought and emotional (mood) disturbances seen in psychiatric settings because they were developed in that context. In other words, they are extremely good at assessing those deficits seen among psychiatric inpatients. They are less well suited (though hardly un suited) to detect personality problems known as conduct disorders-problems in living due to long standing and inflexible traits.

A conduct disorder requiring special note is psychopathy (which fortunately, is evaluated on all major tests of maladjustment). In contrast with its popular depiction, it does not necessarily involve aggression. What it does involve to a very large extent is a pathological search for excitement. Some indirect evidence for the greater prevalence of this disorder among law enforcement applicants than similar personnel seen for

screening (e.g., non-security at nuclear power plants) exists, in that the percentage of law enforcement applicants with elevated scores on the MMPI's measure of psychopathy does run higher than these other personnel. This is not surprising. People with psychopathic traits would be expected to seek out law enforcement careers for the perceived excitement. What often happens, of course, is that the real life world of law enforcement fails to provide this excitement, so they supply their own, thereby causing mischief, to put it mildly.

There are other forms of conduct disorder. It remains the task of future research to assess these traits more adequately.

"Normal" Personality Tests: Cattell's Sixteen Personality Factor tests (the 16 PF, also known as the CAQ-Part I) and Gough's California Psychological Inventory (CPI) represent the third category of test I will talk about today. These tests measure a variety of traits that are, as a rule, less directly connected with psychiatric traits than the previous category, although most of the traits, like the CPI's Responsibility Scale, have obvious "Good" and "Bad" poles. Specifically, the CPI, which I have used rather extensively, has 6 scales which measure personality skills. One would see in a face-to-face or short-term setting such as Dominance, 6 scales which assess more long-term traits like Responsibility, 3 scales which measure social intelligence and achievement values and 3 miscellaneous scales (Psychological Mindedness, Intellectual Flexibility and "Masculinity-Femininity" in the active-passive sense).

Although test results from the MMPI and CPI (or similar pairs of tests) are certainly not independent of one another, they are not intended

as substitutes. Many people who are not emotionally or psychiatrically maladjusted lack the skills necessary for success in law enforcement, especially in a supervisory capacity. I stress this because some suggest the use of tests like the CPI as a substitute for the MMPI, because the former contains fewer objectionable items. However, we find that these objectionable items, like "I have a compulsion to steal" which is paraphrased from the MMPI, are acknowledged by a not insignificant percentage of people (1-2%) even after they have been interviewed by personnel managers and evaluated favorably by them.

## Test Validation

It is always proper to ask the question "Has test X been validated for Law Enforcement work." However, a fair answer cannot always be given simply.

When most people think of the term validated, they are thinking in terms of a demonstration empirical relation between scores on the test and actual work performance. Technically, this is but one of three accepted forms of validity called Predictive validity. I'll discuss the other two, construct validity and content validity below.

In one study, we found a small, but statistically significant, i.e., non-chance relation between Scale 1 of the MMPI, which was developed using hypochondriacs as a target group. This was not surprising - Scale 1 consists of items dealing with bodily complaints. It is reasonable to assume that those people who were more inclined to complain about their health at the time they were hired will report in sick more often at a later time. Likewise, we and several others find similar small but

significant relations between Scale 9 on the MMPI and accident rate - again no surprise because Scale 9 deals to a large extent with items reflecting impulsivity. These are the standard sorts of relations reflecting predictive validity.

Now consider the following; MMPI scale 8 consists of various items reflective of unusual and inappropriate thoughts and ideas. It was developed using hospitalized schizophrenics as a target group. Using the T-score scale standard on the MMPI, normal groups average around 50 and hospitalized schizophrenics around 70. The latter is a conventional cutoff defining an elevated score on that scale.

Suppose you got MMPI measures from a group of people performing a task potentially dangerous to others such as police officers or nuclear reactor operators. You might well find no relation or a minimal relation between scores on Scale 8 and measures of job performance. Does this mean the measure is invalid? Hardly! In the course of analyzing your data, you would probably note that with almost any decent form of personnel selection, there will be very few people with high scores on Scale 8. This will obviously be the case when the MMPI is explicitly used as a selection tool but will also occur to some extent when ordinary interviewing is used because people who act "strange" are less likely to be hired than people who act more normally. In short, those people most likely to do untoward things are screened out and, hence, not given an opportunity to confirm the relation between scores on Scale 8 and poor judgment on the job. The technical name for this vitally important reason why even highly valid tests are likely to show low correlations with

on-the-job performance is range restriction.

