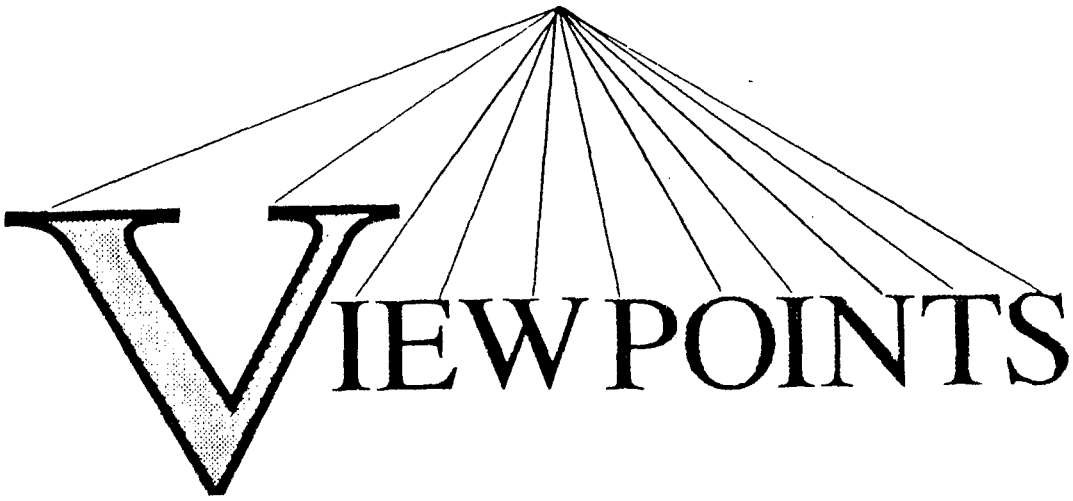
VIEW

A PUBLICATION of the NATIONAL CLASSIFICATION MANAGEMENT SOCIETY
VOLUME 2, 1994

ISSN-0009-8434

Published by the National Classification Management Society. Mailing address: Executive Secretary, NCMS 6116 Roseland Drive, Rockville, Maryland 20852. Editor of this volume: Raymond P. Schmidt. Editorial Review Board: Carol F. Donner, General Research Corporation; Marilyn H. Griffin, Naval Coastal Systems Center; James H. Mathena, Martin Marietta Corporation; Dr. Arvin S. Quist, Martin Marietta Energy Systems. Board of Directors Publications Oversight: Dr. Roger P. Denk. Publications Coordinator and Publisher: Eugene J. Suto. The information contained in this periodical and presented by the several authors does not necessarily represent the views of their organizations or the National Classification Management Society.



PURPOSE

The purposes of the National Classification Management Society are:

- To advance the profession of Security Classification Management.
- To foster the highest qualities of professional excellence among its members.
- To provide a forum for the free exchange of views and information on the methods, practices, and procedures for managing security classification programs and related information security programs.

Members are encouraged to submit articles, think pieces, scholarly studies, and letters about any aspect of classification management and information security. All security subjects are fair game for inclusion in ***NCMS VIEWPOINTS.***

PERIODICAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY

CONTENTS

EDITORIAL COMMENTS

It seemed axiomatic in the years following World War II that Americans should and must study the history of their own country. A firm grounding in our past would help us understand several traditions of Western Civilization: the discipline of science, basing interpretations on verifiable facts, the exercise of logic, a faith in the democratic process, commitment to equality before the law and to opportunity for individual development, working toward improvement by learning from our personal and collective experience, striving for peace, and curiosity about the worlds around us–including the world of ideas and, as the war showed, the all-too-often violent resolution of conflicting ideas.

Moreover, our educational experience must not end at the water's edge, or with the awarding of degrees and certificates. Western Civilization was rather intended to provide citizens with a vantage point from which to study other civilizations, their culture and history, and to know the world we inhabit.

The late Professor Edgar N. Johnson, latterly of Brandeis University and previously of the University of Nebraska, imparted this perspective in his courses on Western Civilization and Medieval Europe. He was part of that generation of historians who served their Nation during the Second World War and defended these values of the Western Tradition, some with their lives. His two-volume study, An Introduction to the History of the Western Tradition, addressed the responsibility of those in authority to meet the needs of oncoming generations, particularly in dealing with competing ideas about government and politics.

Dr. Johnson drew two major conclusions in his 1958 history that seem still relevant. First, he observed that we must learn how to control the rapidly accumulating knowledge and technique of modern science. Second, and only slightly modified for 1995, we need to avoid wars in which this knowledge and technique would be applied by nations to their certain destruction. The logic of his argument leads one to the point that failure to control the rapid explosion of science might bring about wars that end Western Civilization, and probably other civilizations as well. The causal relationship might not be simple and direct, but the indirect effects of science can be considerably more sophisticated and even more powerful, such as is so richly illustrated by James Burke in his television programs and books, Connections and The Day the Universe Changed.

Conflict and war are dominant themes that permeate human history. Conflict, internal and international, remains a constant in human affairs during this period after the end of the Cold War. The stakes in harnessing science have never been greater. Those of us engaged in security disciplines face challenges that may be different in scope but still contain these familiar themes. NCMS members serve agencies and companies engaged in defense work. We must be at once accountable to our employers, yet flexible—and responsive to the changing needs of the American public. This edition of Viewpoints presents articles written by authors who are familiar with conflict and who understand the implications of losing control of the knowledge and technique of science.

Readers will appreciate **Nicholas Rostow**'s perspective on managing conflict as he offers his insights into the vital operations of the National Security Council (NSC). This is a rare opportunity for readers to learn how the NSC works. His article should help members understand how senior policy makers view national security as they formulate and defend positions on issues that concern the National Classification Management Society (NCMS)—and, indeed, all US citizens.

In this guest editorial, Mr. Rostow also illustrates how competing interests bear on the NSC staff from many quarters. His discussion of constraints on public discourse particularly deserves careful study. He offers us reassurances that the NSC of the 1980s held strong and professional concerns about security matters, even while not always taking time to cope with downgrading and declassification of documents.

There are indications that some NSC procedures and policies may have changed in recent years. If an account of more recent years becomes available, it will be published in Viewpoints.

Joseph A. Grau is known widely throughout NCMS, Government, and industry. His article on dealing effectively with managers offers specific ways for security specialists to present their concerns

in a constructive manner. He writes the way he has presented this "talk" orally to security professionals—clearly, directly, informally, and humbly. All of it comes across as uncommonly good common sense. Members who wish to communicate further with him are invited to write or call him at the Department of Defense Security Institute in Richmond.

Christina M. Bromwell provides the first response ever received to a previous Viewpoints author. In her thoughtful and analytic counterpoint to Maynard C. Anderson ["Information Security Program: Is the Future Behind Us?," Volume 1, 1994, pp. 1-9], she challenges the often-repeated outsider's criticism that the current national security information program is "broken" throughout Government and industry. Noting that more than one program exists, she recommends taking a surgical—rather than a meatcleaver—approach to the "patient."

Her article should not be viewed by critics as a defense of the status quo by a hidebound "security cop" nearing retirement. She does have over a decade of experience in security and brings a fresh perspective based upon her own extensive interactions within her agency and throughout the security community. Indeed, she asks that both critics and defenders of the existing and proposed security program examine and justify their mantras!

Participants in the Presidential Review Decision (PRD)-29 Task Force can attest to the vast differences in efficiency, effectiveness,and structures of their programs that reflect their different agency missions and cultures. After all, no one expects the Department of State to conduct a daily routine exactly like that of a tank or ship crew. So why expect their security needs to be identical? One size rarely fits all, and PRD-29 Task Force members generally acknowledged this. She also suggests that citizens and taxpayers might fairly ask for limits on the efforts that agencies should be required to take to preserve, and then expedite the release of, classified records documenting their activities for the benefit of special interest researchers.

In this connection, members should know that, on 10 November 1994, the Administration issued Executive Order 12937 declassifying 43.9 million pages of records covering World War II and more recent decades up to US involvement in Vietnam. According to National Archives officials, the records constitute about 14% of all their classified holdings. Executive Order 12937 marks a departure from previous practice in that few of the records were subjected to a page-by-page review prior to release. Rather, various risk-management approaches were taken to ensure that passage of three or more decades permitted declassification of the information. It should be noted that approximately 12% of the records initially proposed for declassification using this "cost-saving" approach were quickly determined to require continued protection—even decades after they were created. A copy of the Order appears as the final Viewpoints article before the appendices.

Neither Christina Bromwell nor **Maynard C. Anderson** was aware of their dialogue taking shape over the summer and fall of 1994. Nevertheless, we are fortunate that Maynard Anderson expanded his thoughts beyond those he provided Viewpoints last time. His latest contribution avoids the very misperception cautioned about in the previous "Editorial Comments." At least one critic [Steven Aftergood, "Secrecy and Government Bulletin," Issue Number 40, October 1994, Federation of American Scientists] captured perfectly a selected aspect of Maynard Anderson's earlier article. Unfortunately, Mr. Aftergood's comments overlook these observations also made in that article:

"[T]he best information concerning our [policy-making] process is with those who must implement the policy."

"[The information security culture] will not change unless its constituencies cooperate and make it change."

"Directed actions derived from the work of non-professionals who ignore the culture will be ignored, in turn."

"[C]ustomer and client feedback analysis is seldom undertaken, or if undertaken, application of the results is seldom evident. This was vividly demonstrated during the PRD-29 process when committees were established within the task force only to have their respective products ignored or disregarded by higher levels of the review hierarchy."