Fortunately, we don't need to hire a group of schizophrenics to show that they perform more poorly than normals in order to use Scale 8. What we can do however, is resort to construct rather than predictive validity as a strategy by showing that (a) the ability to think in a conventional, logical manner is job-related and (b) the difference between normals vs. schizophrenics and others with thought impairments on Scale 8 is supportive of this scale as an index of ability to think conventionally. More generally, construct validity entails showing that a measure indexes a particular trait.

Though content validity is less applicable here than in other settings, it is useful to note in passing. It refers in essence to "testing by doing," i.e., by showing that the behaviors sampled on a test are also those demanded by the job. Tests of specific skills like typing are frequently validated in this manner.

In performing a predictive validity study for a local police force, we observed what has been suggested by others. Both CPI and MMPI measures relate in the expected manner with a variety of objective , but limited measures of performance of police officers. Better adjusted and more socially adequate officers took fewer sick days, had fewer accidents, etc. As further expected, these relations were relatively low. We also found that relations with more global measures, the supervisory ratings were stronger, but in the "wrong" direction. Better adjusted and more socially skilled officers were rated more poorly by their supervisors.

This is clearly a relation that should not be taken at its face value.

Being neurotic, psychotic or character disordered does not a better officer make. Rather, it reveals the difficulties in using supervisory ratings and, more generally, in defining adequate, global criterion measures. What best seems to fit the facts is that supervisors preferred the more maladjusted and unskilled officers, because these officers were also the more submissive and less threatening to them.

Millions of dollars have been spent trying to define adequate criteria and I wish I had a ready answer to suggest a single, simply obtainable measure to you. I don't. I certainly can tell you that you individually may have a good idea of what a good law enforcement officer or, more generally, subordinate, is, and you probably do. However, your concept may turn out to be very different from your colleague's concept and (let's blame him); his idea may be unrelated or inversely related to yours or any other meaningful definition.

I don't want to make the problem seem insurmountable, only complex. Well trained people in test construction and utilization methods (psychometricians) learn how to combine objective indices like sick days, accident rate, superivsory ratings and other sources of data such as peer ratings to have their individual liabilities offset one another. There is no substitute for clarity of thought on any matter. However, the modern computer and associated data analytic techniques allow thought about validation to be implemented in a manner not possible a generation ago. As a psychometrician I am biased, but I feel no area of psychology better reflects the interactions among pure research, applied research and technology better.

A Note on Selection of Minorities: The issue of validation is intimately tied in with problems of selection from minority groups. Indeed, the EEOC Uniform Guidelines (1978) explicitly note that test validity is only an issue when there is adverse impact upon one or more protected groups of individuals.

Historically, pencil and paper tests of all forms have had adverse impact upon many cultural and ethnic minorities in much the same manner as physical agility tests have had upon females. As noted, tests have been misused because of inappropriately chosen cutoffs, e.g., requiring people to do things on a test they would never have to do on the job, or poorly chosen tests.

A particular argument that was raised in the 1970's is that a test may be valid for one group (usually stated as Whites) but may not be valid for another (usually, Minorities). This is the hypothesis of differential validity. However, Hunter and Schmidt have looked at the issue of differential validity. Although their results are somewhat controversial, they argue against the generality of this hypothesis in a way I find most convincing.

Because of the appeal of the differential validity hypothesis, let me spend a minute illustrating how spurious evidence for differential validity may arise when a predictor itself is (imperfectly) but equally valid for two groups. I'll use height as a simple example and males and females as the two groups. Assume, for argument's sake that, in general, taller people make better police officers and that this relation is equally true for both sexes. Knowing this, a minimum height requirement of 5'6" is

set. This requirement might only eliminate 10% or so of the males but would eliminate 50% or so of the females (the precise numbers don't matter as long as it is considerably different for the two groups). What is the effect? The range of heights will be much less for the remaining females and, due to this important but often overlooked effect of range restriction, correlations between height and performance will be lower among those females selected.

While on this point, let me note one more point about the issue of test bias made by Hunter and Schmidt. There are three clearly discernable philosophies regarding how one should take minority group differences into account:

1. One should totally ignore sex, race, etc. in deciding what to use in personnel selection and select the "best" person.

2. One should correct for biases in selection devices by some compensatory device.

3. One should insure representation of minorities in some proportionate sense, i.e., use a quota system.

Each of these philosophies has, I hope, some appeal. The philosophy of "pick the best person" is rooted in our country's values. Also, recognizing the imperfections of any selection system, it would seem morally wrong not to correct for sex and racial biases, if they exist. Finally, most recognize the need for diversity of backgrounds and adequate representations of various cultural groups in any position.

Hunter and Schmidt show how each of the three philosophical positions leads to a statistical definition of bias. I will not go into these

technical issues. Rather, I'll simply go to the conclusion: The inherent conflict among the three philosophical positions, each of which appears so worthy by itself, means that a test which is unbiased by one standard must be biased by another as long as group differences exist!

Validity Across Jobs: I am often asked whether a particular test, such as the MMPI, is valid for a specific job. At this point in my talk, I hope the question of what type of validity enters your mind. Here are some important considerations.

1. Suppose a particular relation exists for one group, say MMPI Scale 1 predicts sick days for police officers. If similar factors operate with a related group, say security officers, and if the underlying variability in the trait measured by Scale 1 is similar, there is no reason to expect a very different relation. Neither "if" is trivial. Situational variables affecting the police force and the security organization can produce substantial differences in motivation to take days off. Depending upon selection criteria, there may be more, less, or the same spread on Scale 1 in the new group. The relation would be stronger, weaker, or the same (based upon experience there would probably be more in the security officer group).

2. Task analysis is vital to a determination of suitable assessment instruments. You can't determine what skills must be measured in applicants unless you know what they are to do. People sharing a common title in two settings may perform a vastly different function and require different skills.

3. Gathering criterion data; Using data from a related job is a

useful start but the process of validation is a continuing one. Relations between predictors and performance change as the nature of the job changes. At DNA, potential adversaries are getting more sophisticated - hence the demand for an intelligent security force increases. Still, you don't know how effective your selection program is unless you monitor it.

4. Don't expect too much from your selection devices. Depending upon various factors, good selection devices can improve things by about 10 to 30 percent. Various people will try to sell you on "the newest" psychological test and claim enormous success.

Don't believe it. Too much of what a person does is determined by factors that are present after a person is hired, i.e., the work environment, including the attitudes of the supervisor. The technology of testing hasn't changed all that much. For example, maladjustment screening devices developed since the MMPI probably don't predict any better than the MMPI. They are less time consuming from the applicant's standpoint, which may be a plus, especially if the situation demands several tests be given. The Millenium hasn't come and, with the limited attention given to basic research in the behavioral sciences, isn't likely any time soon. This doesn't mean that what we have to offer isn't valuable, which it is. It just isn't magical. Consider what a 10 to 30 percent increase in efficiency of selection with standard (and reasonably cost effective) assessment devices translates into in dollars and cents terms and you'll get the message.

## Conclusion

To return to what I said at the beginning of my talk, let me make the following points in summary:

1. In dealing with selection of police and security officer personnel, use standard tools to make sure they: (a) possess sufficient intelligence, (b) are emotionally stable, and (c) have adequate interpersonal skills. I prefer the Differential Aptitude Test, the MMPI and the CPI, respectively as part of a basic, inexpensive screening battery (I have been doing some work on a summary report which pools the data from these tests). Other tests can serve similar purposes.

2. Consider the importance of continued job validation, including task analysis.

3. Understand the statistical limits on what can be expected from even the best selection devices and the modifying effects of the work environment.

I THANK YOU.

Ira H. Bernstein, Ph.D.

Biography

1. Education: B.A.-University of Michigan, 1959
M.A.-Vanderbilt University, 1961
Ph.D.- Vanderbilt University, 1963
Postdoctoral-University of Illinois, 1963-64

2. Academic Experience:

Assistant Professor to Professor - University of Texas at Arlington. Also, Clinical Professor of Psychology, University of Texas Health Science Center at Dallas.

3. Professional Experience:

Screening of police applicants and various applicants to positions at Nuclear Power plants, including guards since 1978. Currently consultant to Psychodynamics, Inc., a company which screens such personnel.