"Unfortunately,...contributions [of experienced security professionals] are most often run through filters in the bureaucracy or ignored completely while an order is drafted and approved by officials

who have no hands-on experience in administering or managing the program. In the current case, agency positions have been ignored while others lacking basic knowledge of program requirements, legal requirements, and administrative requirements have told us what is good for us once again."

These, it should be clear, are many of the same points he emphasizes in this edition, and are similar to those raised by Christina Bromwell.

Perhaps the most helpful suggestion is for readers to study all three articles in one sitting and decide for yourself what requirements must be satisfied if the US intends to create a single security program that will work in all agencies and industry.

Edward Keith Jackson obliged NCMS by preparing a brief summary of a classified document that cannot be released. The demise of the Coordinating Committee on Multilateral Export Controls (COCOM) is not news to most NCMS members, but the implications of its disappearance may be less obvious; certainly, the majority of voters and taxpayers are only vaguely aware of this issue.

Aside from the pros and cons of COCOM, another issue arises from the "new world" that we have entered so boldly—that of "the threat." The persistent clamor for someone to define "the threat" to US classified information (NSI) has been viewed by some with skepticism and even bemusement. One security specialist recently made a statement that illustrates why some among us are puzzled. "Cleared personnel," the official said, "are constantly challenging us to explain why, since the KGB and GRU are no more, we still need an array of elaborate protective measures."

Perhaps security professionals have fielded such challenges from within and even outside their organizations. Naturally, those with intelligence and counterintelligence backgrounds immediately will respond with surprise by asking who thought that the KGB and the GRU were the only hostile intelligence gathering organizations in the world?! How many of us are not aware that such activity continues today under new names? Who in this nation of highly competitive business people remains innocent about the potential loss of trade secrets, or NSI, or other information and data?

Security professionals understand that the legitimate employment of classification and protective measures is intended to restrict access to NSI to those with the authorization and need to know it. We may not know precisely who wants the information [foreign nations, international corporations, terrorist groups, rebel factions, organized criminal elements], but we do know who should see it. Why should it be necessary to name all who may NOT have access?

An illustration from contemporary urban and suburban living in these United States might help focus on a key aspect of this issue. Most homeowners lock the doors to their residences. We do this because we have things of value to protect. Normally, we have no names in advance for the criminals or mischief-makers who might trespass. Nor should it matter that we know the names of those targeting our homes. The objective is adequate protection, no matter whether it keeps out "robber A" or "vandal B." It is sufficient to understand the consequences of unauthorized entry into your house, just like the consequences of losing or compromising NSI.

Mark O. Hamersly took us up on the offer that "all security subjects are fair game" for publication in Viewpoints. He brings considerable expertise and long association with various terrorist threats to his discussion of violence in the workplace. Many US workers are concerned about this relatively recent phenomenon. Other Viewpoints authors have referred to it; Mark Hamersly addresses it directly.

Readers will almost certainly find something in his article to agree with, or disagree with, but we hope not too violently! In this, as all other issues, readers are invited to write and express your own viewpoints. This is precisely why Viewpoints exists.

Viewpoints lost a mentor and strong advocate several months ago when Mr. Dave Whitman transferred oversight responsibility to Dr. Roger Denk, another Board of Directors member who brings the same quest for excellence to this assignment. All of us wish both of them success in their current and future endeavors. Similarly, I express my regret at the retirement of Mr. Eugene J. Suto as Executive Secretary and Publisher of NCMS. Like other members, I appreciate his cooperation and support and I will miss the professional association with him and Barbara, the lady who never seems to

rest. Fortunately, Gene and Barbara will continue our association as friends and neighbors.

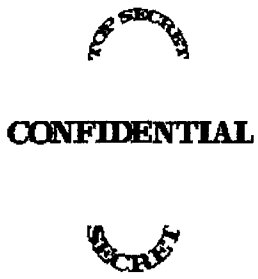
After four years as editor of Viewpoints, I believe that NCMS should take a look at this publication along with a number of questions relating to internal communications among the highly intelligent and well-informed members of this Society. We need to keep pace with your needs and to provide you with the information and opinions important to your professional development.

Therefore, I invite members to let me know what topics have been helpful and what has been lacking. I also urge you to express your views to chapter and national officers, including the Board of Directors. Members should take every opportunity to articulate your needs and wants and to express your views about NCMS publications. This is your publication, just as NCMS is your organization.

Any form of expression is welcome, of course, but I prefer that you state your comments in writing and sign them! And, as our "Guidelines" for submitting articles notes [Appendix B]: "Commonly-accepted professional standards of propriety, civilized discourse, and discretion should be observed." Here's looking to a viable NCMS in the year 2000 and beyond!

RAYMOND P. SCHMIDT
NOVEMBER 1994

GUEST EDITORIAL



The People's Secrets as Viewed from the National Security Council

Nicholas Rostow

Mr. Rostow served as Special Assistant to the President for National Security Affairs and Legal Adviser to the National Security Council from 1987 to 1993. During that time, he worked closely with many professionals whose business is the preservation of the people's secrets. In this speech to the NCMS Washington Chapter in December 1993, Mr. Rostow acknowledged that he came to respect and admire security professionals. Furthermore, he noted that he appreciates "how thankless your job is and how well it is discharged."

My theme is the relationship between the people's secrets and their preservation, and our Government's choices in foreign and national security policy. The subject is as old as history. One need only think of the consequences for the Greeks if their plan to use a wooden horse to enter Troy had leaked to the local Asia Minor "Washington Post." True, Cassandra cautioned the Trojans against the horse — but she was not in a position to quote a secret government document provided to her newspaper by an "hitherto reliable senior Greek official!"

"[Alexander Hamilton argued in favor of adopting the Constitution because it strengthened the national government. His argument] ultimately rested on the premise that the world is a dangerous place and that secrecy is sometimes needed."

In the United States, of course, efforts to establish a national, Government-wide system of classifying national security information on a rational, across-the-board basis dates only from 1951,[1] near the beginning of the Cold War. But the problem of protecting the confidentiality of information important to the country's foreign and national security policies goes back to the adoption of the Constitution.

One of Alexander Hamilton's most commonly cited arguments for the proposed Federal Government was that it could fulfill the need to act with secrecy and dispatch in foreign affairs. His argument, of course, was addressed to the relative merits of strong and weak national governments. Nevertheless, it ultimately rested on the premise that the world is a dangerous place and that secrecy is sometimes needed.

Hamilton is worth recalling in these rather different circumstances of 1994 because those who believe that information — in addition to the blueprints for nuclear weapons—needs to be classified are now challenged to explain why. For many people in our country, the end of the Cold War has removed all justification for secrets.

The disappearance of the Soviet Union was an extraordinary event, transforming the threat picture for the United States and the rest of the world. But it has not meant that all threats have disappeared or that the need for some military readiness has vanished, or that we cease to need robust intelligence capabilities. In short, the end of the Cold War has not meant that we have no national security interests to protect and that we no longer need a Government capable of acting secretly and with dispatch. We do. And therefore we continue to have measures for protecting national security information from unauthorized disclosure.

"[T]he end of the Cold War has not meant that we have no national security interests to protect or no longer need a government capable of acting secretly with dispatch."

[1]Executive Order 10290, issued by President Harry S. Truman on 24 September 1951. For discussion of antecedents to this Order, consult NCMS-member Arvin S. Quist's Security Classification of Information, Volume I; Report of the Commission on Government Security, signed by Chairman Lloyd Wright on 21 June 1957 and prepared pursuant to Public Law 304, 84th Congress, of 10 November 1955; and various other published and unpublished monographs.

It ought to be clear now that I am speaking of national security information only. The Government generates and receives lots of other information that is sensitive and needs to be kept in confidence. Some involves trade or business secrets of private companies. Some involves delicate political dealings that might unravel through premature disclosure. Still other information reflects the views and advice of Government officials who would cease to offer their candid advice and certainly would cease to be candid in writing if there were no lawful means of keeping such advice and views in confidence. This information may have its dissemination limited to a small number of officials based upon specific laws and regulations, and not necessarily because it is national security information.

At the same time that the need for secrecy persists, the pressures for disclosure increase. Other governments and international organizations demand to share our capabilities and knowledge. Ordinary citizens with all kinds of agenda increasingly ask for disclosure—researchers, private litigants, defendants in criminal proceedings, congressional investigators. All are relatively intolerant of traditional arguments for preserving the nation's secrets or even for the existence of such secrets.

"Policymakers are not immune...to the temptation to use national security information for advantage in political give-and-take."

Policymakers are not immune to these pressures or to the temptation to use national security information for advantage in political give-and-take. We all know that. At the same time, policymakers are the duly authorized persons to decide when and under what circumstances information may be or should be declassified. The choice is never easy.

U.S. Nicaragua policy provides a useful example of what I mean. In 1985, the United States was engaged in a politico-military struggle on three fronts. First, there was the situation on the ground in Central America — Sandinista support for guerrillas in El Salvador, Honduras, and Guatemala, and, to the extent permitted by law, U.S. support for guerrillas in Nicaragua.

Second, the Administration was engaged in a political struggle at home for support for the Contras. Despite great efforts by President Reagan, the American public was evenly divided on the question.

Third and finally, the United States was sued by Nicaragua in the World Court; the Court's procedures required in 1985 that the United States decide whether and how to participate. The Administration decided not to appear in Court. It strongly believed that the Court had no power to decide this case, and that, in any event, the court was hopelessly biased and politicized. In the Administration's view, the Court hardly deserved to be called a court at all.

At about this time, the State Department decided to issue a paper setting forth the facts of Nicaraguan policy and aggression. All relevant departments and agencies contributed to this paper. Those who worked on the paper at the State Department were frustrated at the dearth of usable data. We knew the Sandinistas were subverting their neighbors. But we had little open smoking gun data. To use intelligence would have shut down our information flow for months. We worried that the need to protect sources and methods would end up preventing the country from supporting a policy designed to address the dangers revealed in the intelligence. What good was such information if one could not use it? This question probably has dogged policymakers forever. And probably will continue to do so. The open use of such information is a principal issue concerning intelligence, and it must be addressed by the National Security Council.

"Those who worked on the paper...were frustrated at the dearth of usable data....To use intelligence would have shut down our information flow for months. We worried that the need to protect sources and methods would end up preventing the country from supporting a policy designed to address the dangers revealed in the intelligence. What good was such information if one could not use it?"

I should perhaps say a word about the National Security Council (NSC). It is something of a mystery for those who have not been there. It also is mysterious even for people who have studied it closely. The NSC is best understood as a forum in which departments and agencies with overlapping

jurisdiction and responsibility in the foreign policy and national security area coordinate advice to the President and the implementation of presidential decisions.

The NSC staff has principal responsibility for the day-to-day management of the system. The chief check on the staff's power derives from the fact that the Secretary of State and the Secretary of Defense are statutory members of the council and in a position to demand honesty and impartiality from the staff. In a real sense, the staff serves them as well as the President.

The NSC was created in 1947. Under President Richard Nixon and his successors, the NSC has become a central institution for presidential management of foreign and national security policy. It also has become the model for interdepartmental coordination in other areas. Part of its coordinating responsibility is discharged in the national security information area.

From the NSC perspective, information security becomes an issue in a variety of policy contexts. The ordinary context—if any context at the NSC is ordinary—concerns the creation of classified documents. As you might expect, in this context one deals with humans, not angels. Some NSC staff historically have overclassified information on the grounds that nothing they do could possibly be unclassified or "merely" Confidential.

Apart from this aspect of its work, the NSC often deals with ephemeral classification. For example, papers created for President George Bush's meeting at Malta with President Mikail Gorbachev might have been highly classified the day before the meeting but unclassified the day after. Of course, no one had the time or the inclination immediately to review those papers for downgrading or declassification.

A third context of the NSC role in national security information has developed because it has come to mean more in the public mind than a bureaucratic corral. This role for the NSC owes much to the late President Nixon and his National Security Advisor, Dr. Henry Kissenger, who transformed the NSC and altered its relationship with other departments and agencies. In the earlier Administration of President Lyndon Johnson, for example, the NSC did not clear documents. The National Security Advisor at the time was fond of responding to Government colleagues who asked for NSC concurrence in documents by saying: "There is only one person here who can clear anything, and if you really want me to ask the President, I will."

President Nixon changed the NSC into an important policy creator and implementer. He used it as a substitute State Department. The handling of Iran-Contra matters by President Reagan's Administration just confirmed public and congressional belief that the NSC had become much more than a structure through which decisions are made, but rather had become some kind of secretive (if not secret) presidential arm. As a result, the NSC itself has been at the center of battles regarding future policy with respect to the definition and protection of national security information.

From the perspective of the NSC, national security information policy should reflect two concerns. The first derives from the need to protect the national security from damage arising from unauthorized disclosure of classified information. The second concerns the President's constitutional prerogatives: Whatever the information policy is, it should be presidential, not legislated. This view is consistent with Supreme Court decisions affirming that the President defines national security information and establishes policies to protect it.

"[N]ational security information policy should reflect two concerns....[F]irst...[is] the need to protect the national security from...unauthorized disclosure....The second concerns the President's constitutional prerogatives...Supreme Court decisions [affirm that]...the President defines national security information and establishes policies to protect it."

In performing its roles as honest manager of the interagency coordination process, the NSC has to broker disputes between departments and agencies regarding information security. These disputes often pit narrow interests against each other.

An example involving communications rather than security conveys the point. In connection with a system that was under development for a

special application, a number of departments and agencies had to work together at an operational level. Each insisted on sending not only its own representatives, which was desirable, but also communications equipment, no matter how redundant they were. Obviously, this resulted in a multiplicity of communications systems allowing each representative to talk to his or her home base without using another's equipment. The result was an unnecessary logistical nightmare. Similarly, in the information area, one department or agency will often insist on its interests prevailing over the larger interests of the team.

The NSC is supposed to take the President's perspective, bringing the broad national interest to bear. In doing so, the NSC performs in the information security area the same function it provides in other policy areas. Thus, it brings the policy perspective to what often is a technical question concerning the relationship between this or that piece of information and national security narrowly conceived.

We are now in the midst of a spasm of reform of the classification system. Despite being away from Washington, I have retained a few sources who have provided me with a sample of opinion and an indication of what is afoot.

"The pressure to reform national information security policy really does not recognize important realities....Any rational program of classification review...is going to require time and money to be effective — much more than anyone so far has been willing to devote to it."

The pressure to reform national information security policy really does not recognize important realities. One of them is that the State Department typically sends out some 500,000 cables a year. Not all the cables are classified. And this number does not include cables received and memoranda prepared. Any rational program of classification review of this quantity of paper is going to require time and money to be effective — much more than anyone so far has been willing to devote to it.

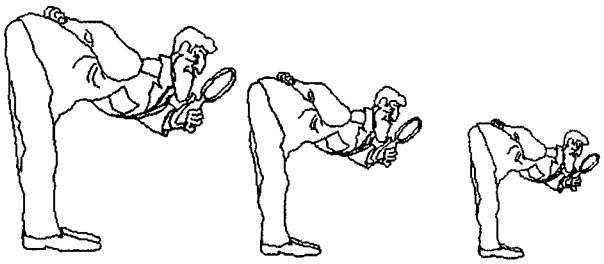
The volume of paper and the demands for rapid declassification require more than just a new Executive Order, however much each Administration seems to require one. We need a better informed public. The public needs to understand the contours of national security information and the institutional checks against abuses. Such understanding is the basis of public trust, and the system requires public trust to work. That trust has been battered over the decades of the Cold War; this is simply one of the many prices we have paid as a country.

We need to restore trust so all citizens have confidence that national security information truly does mean the people's secrets. If we do not do this, our country will get weakened national security and bad government. The weakened security will come from diminished capacity to know what our enemies are up to and lesser ability to take appropriate measures to protect ourselves from them. And increasingly bad government processes will come from a pervasive view that everything leaks.

"We need to restore trust so all citizens have confidence that national security information truly does mean 'the people's secrets.'"

The result of weakened security and bad government must inevitably be a deterioration of the policy process: officials increasingly will not allow notes of meetings, and there will be growing tendencies to pull punches in memoranda of advice. I saw these developments during my years in Government service. They serve no one's interests.

Nicholas Rostow is Associate Processor of Law and History at the University of Tulsa in Tulsa, Oklahoma.



Managing Your Management: Hints, Tips and Lessons Learned

Joseph A. Grau

This is a collection of hints and tips for getting your organization's managers to play active constructive roles in your (actually, *their*) security programs. Some of these suggestions deal with style, general approach, and specific tactics. Others focus on *positioning* yourself to be able to *influence* their performance, rather than on the influencing process itself. Not all of them will work for everyone, and not all of them will work in every situation. But I believe they are all worth considering.

In presenting this list of ideas, I am going to take a shortcut. Refer to the top manager in an organization as "the boss." "The boss" might be a military officer, a senior civilian executive, or a corporate chief executive officer or chief operating officer. Whoever "the boss" is — military or civilian, male or female, in government or in industry — his or her words, actions, decisions and attitudes can have a dramatic impact on the quality of our security programs. We need to find ways to make sure it is a positive impact. Here are my suggestions.

1. Be Positive

Approaching managers with the built-in assumption that they do not care or will not respond positively to security is disastrous. There is a lot of truth in the idea that people rise and fall to meet our expectations. If we communicate an exception that bosses will react negatively, we set them up to do just that.

- *Never apologize for your program.* If you believe that the security program is an important part of the organization's life, act like it.

- *Do not over-sell.* You approach the boss with a request for support, and immediately give him 4,216 reasons to grant it. The boss may have quickly seen the logic of the request and was predisposed to grant it. But your obvious anxiety makes him do a mental double-take. He begins to doubt his immediate reaction.

- *Do not under-request.* Our pessimism about what we will be able to wring out of management sometimes leads us to minimize what we ask for. That ensures we will never get more than the minimum. Say you need an hour of a manager's time for a presentation. But you know this manager is a very busy person and cut down your request to a half hour. Not enough to do the job right, but better than nothing, you figure. Your chances of getting an hour are now 0. What would they have been if you had asked for an hour? I do not know, but I do know they would have been better than zero!

- *Do not provide ready-made excuses.* When you start out a request with "I know your schedule is very full, but...," you are just asking to be told, "I can not. My schedule is very full." Saying "I know money is awfully tight these days.." will almost automatically bring a reply, "we cannot afford it. Money is awfully tight these days." Let the boss come up with reasons not to honor your request. Do not provide them yourself.

2. Talk opportunities.

Providing support to the security program is not a favor management does for the security staff. It is an opportunity for the manager to promote quality in a function for which he or she is responsible.

3. Emphasize pay-offs, not requirements.

Managers tend to be even more resentful than most people of things we do because "the book" requires them. Downplay compliance and highlight benefits.

4. Internalize the security program.

In order to promote ownership of the security program by managers, present it as a necessity for doing business rather than as a set of externally-imposed requirements. Position it as something *we* need, rather than something *they* say we must do.

5. Focus on the organization rather than the program.

Most managers (with the exception of technical folks thrust into management roles) focus their attention on the organization itself, with various programs seen as pieces of the whole. They are usually more responsive to discussion on the organization rather than a specific program.