4. Honors:

(1) Certificate of Merit from American Medical Association for research on diagnosis of effects of early eye diseases.
(2) Fellow of American Psychological Association and Society for Personality Assessment.
(3) Who's Who in the South and Southwest.
(4) Invited participant to Attention and Performance in 1959 and 1975. This is an international symposium on research in human thought processes.

5. Relevant Publications:

Over 50 scholarly articles plus two which appeared in Security Management, the trade publication of the American Society for Industrial Security. The most recent publications deal with the internal structure and validity of personality tests, especially when used in the selection of people for jobs that bring potential danger to the public.

Examples include:

(1) "One Way to Screen Security Guards", Security Management, 1981.
(2) "Truncated Component Regression, Multicollinearity, and the MMPI"s use in a Police Officer Setting", Multivariate Behavior Research, 1982 (with L.S. Schoenfeld and R.M. Costello.

## ROSTER OF PARTICIPANTS

Preston S. Abbott
President
Abbott Associates, Inc.
801 N. Pitt St.
Alexandria, VA 22314
(703) 836-8080

Joseph A. Barry
ASEC
5 Old Concord Rd.
Burlington, MA 01803
(617) 272-7910

Harvey G. Beavers
GM-14, Air Force
Action Officer
Aerospace Security Division
AFOSP/SPOS
Kirtland AFB, NM 87117
(505) 844-9091, AV 244-9091

Thomas M. Belcher
Senior Security Advisor
Audio Intelligence Devices
1400 NW 62nd St.
Ft. Lauderdale, FL 33309
(305) 776-5000

Dr. Ira Bernstein
Professor of Psychology
Department of Psychology
University of Texas at Arlington
P.O. Box 19528
Arlington, TX 76019
(817) 273-3183
***Speaker***

William D. Bitler
LTC, USA
Chief, R&D Branch
Defense Nuclear Agency
ATTN: OPNS
Washington, DC 20305
(703) 325-7881

Benjamin J. Bonner III
Colonel, USA
Chief, Command Security Office
HQ, Defense Logistics Agency
Cameron Station
Alexandria, VA 22314
(202) 274-6066

C.R. Bukolt
Head Equipment Branch
Chief of Naval Operations (OP-009D)
Navy Department
Washington, DC 20388
(301) 763-3490

Deborah A. Burke
Senior Consultant
Booz, Allen & Hamilton, Inc.
4330 East West Hwy.
Bethesda, MD 20014
(301) 951-2517

Loren L. Bush, Jr.
Senior Security Specialist
Nuclear Regulatory Commission
7716 Falstaff Ct.
MCLean, VA 22102
(703) 893-7480

Kim F. Cashbaugh
LT, USA
Special Agent
Pentagon, CI Force
Washington, DC 20310
(202) 697-0150

Allan N. Cheuvront
CPT, USA
MP Operations Officer
Provost Marshal Office
ATTN: OPNS Officer
Fort Belvoir, VA 22060
(703) 664-1254

Dr. John C. Chin
Clinical Psychologist
Department of the Army
P.O. Box 70217
Ft. Bragg, NC 28307

Dr. Thomas W. Christ
Vice President, Administration
HDS, Inc.
12310 Pinecrest Rd.
Reston, VA 22091
(703) 620-6200
(919) 396-7533

Hugh D. Clark
LTC, USA
Provost Marshal
Fort Belvoir, VA 22060
(703) 664-2727

Charles H. Cogswell
MAJ, USA
Provost Marshal
Office of the Provost Marshal
Fort Myer, VA 22211
(202) 692-15[illegible]

Thomas F. Co[illegible]less
Professor of Law and Sociology
The George Washington University
Washington, DC 20052
(202) 676-7465

Cheryl A. Cross
Supervisory Security Specialist
Naval Surface Weapons Center
White Oak Laboratory
Silver Spring, MD 20708
(301) 394-3520

Barbara G. Curtis
MAJ, USA
Defense Nuclear Agency
ATTN: OPNS
Washington, DC 20305
(703) 325-7361

John DeMarco
Chief, Technical Resources Branch (PS[illegible])
Office of Federal Protective Service
General Services Administration
18th & F Sts. NW
Washington, DC 0405
(202) 535-7292

Robert W. Doms, S[illegible]
LTC AUS, Ret.
Regional Manager
Audio Intelligence Devices
P.O. Box 1
Timonium, MD 21093
(301) 252-85[illegible]5