6. Explain collateral benefits.

Many things we do for security's sake also have other benefits for the organization. If we make sure managers know about these, it facilitates acceptance of and investment in the measure. For example, many of the same measures that help keep confidential on a computer are important contributors to virus protection. Visit controls required by classified programs can also help promote a more crime-free and orderly workplace. Classified document accountability systems can contribute to easy retrievability of information. In a more general sense, establishing a climate of security which protects classified information will also heighten protection for other information which must be protected if the organization is to stay healthy — like corporate proprietary information and trade secrets.

7. Do not assume knowledge or understanding.

Just because a top manager is a top manager doesn't tell you beans about his or her knowledge or understanding of the security program. This is especially true when it comes to knowledge of basic program concepts. If they were ever taught these concepts, how long ago was it and how often have they been reminded of them? What are the chances they will recall them? If understanding the concept is necessary for understanding your request or learning what you're teaching, better make sure the basic understanding is there.

8. Be specific.

Do not just ask you management to "care" or "show support" or "put command emphasis" on security. Ask the boss to do specific things. Providing management support to a security program is a role, and we should identify specific tasks to be performed.

9. Adapt to the manager's style.

By the time they reach senior positions, many people have adopted a "style" of learning and management that they heavily favor. Sometimes, they get so attached to this style that we mere mortals would call it a "hang-up." For instance, some managers see themselves as "strategic thinkers" only concerned with "broad issues," while others want every detail laid out for them. Some favor learning from print; others want live discussion of issues; some are into charts and graphs. Learning about and accommodating the manager's style smoothes communication. Bucking the tide can cause credibility problems and build resistance to your ideas. Failing to learn can leave you ineffectual and frustrated. Members of the manager's staff can often be valuable sources of information and guidance.

10. Be time-conscious.

Many managers operate under heavy pressure and demands for their time. And even those who do not often act like they do. Being busy is something of a status symbol for many managers. Accommodate this by being careful to use your time with the manager profitably. Never allow the manager to suspect his or her time has been wasted. That translates too easily into the perception that security itself is a waste of time.

11. Speak managementese.

A basic principle of teaching is the benefit of establishing a close connection between what you are teaching and the student's work setting. Using the language (well, OK..."buzz words") of management sends a signal that what you have to say has relevance to their duties and concerns. It also helps you establish credibility.

12. Be part of the management team.

Like birds of a feather, managers tend to flock

together. Managers tend to have a higher comfort level when dealing with other managers who are on the same team. This facilitates communication and learning. Also, the more managers view you as part of the organization management team, the more readily they will accept your recommendations as being in the organization's best interests. Some specifics —

- *Know the organization.* The more you know the organization, the better you can talk to managers in terms of their specific situations and concerns.

- Be aware of current issues. Keep current on the various influences that are impacting your organization — things like down-sizing, employee empowerment, privatization, market trends, and fiscal uncertainties.

- Participate in management. Invest some of your effort in management activities, even if they do not directly impact the security program. Get involved (or, at least, show interest) in management initiatives like TQM and employee wellness. One government security manager became a regular instructor in his organization's TQM training, which was presented by line managers. His staff reported a noticeable change in the ease with which they could deal with managers in other elements.

13. Establish a viable presence.

You want your top management to perceive the security program as an integral part of the organization's operation and of their management responsibilities. Keeping yourself visible to management can contribute to this, besides raising the perception of you as part of the management team. For example, attend and have something to contribute to staff meetings. Do not be one of those people who sits along the wall of the conference room and fervently hopes nobody asks you anything. Send a signal that security is something management needs to hear about.

14. Talk trade-offs and least cost solutions.

Managers tend to be very conscious of and concerned about resources. When presenting new or changed requirements and your plans for meeting them, be sure you are ready to discuss what alternatives you have considered and why you selected the one you're presenting

15. Do not be a habitual bearer of bad news.

People tend to generalize their perceptions of us to our programs. If the only time a manager sees the security officer is when things go wrong, security becomes perceived as a program where bad news is the norm. The result? Avoidance. Yet there are security officers who hesitate to "bother" the boss unless it's urgent — which usually means just after the dam has burst.

16. Learn to deal with the staff.

Almost every manager is surrounded by staff, be it a single secretary or administrative assistant, or a whole battalion of aides, executive officers, administrative officers, and the like. Staffs exist to enhance the effectiveness of managers by providing effective communications, minimizing distractions, and organizing the flow of information to and decisions from the manager. In many organizations, staffs also perform other, we-intentioned but less legitimate functions — like protecting the manager or advancing their own views and objectives.

- Distinguish the manager from the staff. As you form your perceptions of the manager's attitudes and behavior, do you best to sort out the influence of the manager himself from that of the staff. We have all run across cases where our perceptions of a manager's wishes or instructions were clouded, colored, or even twisted by the "spin" put on them by the staff. Be alert for this; reorganizing it can save a lot of trouble.

- Learn how the staff operates. Watch the staff carefully. Figure out who has the power to control what. Who actually controls access to the manager? Who has the greatest influence on how the manager spends his or her time? How does the flow of information to the manager work, and who is involved? Which staff members have the greatest

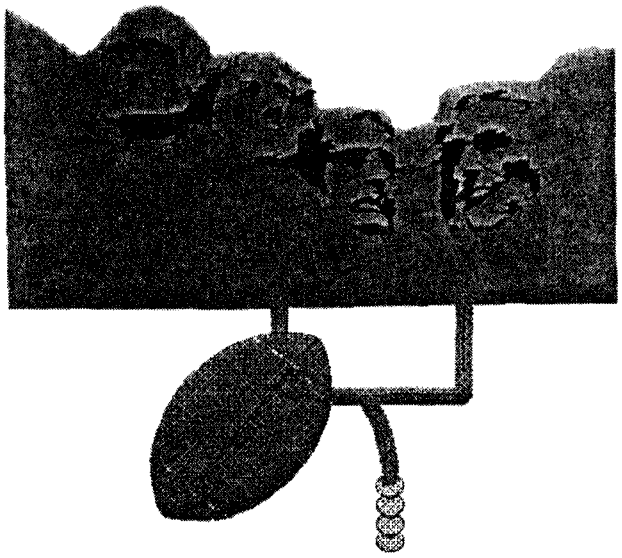
influence on the manager's perceptions and opinions? Are there issues on which the manager tends to defer to a staff member's judgement? Whose?

- Cooperate. Staff members often work in a very high-pressure environment, and sometimes feel defensive if a "we-they" atmosphere has developed between them and the line managers. They tend to be quick to recognize and appreciate someone's willingness to cooperate with them. They will often be most willing to pay back that cooperation, making it possible to turn into very influential allies for your security program.

- Build alliances. Let the staff members know that you value their ability to help you deal effectively with the manager. Ask for their help. Say "thanks" when you get it. Do not just ask them to do things for you; ask for their advice about how best to get things done.

That's the end of the list. I have just exhausted my small supply of ideas. If you have suggestions for additions to the list, I'd be pleased to hear from you. Or — better yet — give some thought to putting together an article of your own to share the benefits of your experiences. The ability to influence effective management is a skill — something we learn from our own experiences and the experiences of others. Learning it quickly and well can be of tremendous benefit to our security programs and a key factor in our professional survival.

Joseph A. Grau is a member of the Information Security Team at the Department of Defense Security Institute and a member of the Board of Directors of the National Classification Management Society.



NATIONAL SECURITY: A POLITICAL FOOTBALL?

Christina M. Bromwell

Information security professionals have been very busy the last 18 months. The Presidential Review Decision (PRD)-29 Task Force and the Joint Security Commission (JSC) were created and directed to re-evaluate the current security system to ensure that proposed new policies and procedures reflect perceived changes to the threat and to develop a new system that reflects those changes. This was interpreted by some as mandate to develop radical rather than evolutionary changes to the current security system. Not too long ago, the word "radical" was viewed as a "four-letter word." Now, it seems to be in vogue and being as overused as Bart Simpson's "COOL." (Interesting that both words were popular during the same era.)

Maynard Anderson's article, "Information Security Program: Is the Future Behind Us?," 1 provides the reader an opportunity to think about the underlying policies of a program which has evolved over the last 40 years and causes one to question why the information security program is held hostage to the ebb and flow of administrations. Too little time has been spent developing a vision with goals and milestones, and too much time spent reacting to unplanned situations. Unfortunately, parts of the article reiterate some of the same criticisms which have been made by others during the PRD 29 Task Force and Joint Security Commission reviews.

Accusations that individuals involved in information security are resistant to the changes proposed since May 1993 because the system would become more efficient and, therefore, threaten their jobs, are false. The majority of resistance came because the practitioners recognized, where the politicians would not, the **inefficiency**, of their proposed system. Proposals to declassify all information in 10 years and have one level of classification are not going to cause loss of employment. It is easy to turn the argument around and say that jobs and bureaucracies were created because of the proposed changes.

The assertion there is "a widely accepted conclusion that the information security program is inefficient" was first stated at the inception of the PRD-29 Task Force in May 1993, and has been repeated like a mantra by the Joint Security Commission staff. No proof, however, has been proffered of this overwhelming condemnation of the current system in the way of a survey with accompanying statistics. This conclusion may be based on no more than interviews with a few select people who already have an ax to grind and believe it is politically correct to criticize all that preceded the current Administration.

Another often repeated statement is that security people are risk averse. I would argue that the owners of the information, original classification authorities and program managers, are managing risk to their programs when they determine the value of their information, the threat to it, and how to protect it. You cannot, on one hand, make individuals responsible for protecting something and then, on the other hand, tell them not to protect it to the best of their ability. I believe risk management is currently accomplished by those agencies which have developed written security classification guides. Owners of information thus codify their thought process in determining what to protect, how, and for how long.

1 Viewpoints, Volume 1, 1994, pp. 1-9

The judgement that, because of poor classification standards, "original classification authorities continue to decide that information needs protection without providing adequate justification" tars all Executive Branch agencies with the same brush. A more precise review of this issue needs to be conducted. While no agency would come away with an "A," many would not fail. Part of the misperception about classification standards stems from the fact that some management officials are so removed from the working level that they do not understand why certain information is classified; therefore, they assume it should not be. Additionally, some agencies do not codify their original classification decisions, which probably adds to the confusion. Something that everyone needs to remember is that the existence of the Soviet Union was not the only reason for classifying information, and its dissolution should not be an overwhelming justification for declassifying information.

Saying that "a new classification system will not come from within" contradicts comments made on page 7 of the article which criticized the information security reviews as ignoring the input from the practioner and flies in the face of our own democratic system versus that of a dictatorship. If the people within the system are not the creators of it and do not agree with the principles, it will sooner or later fail, as have other systems imposed from without.

The article also claims that "classification levels are arbitrary, artificial designations of information sensitivity devised...to satisfy desires for exclusivity." One might conclude from this that the majority of information is classified at high levels, but this is not supported by the numbers presented in the last two Information Security Oversight Office Report to the President. In fact, the large volume of material currently classified at the Confidential level contributed in part, I believe, to the decision, so far, to retain Confidential as a classification level. If it is believed that agencies, especially those in the intelligence community, are classifying information at too high a level, a more surgical correction of the problem is required.

The criteria suggested for consideration in determining whether to classify information are already listed in various policy documents. DOD 5200.1R states that: reasoned judgement must be exercised,... [a] positive basis must exist for classification, ...advance planning is necessary to assure adequate protection for the information...and eliminate impediments to execution or implementation,...advantages and disadvantages of classification must be weighed,...each item of information that may require protection shall be identified,... [and] state of the art in other countries and extent of knowledge by others must be considered.

The Department of the Navy's Information and Personnel Security Program Regulation states it even more clearly: "In arriving at a reasoned [classification] judgement, the following factors should be considered:

a. The degree of intended or anticipated dissemination or use of the information....
b. Net national advantage....
c. Lead time advantage....
d. [C]ost of classification in terms of time, money and personnel and whether the cost of protecting the information might impede or prevent attainment of the program objective....
e. [S[tate of the art....
f. The appearance in the public domain...."

If rules and standards are not implemented as intended by all agencies, it is the fault of the overseers. It is also an indication that enforcing current requirements is a better answer than imposing an entirely new system with no assurance that it will be implemented any better.

When we discuss value of information and the potential for damage if it is disclosed to adversaries, it is important to remember there is a difference between national interest and national security. If information if of value to the national security, it would seem to follow that it requires protection because of the potential for some damage if it is known by someone who could cause it to have less value to us. Hence, it would seem that "value" and "damage" are interlocked and it is illogical to try and determine either one without knowing the other. The following definitions demonstrate that.

VALUE:	Worth in usefulness or importance to.
PROTECT:	Keep from harm.
HARM:	Damage.

I endorse developing security classification guides for information to be classified. Doing so exercises discipline in decision making, both for the original classifier and the derivative classifier. Those agencies which argue it is impossible to do so for their information may learn from those agencies that have them. During the public hearings held during the PRD 29 Task Force review, the special interest groups complained primarily about the agencies that do not have security classification guides.

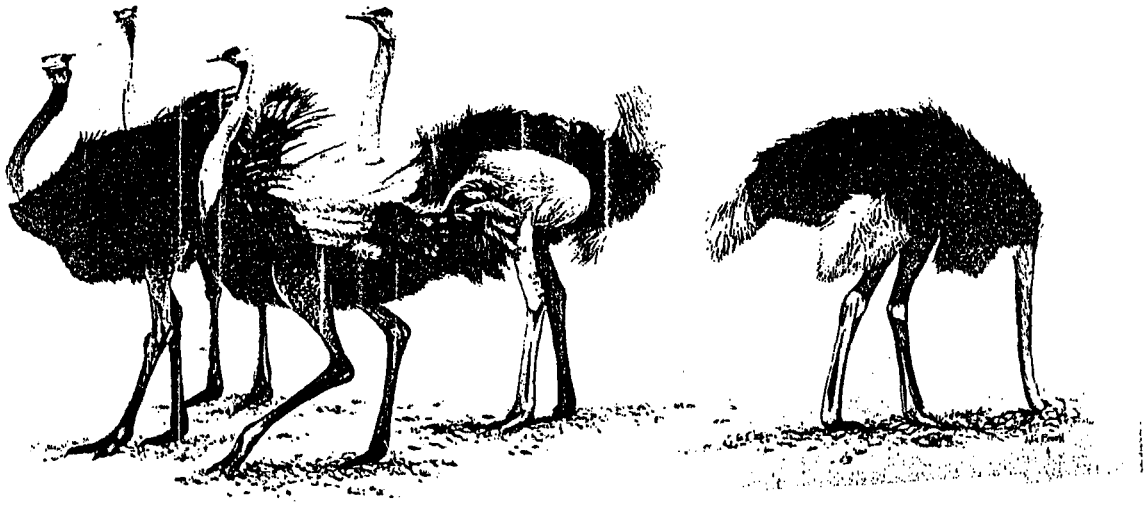
Finally, one must question the drive to limit classification to a finite number of years, especially when that number of years is shorter than the anticipated life span of our weapon system or military operation. The article, "An Engineer Looks at National Security Policy,"[2] explains clearly the difficulty with this approach. That author's explanation echoes the same argument presented to the PRD 29 Task Force and the JSC regarding the duration of classification issue.

National security--both policy and procedures--should transcend political party platforms. You can't "reinvent" something that has "evolved." I contend that **the current system is not broken.** there are aspects of implementation which can be improved if the information security professionals are given the time to actually "think things through." So many security policies and procedures seem to be dreamed up overnight in Washington, D.C. because there is little acknowledged leadership in this area and everything becomes a crisis. Such leadership will not come from political appointees; it must come from career professionals.

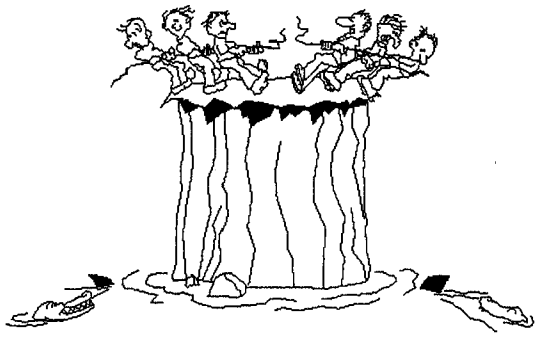
[2] Viewpoints, Volume 1, 1994, pp. 11-15

Christina M. Bromwell is Head, Classification Management for the Department of the Navy and served on the Presidential Review Decision - 29 Task Force.

When you ignore Security...



You expose vital assets!



Meeting the Challenges of Change to US National Security

Maynard C. Anderson

A long time ago, someone said that the biggest fool can ask a question that the wisest man cannot answer. In one sense, I feel like that fool these days because I keep asking questions that seem difficult to answer. Today, along with asking some questions, I'm going to talk about some challenges we face in the next few years.

Many of the challenges to the integrity of our things of value are directly related to the strategic conditions of our world. They are the challenges of change that underline the stress and strife that we must understand for decades to come -- The "New World *Dis*order," as Bob Gates has called it.

In the early part of the 19th century, Alexis de Tocqueville, in the first volume of his Democracy in America, talked about the intellectual links between the most distant parts of earth, and the diminishing difference between his contemporary Europeans and their descendants in the New World. Today, it is perhaps Tocqueville's broader vision of the nations "steer toward unity" that is his most prophetic insight.

Nations throughout the world, including the United States, are redefining their national interest. History, geography, and economics are all things that contribute to the definition. But, it is not a mechanical process. National interest is a product of human decision. That is why mistakes are made, and that is why reform occurs every so often.

Now, we face the challenges of adjusting policies and practices to world changes brought about by political anomalies, new economic and military alliances, the threat of nuclear proliferation, continuing technology transfer, and declining resources to meet these and other new and different tests.

The strategic shape of the world is better than it has been in this century and perhaps for many centuries. There is a global economy and large amounts of man-made and natural wealth cross borders previously closed by political, ideological, or physical barriers. The North American Free Trade Act (NAFTA) is an example of profound change in our own hemisphere.

Our interests in virtually every area of the world--Latin America, Africa, the Middle East, and Asia--involve assuring new democracies, market economics, stable societies, and an end to weapons of mass destruction and their delivery systems. We hope for the political and economic unification of Europe so it can defend itself.

Along with this global economy, there is an information revolution. Information continues to become more important to our goals and objectives in this different world -- both information protection and its dissemination to policy makers, planners, military commanders, economists, coalition builders, humanitarians, and peacekeepers. And to the citizens of our Republic.

There is also a resolution in military affairs in terms of a collection of new and emerging technologies that will transform the nature of war.

Despite my assessment of the world's strategic shape, it is not devoid of risk quite yet. The United States remains the object of unwanted attention by other nations, and vulnerable to the apathy of its own citizens.

In 1990 Senator David Boren, speaking to the National Press Club, expressed his belief that the gravest threat to the future security of this country is our failure to adjust out thinking to all the changes in the world around us. He recalled Einstein's

comment, soon after the atomic bomb was detonated for the first time, when he said, "Everything in the world has changed except our way of thinking." Boren also reminded us that one of the things we must guard against is the tendency of bureaucracies to sanctify the present and ignore the future. Both of those admonitions remain valid in 1994.