Joseph C. Drauszewski
Lt Col, USAF
Nuclear Security Staff Officer
ATTN: OPNS
Defense Nuclear Agency
Washington, DC 20305

Donald O. Egner
Chief, Close Combat Directorate
USA Human Engineering Laboratory
ATTN: DRXHE-CC
Aberdeen Proving Ground, MD 21005
(301) 278-5946

Christopher G. Essig
CPT, USA
Operations Office of Law
Enf. MDW
Headquarters MDW
ATTN: DCSOPS-LE
Ft. Mc Nair, Washington, DC 20319
(202) 693-0246

M. Thomas Fairris
LTC, USA
Chief, Security Management Division
HQ, Forces Command
ATTN: AEPM-SM
Ft. McPherson, GA 30330
(404) 752-3457

Frank Farkas
MAJ, USA
Chief/Senior Policy Staff Officer
US A CIDC
5611 Columbia Pike
Falls Church, VA 22041
(202) 756-1474/70

Francis J. Farrell
Director, Security Division
U.S. Department Agriculture
Rm 412A Admin Bldg.
14th & Independence
Washington, DC 20250
(202) 447-3853

Joseph Fishburne
Colonel, USA
Chief, Psychology Service
Walter Reed Army Medical Center
Washington, DC 20307
(301) 576-1065

John E. Foster
Instructor
Defense Investigative Service
Defense Industrial Security Institute
C/O Defense General Supply Center
Richmond, VA 23297
(804) 275-4891

Kenneth C. Freimuth
LTC, USA
Chief, Physical Security Committee
U.S. Army Military Police School
Ft. Mc Clellan, AL 36205
(205) 238-3760

Gee-In (Gee) Goo
Electronic Engineering GS-855-13
U.S. Naval Surface Weapon Center
Electro-optics Branch R-42
White Oak
Silver Spring, MD 20910
(202) 394-3457

Robert W. Gray
Program Manager
U.S. Capitol
Security Coordination Team
331 First St., N.E.
Washington, DC 20510
(202) 225-5321

Donald P. Greenwald
Colonel, USA
Chief, Physical Security Division
Office of the Provost Marshal
HQ, US Army Europe and 7th Army
APO New York 09086
(0621) 732-845

Hart J. Guenther
Colonel, USAF
Chief, Aerospace Security
HQ, Air Force Office of Security Police
AFOSP/SPOS
Kirtland AFB, New Mexico 87117
AV 244-9091

Charles A. Hammaker, Jr.
Security Department Manager
Dynalectron Corporation
Army Support Division
P.O. Box 1107
NAEC, Lakhurst, NJ 08733
(201) 657-0001

William E. Hawkins
LTC, USA
Commander CI Detachment
Defense Nuclear Agency
6801 Telegraph Rd.
Alexandria, VA 22310
(703) 325-7043

Richard Healey, CPP
President
Professional Protection Enterprises, Inc.
4401 Atlantic Ave
Suite 30
Long Beach, CA 90807
(213) 422-4559
***Speaker***

Dr. Neil S. Hibler
Maj, USAF
HQ, AFOSI/IVSB
Bolling AFB
Washington, DC 20332
(202) 767-5287

Kenneth A. Hirsch
CPT, USA
Chief Psychosomatic Service
Letterman Army Medical Center
Presidio of San Francisco, CA 94129
(415) 561-5115

Billy Hix
Security Administration
C.I.A.
Washington, DC 20505
(703) 351-6620

Jack N. Holcomb
President
Audio Intelligence Devices
1400 NW 62nd St.
Ft. Lauderdale, FL 33309
(305) 776-5000

Van D. Holladay
Colonel, USA (Ret)
Security Consultant
15250 John Marshal Highway
Haymarket, VA 22069
(703) 754-2499

Nettie B. Hudson
SA, USA
Pentagon CI Force
Washington, DC 20310
(202) 697-0150

Douglas P. Huth
CDR, USN
Operations Branch
OJCS J-3/SOD
Washington, DC 20301
(202) 695-4087

Larry R. Israel
Security Specialist
US Government - Dept of Army
Product Manager
Physical Security Equipment
ATTN: DRCPM-PSE
Ft. Belvoir, VA 22060
(703) 664-2893