This New Globalization, characterized by international sales, cooperative research and development and production programs, joint ventures, mergers, acquisitions, and alliances, has become the dominant trend in the industrialized world's defense sectors. In 1988, the Aerospace Industries Association reported the fact that "the internationalization of aerospace is the increasing trend toward business relationships that cross national borders."

Costs of developing systems are rising, but U.S. Defense spending is diminishing. Defense firms logically seek partners as well as the most economical sources for raw materials and technology. Most industrialized nations produce advanced technologies of one sort of another; The United States has no monopoly on progress. In our society, the result of these trends is tradeoffs among defense and social programs at home and integration of the national with the international economy.

In this post-Cold War era, United States military roles and missions are being changed. The defense establishment of military and civilian personnel is adapting to realities of the world that I have just described.

As Dr. David Carter of Michigan State University has written, "The threat button of national security is changing from our pathology of scorn directed at the former Soviet Union and its ideological bloc, to a complicated admixture of "ally-competitors."

In this world, every place name from Granada to Panama, Iraq and Kuwait, Somalia, Haiti, and Bosnia, brings a different set of images along with a different set of military assumptions, techniques, and perceptions of victory and defeat. The United States Government is no longer planning for "total mobilization" for a global war. The real threats to our homeland are not from military enemies -- attacks and wars as we have known them in the past. And, the nuclear weapon that is most likely to explode on our shores might be delivered in a panel truck rather than by any form of strategic missile.

In addition to being trained and ready to defend the territory of our Nation, the United States Armed Forces must be prepared for roles in regional conflicts. We no longer have a single large enemy; but the number of smaller potential adversaries cannot be fixed. Our forces will continue to be engaged in international crises as long as we remain a "superpower," whether for reasons of national values and ideals or simply as a preferable means of deterring or defeating aggression abroad in cooperation with friends and allies.

The primary reason for the military's existence is to deter war and attacks on the United States, and if deterrence fails, to defend our nation and defeat any enemy. Our national military strategy continues to support this premise. Peacekeeping, humanitarian, and other changing roles and missions are secondary uses for forces that are bought and paid for, equipped and trained, to defend this nation.

These peacekeeping, disaster, and humanitarian relief efforts fall under the new category of "operations other than war," which was first called "non traditional missions."

In these new and different circumstances, we must ask whether the traditional ways are adequate to determine the eligibility of our personnel for access to classified information. Are the traditional ways of protecting our information useful? These are two questions for the wisest man or woman!

Sir Henry Royce, co-founder of Rolls Royce, once said, "Strive for perfection in everything. Take the best that exists and make it better. If it doesn't exist, create it."

I believe those should be our guiding words today. Situational economics requires that we use what works, but in ways that meet current demands. World changes force us to find some new policies, procedures, methods, and techniques to do our jobs.

Common sense tells us there are things of value that need protection; but there are things of value that must be shared. The right combination of protection and sharing will promote our national interest.

I am pleased to be able to cite one extraordinary

example of information protection and sharing today. It is a system that supports multinational, coalition, alliance cooperation in United Nations actions, humanitarian efforts, peace-keeping operations, relief activities, NATO actions, and bilateral schemes in Somalia, the Federal Republic of Yemen, Macedonia, and Rwanda, among other places.

It is the Linked Operations Intelligence Centers Europe (LOCE) system that provides U.S. forces, NATO forces, and other international and national allied military organizations with near real-time, correlated situation and order of battle information for threat analysis, target recommendations, indications and warning, and collection management cueing. The system combines the latest automated processing and communications equipment to handle information of value.

Using an enlightened management approach, LOCE controls and disseminates unclassified through secret information from, to, and among an extraordinary group of multinational users. It is a precursor of systems to come and is, inadvertently, a reinvention of some intelligence processes that highlights prudent use of information. It is a customer-oriented (not a producer-oriented) system that continuously demonstrates its benefits to its users. It is one that demands emulation.

As we struggle to meet new, unfamiliar challenges with reasonable, economical answers, the challenges of a global economy, an information revolution, and changing military roles and missions affect our vision of what future information security programs must look like.

There are other factors of influence that can not be ignored. For example, acquisition reform activities will affect industrial security for a long time.

A new generation of computer-skilled criminals is likely to continue to confront our security systems.

An increasingly large group of employees, fearful of becoming unemployed or disgruntled because of lower pay or loss of benefits, may well jeopardize the security of information and personnel as well.

Public apathy and cynicism certainly will come to bear.

Cokie Roberts of ABC News and National Public Radio says that trust in government and in all institutions (except pharmacy and pharmacists) is lower than it has ever been. The trend is to "throw the bums out."

Her brother, Thomas Boggs (Patton, Boggs & Blow) recalls that, in 1967, there were about 17 registered lobbyists in Washington. In 1994, there are about 16,000. They are now a major source of information to public policy makers because of Congressional distrust of the departments of government. Next year, 50% of the Congress will have been elected since 1990.

Distrust on the part of the public and the Congress with an uninformed Congress relying on lobbyists for information, combined with policy-formulating officials in government departments who are generally not experienced and who serve for short tenure, all add up to a conclusion that improving information security is *up to you.*

Yet, the National Performance Review (NPR) and the Joint Security Commission (JSC) review, took place so rapidly that meaningful consultations concerning recommendation implementations with career professionals, managers, and executives could not take place. Nor was it possible for professional associations to examine the recommendations and provide worthwhile comments.

As government leaders were saying that government is broken and not working, they really were breaking the morale of the government's highly trained corps of professionals and managers -- the very people who have the responsibility for implementing change.

Actually, the JSC has recommended a new hierarchy that competes with the one in place. We were taught at the Federal Executive Institute that an organization containing incongruous hierarchies produces a dysfunctional system marked by chaos. It produces a pathological system characterized by stress and strain: unhappiness, low morale, declining productivity, and unfocused employees who are unable to concentrate on serving the customers.

The administration has been told that there is no way a plan can work unless the people who have responsibility for implementing the plan are included in designing the implementation plan.

Unfortunately, Bob Stone, who purports to represent the career Federal executives on the NPR, has carried a negative message: "You need horror stories to make a case for change. People won't accept change if there is nothing wrong." Well, I do not think you have to destroy something to make it better.

I do not think we have yet established a base--political, economic and military--on which to build. There has not been articulated a larger strategy on which to build an argument that rationalizes why you need the ingredients of security countermeasures today and tomorrow. We need a floor that forms a base for the minimum things you are required to have in this world. It is different from the one we have lived in. We are a little bit unwilling to split ourselves from the past and admit that we really do not need everything, or, we need things that are different, or, we need to find a combination of the two that will work tomorrow.

The critical question for the wise man or woman is -- What do we do now?

Part of Thomas Paine's Philosophy of Revolution included the thought that there is always opportunity to start over again. We should start again remembering that we must devise a program for tomorrow, not for today. And, it is not a simple situation. Alan S. Blinder, a Princeton economist, says "There is apparently something in the American character that rejects any remedy too complex to be emblazoned on a T-shirt," We must get beyond the T-shirt.

I have always believed that most innovative and radical proposals come from the bureaucracy if there are no artificial impediments to their proposition. Experience tells me that our practitioners often quite accurately forecast what will be needed.

So, your mission if you choose to accept it, is multifaceted.

You must contribute to a long-range information security program that incorporates handling procedures for all information of value; puts someone clearly in charge who actually controls the process of information protection designation; controls protection duration; and *facilitates* information dissemination for our Government's benefit.

The future program must adjust its strategic course to incorporate all disciplines of security and create synergy among those disciplines. It should begin with an executive order entitled "National Security" which sets prudent standards for protection of information in government and industry, as well as the standards for clearance and access of personnel who must know the information. It must include reciprocal oversight mechanisms.

The program should be centrally managed but locally administered, allowing flexibility of application.

You must carry a message to your constituency that is current and objective. You will have to persuade people to take action that is needed. That persuasion will require truthful advertising.

- People must be made to understand security intellectually;
- They must believe in it emotionally; and
- They must be aware of it professionally (and transparently).

Those are some of the objectives we tried to achieve in the National Industrial Security Program (NISP).

I would think that NCMS would want to increase programs of education and training and research; develop teaching materials; and perhaps produce a curriculum resource package in information security for the future.

For example, "value" is a legitimate criterion for information protection. The JSC report even mentions it, but then mixes the criterion with threat. Information is protected because of its sensitively (read:value); the means selected to protect it may be threat dependent.

Value is often thought of as an abstraction, a relative consideration in the "eye of the beholder." But, value is absolute. It is determined by the reality that ownership of information involves ownership in an enterprise--the U.S. Government. Value is governed by the practical measures that govern the process of government. It inherently implies the need for protection depending on its owner's assessment--which is real and provable.

In the absence of understanding what they own, originators of information have difficulty assigning it value. They surely can not figure out what damage might be caused by unauthorized disclosure.

Your customers must be trained and educated to understand that any piece of information is worth only so much for a certain period of time. That is value, and it is absolute.

And, information does not lend itself to nebulous characterizations like "NORMAL," "GREATER THAN NORMAL," or "LESS THAN NORMAL."

Information security systems must be devised to fit the management structure of the organization(s) they support. For example, I have advocated the formation of executive security committees in the organizations served (particularly industry), and I continue to believe they are necessary.

In each company in the United States that has a classified contract with the United States Government, I would like to see an executive security committee composed of some members of the Board of Directors, the Chief Executive Officer or the Chief Operating Officer, and the firm's security director. The existence of that kind of committee would demonstrate the participation of corporate officials in the security program. It would be a form of security awareness by leadership example and would impress on the company's employees the necessity to participate in the security program.