Brian Michael Jenkins
Program Director
Security and Subnational Conflict
Rand Corporation
1700 Main St.
Santa Monica, CA 90406
(213) 393-0411
***Speaker***

Chester C. Jew
Security Specialist
Office of Federal Protective Service
General Services Administration
Rm 2314 GSA Bldg
18th & F Sts. NW
Washington, DC 20405
(202) 535-7293

Thomas E. Johnson
GM-13
Nuclear Security Staff Officer
Defense Nuclear Agency
ATTN: OPNS
Washington, DC 20305
(703) 325-7361

Paul A. Jureidini
Vice President
Abbott Associates
801 N. Pitt St.
Alexandria, VA 22314
(703) 836-8080

L.J. Kimball
Lt Col, USMC
Plans & Policy Officer
HQ, JSOC
P.O. Box 70239
Ft. Bragg, NC 28307
(919) 396-0576

Arthur A. Klekner
Director, Office Security & Safety
US General Accounting Office
441 G St. NW
Washington, DC 20548
(202) 275-8119

Dr. Richard W. Kobetz
Richard W. Kobetz & Associates, Ltd.
North Mountain Pines Training Center
Route 2 - Box 342
Winchester, VA 22601
(703) 662-7288

Richard Krumm
Consultant
Abbott Associates
801 N. Pitt St.
Alexandria, VA 22314
(703) 836-8080

Richard F. Law
Colonel, USAF
Director of Counterintelligence
HQ, AF Office of Special Investigations
Bolling AFB, DC 20332
(202) 767-5131

David L. Lemon
LTC(P), USA
Chief, Military History Division
Center of Military History
Pulaski Bldg.
20th & Massachusetts Ave., NW
Washington, DC 20314
(202) 272-0303

Charles R. Linton
Colonel, USAF
Director for Operations
6801 Telegraph Rd.
Alexandria, VA 22310
(703) 325-7032

Angus Boyd MacLean
Chief, Metro Transit Police & Director
Office of Transit Police & Security
Washington Metropolitan Area
Transit Authority
600 Fifth St., NW
Washington, DC 20001
(202) 637-1550

D.G. Macnair
Manager
Marine Security
Gulf Refining & Marketing Co.
2 Houston Center
Houston, TX 77218
(713) 754-4830
***Speaker***

Ira R. Meyers
Deputy Director
Federal Protective Service
GSA - National Capital Region
Bldg. 159 E - Navy Yard Annex
2nd M Sts. SW
Washington, DC 20407
(202) 472-1632

R.T. Moore
Manager Computer Systems Group
National Bureau of Standards
Tech A216
Washington, DC 20234
(301) 921-3427

Dale L. Moyer
Maj, USAF
Nuclear Security Staff Officer
Defense Nuclear Agency
ATTN: OPNS
Washington, DC 20305
(703) 325-7365

Ralph H. Murphy
Manager, Technology Requirements
Magnavox Government & Industrial
Electronics Co.
1700 N. Moore St.
Suite 820
Arlington, VA 22209
(703) 522-9610

William D. Norman
Director of Security
New Zealand Embassy
37 Observatory Circle, NW
Washington, DC 20008
(202) 328-4800

O.P. Norton
Research and Certification
American Society for Industrial Security
1655 N. Ft. Myer Dr.
Suite 1200
Arlington, VA 22209
(703) 522-5800

Timothy R. O'Neill
MAJ, USA
U.S. Military Academy
West Point, NY 10996
(914) 938-2515

Daniel A. Perkowski
CPT, USA
Nuclear Security Staff Officer
Defense Nuclear Agency
ATTN: OPNS
Washington, DC 20305
(703) 325-7361

David J. Poel
Colonel, USA
Provost Marshal, Director
Law Enforcement & Security
HQ, TRADOC
ATPL-L, Ft. Monroe, VA 23651
(804) 727-3262

Richard A. Pomager, Jr.
LTC, USA
Military Assistant
Nuclear Security
ODUSD(P) (SPCP)
Washington, DC 20301
(202) 697-2242

Commander William Rathburn
Office of the Chief of Police
Olympic Games Planning Group
Los Angeles Police Department
P.O. Box 30158 (Mail Stop 950)
Los Angeles, CA 90030
(213) 485-7267
***Speaker***