An executive security committee should routinely receive the briefings by industrial security representatives at the beginning and end of each government inspection. The committee would serve as an opportunity for senior management to understand the requirements of the security program. The committee would serve as the focal point for intelligence briefings, for receipt of counterintelligence and threat information. The committee could take immediate action on the information received or, if necessary, recommend actions to the Board of Directors. The committee would give the Security Director a recognized level of authority within the firm.

I believe that executive committees would be of great help in ensuring protection for those emerging technologies that will be the prime objects of our security efforts in the future. I would think the NCMS might want to consider supporting their formation.

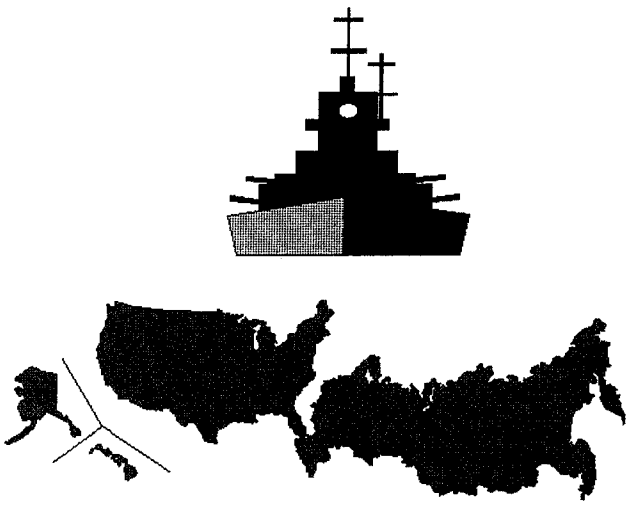
I believe that senior leadership involvement in the security management process would result in great integration between personnel management and personnel security. That would lead to improved understanding of the needs of the employees and possibly opportunities to deal with disgruntled employees before they take revenge possibly in the form of disclosure of classified information or the sale of trade secrets.

In order for US companies to compete in the international market place, let alone at home, senior executive support for security programs throughout industry is essential. Their involvement in security planning will result in more appropriate spending on security countermeasures. An executive security committee would move the defense contractor community toward more efficient and cost-effective security in industry, one of the goals of the NISP.

Despite our best attempts at forecasting, none of us knows what the future holds. Consequently, we must continuously challenge the processes of security. There must be developed a system of measurement empirically to assess the effectiveness of the procedures so those of no value can be eliminated. Standards and performance objectives must then be established that focus on customer needs.

Finally, we must establish a "Security Futures Group" to examine the trends in society, politics, and economics, and alert us to the changes that will affect security. Then, we can make changes on the basis of reasoned judgements rather than on old wive's tales, hunches, emotional experiences, folklore, and personal parochialism.

Maynard C. Anderson is managing director of Arcadia Group Worldwide, a consulting firm in Arlington, Virginia. He retired in February 1994 as Assistant Deputy Under Secretary of Defense for Security Policy. This article is adapted from a speech he delivered in June to the Washington Chapter of NCMS. It retains a challenge he presented to professioanl security personnel, addressing the listener/reader in the second person.



The Demise of COCOM: Implications for the US Navy and Russian Defense Industry

Edward Keith Jackson

COCOM (Coordinating Committee on Multilateral Export Controls) restrictions on export of dual-use technology have been eased and will eventually be terminated entirely. This could negatively affect U.S. Naval Forces in the future and undoubtedly will stimulate the Russian defense industry.

While the Cold War has been won, new and different challenges face U.S. Naval Forces in carrying out their littoral warfare missions and in potential regional conflicts. In fact, all branches of the U.S. Armed Services find themselves operating under dramatically changed circumstances. As witnessed during the 1991 Gulf War, superior technology is critical to success.

Some critics believe that the end of the Cold War means the U.S. no longer needs to be concerned about exporting dual-use technology to Russia -- or to any other country. During the Cold War, the Soviet Union used intelligence organizations such as the KGB and the GRU to collect western technology for its defense industry. This remains the case today, only with new titles for some of the organizations. In fact, with the demise of COCOM, decisions on all exports are at the discretion of the exporting nation. Obviously, foreign collectors have easier access to our technology and can be more selective in what they target.

Russia will have access to a wide range of current dual-use technology. Some of it will likely be used in weapon systems exported by Russia to aggressive developing countries. Currently, no effective control regime is known to be in place in Russia, so Moscow relies on arms exports to preserve its defense industry. Therefore, with this lifting of export restrictions, U.S. Naval Forces would very well be confronted with more technologically advanced weapons on the battlefield in future regional conflicts around the world.

So, the world is not really safer. Yes, "Soviet" power is gone, but more nations possess nuclear weapons and the demise of COCOM just adds more variables to a increasingly complex situation. Currently, a new export control regime is being negotiated among former COCOM member nations. If successful, this new regime will target controlling exports to pariah nations such as North Korea, Libya, and Iraq. On the other hand, several key principles, with implications for future U.S. military planning, appear to dominate the attitudes of negotiators:

First Russia will be a member and full partner in the new regime. Second, enforcement of export controls will remain at each nation's discretion. In other words, any nation would be able legally to sell anything at will. Consider the implications!

Edward Keith Jackson. a Lieutenant in the United States Navy, serves as an intelligence analyst in the Maritime Technology and Weapons Proliferation Division, Office of Naval Intelligence. He has extensive worldwide operating experience and has authored several papers on technology issues.

Surviving Workplace Violence: A Viable Response

Mark O. Hamersly

In the case of most small businesses that possess a Facility Security Clearance-- and I'd venture to guess that would include most non-possessor facilities-- the function of Facility Security Officer goes to a person who falls into the category of non-dedicated-personnel, as it does for me. I am responsible for a number of activities within the company, and security is only one of them. Yet, when you say the word security to most people in these companies, they do not normally limit their thinking solely to concerns of safeguarding classified information. To the majority of people--and thus most of our employees--security includes many other considerations as well.

While the term obviously covers traditional concerns over the protection of classified assets and information, it also includes other issues ranging from parking lot lighting adequate to ensure the safety of employees who work late at night, to workplace safety and injury prevention, to earthquake and disaster preparedness, to threats of workplace violence. We must each address all of these concerns in the best way we can. Those of us in this business have an obligation to our people to keep them, and their workplaces, safe and secure. It is our responsibility to take care of our fellow-workers, as they are, in a sense, members of our extended families.

In my company, we conduct the normal periodic refresher briefings on Defense Investigative Service (DIS)-related issues pertaining to safeguarding classified information. We also supplement these with periodic discussions of disaster preparedness, personal security and safety, and changed conditions when appropriate. We do everything from providing lists of suggested contents for earthquake survival kits, to offering monthly firearms safety and marksmanship training. We try to offer quality information about local concerns before they become problems. For example, we provided information on snakebite to our employees more than a year before another tenant of our facility experienced a snakebite *inside* our building. We also encourage training in cardiopulmonary resuscitation and first aid. These efforts are supported throughout the company, and at all levels.

Lately, I've become concerned about a subject that has been getting a lot of attention over the last few years--workplace violence; workplace violence caused by distraught employees, by criminal activity, or even by terrorist acts. As we had several of our employees working in the Elgar Corporation facility in San Diego until just weeks before John Hansel killed two people there on 4 June 1991, this has long been on the minds of my fellow employees as well.

The NCMS-sponsored mini-seminar and trade-show held last February in San Diego featured a presentation by Dr. S. Anthony Baron, Ph.D. on this subject, and copies of his excellent book "*Violence in the Workplace*" were available for purchase. Much of the useful information he offers can be implemented with little effort in most workplace situations. I recommend the book to everyone who has concerns in this area--and that should be all of us.

I must say, however, that the most critical aspect of the issue is not addressed in any detail in his work. I am speaking of the initial, immediate, response to violent actions. I am speaking of saving lives. Unlike speakers whose presentations I have attended in the past, I am speaking not of how to handle the media response to such an incident, or of helping survivors deal with the mental anguish suffered, but rather to ensure that there *ARE* survivors to be concerned with. The question of response is the single most critical problem we face. Once we accept the reality that we cannot prevent 100% of aberrant, often violent, behavior, we must be prepared to deal with it when we face it.

Years ago, while serving as a Reserve Aviator, I took the Federal Emergency Management Agency (FEMA) course "*Emergency Management, USA*" along with the rest of the officers in my unit. Those of us who paid attention got some good information out of this course. FEMA establishes a four-phase process

for dealing with any form of emergency: preparedness, response, recovery, and mitigation. Applying their methodology to the problem of workplace violence, my concerns are primarily in the areas of preparedness and response, proper execution of which will help in recovery and at the same time mitigate the effects of the violence. In short, we can save lives and at the same time minimize the overall impact on people caught in such a situation.

But how does the small business do this? Most larger contractors have either uniformed guard force personnel in-house, or contract out this function to a commercial provider of such services. With uniformed guards to deal with right up front, a significant number of potentially violent individuals are quite likely prevented from anything more than thinking about taking some kind of action. But what are smaller companies to do? Well, I'd like to suggest a potential course of action that may bother some people. Political correctness is not my concern. The saving of lives, is.

What can those of us in small businesses do in response to acts of workplace violence? Sure, we can dial "9-1-1," and we should do so, immediately. We must, however, keep in mind the words of such professionals as San Diego Police Sergeant Roy Huntington (Feature Editor for "*The Informant*," the SD Police Officer's Association newspaper) who says "Dialing 9-1-1 just tells us where to find the bodies."