Michael A. Rauer
CPT, USA
Nuclear Security Staff Officer
Defense Nuclear Agency
ATTN: OPNS
Washington, DC 20305
(703) 325-7361

James L. Rea
Sandia National Laboratories
P.O. Box 5800 Division 9212
Albuquerque, NM 87185
(505) 844-9970, AV 244-9970

William K. Rector
Colonel, USAF
Commander
3280th. Technical Training Group
Lackland AFB, TX 78236
(512) 671-3626, AV 473-3626

George Riddick
Senior Associate
Systems Research Corporation
5201 Leesburg Pike
Suite 600
Falls Church, VA 22041
(703) 379-6844

Edward E. Ridgley
Special Agent
Federal Bureau of Investigation
FBI Academy
Quantico, VA 22135
(703) 640-6131

Dr. Alexander G. Rozner
Group Leader
Naval Surface Weapons Center
White Oak
Silver Spring, MD 20910
(202) 394-2737

Frank S. Salcedo
Colonel, USA
Chief, Civil Security Division
Federal Emergency Management Agency
Washington, DC 20472
(202) 287-0785

Daniel P. Scruggs
Director, Testing Services
London House Management Consultant
1550 NW Highway
Park Ridge, IL 60068
(312) 298-7311

Alfred E. Seddon
Federal Bureau of Investigation
10th & Pennsylvania Ave. NW
Washington, DC 20220
(202) 324-4650

Daryl K. Solomonson
Manager, Advanced Security Systems
TRW (Defense Systems Group)
One Space Park
Bldg. 134/7039
Redondo Beach, CA 90278
(213) 217-3431

James L. Stinson
Manager
Behavioral Sciences Department
CACI, Inc. - Federal
450 Newport Center Dr. (#300)
Newport Beach, CA 92660
(714) 720-0672
***Speaker***

W. Michael Symonds
MAJ, USA
Nuclear Security Staff Officer
Defense Nuclear Agency
ATTN: OPNS
Washington, DC 20305
(703) 325-7091

David H. Thompson
CMSgt, USAF
Superintendent
3280th Technical Training Group
Lackland AFB, TX 78236
(512) 671-3626, AV 473-3626

James T. Turner, Ph.D.
Director, Behavior Science
SAS of Texas, LTD
3445 Executive Center Drive
Suite 111
Austin, TX 78731
(512) 345-5635

S. Van Cleave
President
Inter-American Consultants
5647 Conway Drive
Marietta, GA 30067
(404) 992-6452

S.D. Vestermark, Jr.
Fellow Inter-University Seminar on
Armed Froces and Society
Box 46, 1126 E. 59th St.
Chicago, IL 60637
(312) 962-8694
***Speaker***

Roger L. Wadsworth
SA, USA
CT Analyst
Defense Nuclear Agency
6801 Telegraph Rd.
Alexandria, VA 22310
(703) 325-7043

David W. Wahler
SFC, USA
NCOIC Communications
Defense Nuclear Agency
6810 Telegraph Rd
ATTN: LECD
Alexandria, VA 22310
(703) 325-7092

Robert D. Walker
MAJ, USA
Nuclear Security Action Officer
Office of Army Law Enforcement
HQ, Department of Army
ATTN: DAPE-HRE
Washington, D.C. 20310
(202) 694-1214

Timothy Walsh, CPP
President
Harris & Walsh Management Consultants
P.O. Box 698
New Rochelle, NY 10802
(914) 576-0820
***Speaker***

Gerald T. Warren
GYSGT, USMC
Physical Security Chief
MPH-53 Room 4012
HQ, Marine Corps
Washington, D.C. 20380
(202) 694-4177

James E. Wheeler
LTC, USA
Chief, Nuclear Security Division
Defense Nuclear Agency
6801 Telegraph Rd.
Alexandria, VA 22310
(703) 325-7881

Michael J. White
SA, USA
Asst. Ops Officer
Defense Nuclear Agency
6801 Telegraph Rd.
Alexandria, VA 22310
(703) 325-7043

Michael Q. Whitley
LT, USN
Psychologist
Department of Defense
4704 Thresher Ct.
Virginia Beach, VA 23464
(804) 425-4921

Gerald O. Williams
Lt Col, USAF
Nuclear Security Staff Officer
Defense Nuclear Agency
ATTN: OPNS
Washington, DC 20305
(703) 325-7361