It is sad to say, but in the time it will take law enforcement personnel to respond, even in places where such response might take just a few moments, a lot of people can be hurt or killed. Also, their response may be hampered by outside forces, and lives may be lost as a result. For example, according to the San Diego *Union*, in the disastrous July 1984 "McDonald's Massacre" in San Ysidro, only four people were killed prior to the arrival of the police. Seventeen others died in the hour that followed their arrival on scene.

What else can we do; what other assets are available? How about the people working for your company? Some, perhaps all, of our employees hold active clearances which are indicators of a level of trust placed in them by the government of the United States. Some are likely to be former military members, and some may be active reservists or members of the National Guard. It is also not uncommon for some to be reserve police officers or reserve deputies. Why not utilize these resources? All of the people I've just suggested likely possess skills that can be used in such situations. An armed, qualified, experienced, mature, trusted, employee who is able to act in the best interests of the company, may well save lives. Is this a realistic, effective, and legal option? My answer to all three is an emphatic YES.

Let us look first at the proposition of armed employees as a response to workplace violence. I am sure that most people in this country are aware of the most infamous events of this nature. I have already mentioned the "McDonald's Massacre" where James Huberty killed 21 people before being killed by a police sniper. Consider also this year's Long Island commuter train killings, Post Office shootings in Oklahoma (1986), California (1989), and Michigan (1991); and the 1992 Luby's Cafeteria tragedy in Killeen, Texas, among others. On the other hand, I wonder if more than a few of us are even *aware* of the Shoney's Restaurant incident in Anniston, Alabama?

Shortly before midnight on 18 December 1991, three well-armed robbers entered a Shoney's restaurant in Anniston, and began herding some 20 employees and customers into a walk-in freezer. After locking them in, they ordered the manager, at gunpoint, to begin emptying the safe and cash registers. It was at this point that one of the robbers noticed a customer hiding behind a table. To give the manager an example of what would happen if he did not cooperate with them, they opened fire on the patron. What they could not have known, was that Thomas Glen Terry was not the helpless, scared, victim they assumed. Using the Colt Government Model 1911 pistol he was licensed to carry, he returned fire, killing one robber and critically wounding another. The third crook fled the scene.

What sets this incident apart from the others is not just that it proves that an armed individual, trained and experienced in the use of firearms as crisis management tools, can be an effective counter to violent activities. What really sets it apart, is that news of this incident never appeared on any of the three major radio and television networks, nor even in the largest daily newspaper in the entire State of Alabama. There was no news team "reporting live" from the scene, no "film at eleven." There, the good guys won for a change, yet that was somehow not newsworthy. Why? I'll leave the media politics out of this, so you'll just have to answer that question yourself.

That may be just one incident, but I can offer many more. Charles Whitman, the infamous "Texas Tower Killer," was forced to stop his shooting by a

citizen using what may now wrongly be called an "assault rifle" to drive him back. Later, a citizen given a weapon by an Austin police officer accompanied that officer and one other up the tower. The citizen was credited with saving the lives of both the officers by firing on Whitman, who could see the officers when they could not then see him.

In the disastrous 1970 event now referred to in almost every law enforcement training text as the "Newhall Massacre," four California Highway Patrol (CHP) officers were killed; private citizen Gary Ness armed himself with the weapon of one of the fallen CHP officers, and shot one of the cop-killers (something none of the four CHP officers had been able to do) before the gun ran dry and he was driven back by a hail of fire.

In another high-profile CHP shoot-out in March of 1973, career criminal Gerald Youngberg killed CHP Officer Gary Wetterling, San Bernardino County Sheriff's Lt. Al Stewart, and service station clerk Robert Jenkins. It was an armed citizen, James Mayfield, a County Supervisor and former Deputy Sheriff, who was finally able to shoot the cop-killer with his legally carried pistol, bringing the terror to an end.

There are more examples of such intervention that I could mention, but I think I have made the point. It is worth noting here that studies of criminal activity and FBI crime statistics by Dr. Gary Kleck, Dean of the University of Florida School of Criminology at Tallahassee, show that armed citizens kill more criminals than do all law enforcement officers of this nation combined, at about a 60/40 ratio. In addition, armed citizens kill or injure less than one fourth as many innocent by-standers as do law enforcement officers. The same research shows that armed citizens use handguns alone in self defense, more than 650,000 times each year.[1] Yes, armed intervention can work.

What of the potential effectiveness of such a course of action? Can engineers, word-processors, programmers, machinists and administrative staffers be expected to employ firearms and tactics appropriate to such a threat? I have given examples of how that has, indeed, happened in the past. But stop and think for a moment.

[1] "Crime Control through the Private Use of Armed Force," Vol. 35, Number 1, Social Problems 1988, and Point Blank: Guns and Violence in America, Aldine de Gruyter Press, 1993.

Many police officers receive little or no firearms training beyond their Academy experiences, and the majority never fire their weapons outside of their mandatory re-qualification sessions once each year, or perhaps every six months. I suggest that a former military member, perhaps with combat experience, who has an interest in firearms and perhaps competes in a shooting discipline such as Action Shooting or Practical Pistol competition, is BETTER able to react to violence in the workplace than the average officer.

Some of you may be familiar with the made-for-TV movie "I Can Make You Love Me," starring Richard Thomas and Brooke Shields. It tells the true story of Richard Farley, former employee of Electromagnetic Systems Laboratory (ESL), who shot and killed seven people and wounded three others, including ESL employee Laura Black--the woman who had rejected his romantic advances. Legislation in the aftermath of this event resulted in the first law to criminalize the act of "stalking" in California.

While hearing the story of this event from the then-Security Manager of ESL, and later while watching the movie, I found myself wondering what the outcome would have been had one or more ESL employees been armed and able to act. The unarmed security guard force was helpless to control the situation. If someone had been armed, perhaps their Security Manager could later have told of lives saved, rather than of lives lost, while showing slides of blood-stained walls and furniture in the speeches he gave in the years following that tragedy. It could only have helped.

On that note, a quick aside concerning liability exposure: By putting a guard force in place, doesn't that acknowledge a perceived threat? As I understand the words, guards protect, and watch persons observe and report. If there's no threat, then why the guard? If, so, and threat is real, of what possible use is an unarmed guard? I have never heard an acceptable answer to that question.

So, the option of armed employees is both realistic and effective. What about the legalities involved? I am not a member of the Bar, and I can't offer information about other localities than my own, so I will limit myself to the situation here in San Diego County, California.

First, most people no doubt think that it is the job of the Police to handle such situations. After all, it says "To Protect And To Serve" on all their patrol cars. We have already discussed the reality that law

enforcement response is such that they offer minimal potential for timely assistance when workplace violence strikes. Still, is it not the responsibility of law enforcement to protect us, the citizens of this country? Although this is the common perception, it is a misconception that leads too often to fatal consequences.

The entire body of law on this subject counters the thought that we are all due protective services via Police Officers or Sheriff's Deputies. In the case of Warren v District of Columbia Metro Police Department (DC App 444 A.2D 1), the D.C. Court of Appeals upheld a lower court dismissal of charges against the police for "negligent failure to provide police services." The Court held that "Government and its agents are under no general duty to provide public services, such as police protection, to any particular individual citizen, but, rather, duty to provide public services is owed to the public at large...." This stems from a case involving the assault and repeated rape of three women over fourteen hours. During the first hour, two of the women were on the phone with the police department, yet police response was no more than two cars driving by, and one officer ringing the doorbell, then leaving. Repeated calls brought no further police response, and they, too, became victims of public criticism.

Where, then, does the responsibility for protection rest? Where it has always rested-- in the hands of the people. Defense of self is a natural right that cannot be denied to anyone--at least if you still accept the basic beliefs of those who founded this nation and wrote the Declaration of Independence, the Constitution, and the Bill of Rights. There are, literally, volumes of material on this available in libraries everywhere. All one needs to do is look.

So, the responsibility is ours. What of a firearm, most normally a handgun, in the workplace? Many businesses do not allow their employees to possess a firearm in their workplace. Some do, however. In the State of California, it is legal for anyone over the age of 18 and not otherwise prohibited from possessing weapons, to carry a loaded weapon openly or concealed, at their place of residence, temporary residence, campsite, or on private property (Penal Code, Sec. 12026). In addition, any person over the age of 18 and not otherwise prohibited from possessing a firearm, who is engaged in a lawful business, or any officer, employee, or agent authorized for lawful purposes connected with the business, may possess a loaded firearm within the place of business (Penal Code Sec. 12031(h) and 12026). Legal questions are thus simply answered.

At this point, we have a realistic approach to the problem that has demonstrated its effectiveness and is legal. Now, the naysayers will ask, "All in all, wouldn't we be better off using licensed security guards in place of armed employees?" Wouldn't guards who are licensed under the Business and Professions Code be a preferred choice in order to be better able to defend a company against potential liability litigation? Absolutely NOT!

Think for a moment, about the security guards you come into contact with as you go about your normal activities at the mall, your condo complex, or whatever. Do they instill a sense of confidence? Do they appear to be top-notch, high-caliber (no pun intended) people? Would you feel comfortable putting your life in their hands? Generally, I think not.

Having acted as a Rangemaster for security guard firearms qualification shoots, I must tell you that, in this state, anyone who can successfully send sixty rounds down-range without inflicting major self-injury, will get a license to carry an exposed weapon as a security guard.

I took a look through the classified advertisements in the local newspaper while preparing this article. When I found the section for Security Guards, I found job offers requiring no experience. I found companies that would guarantee same-day licensing of guards, and have them working the next day. [Unarmed only; armed must wait for the final copy of their license to be sent to them by the Department of Collection and Investigative Services before they can work armed positions.] Many of these jobs, perhaps the vast majority of them, will pay just $6.00 to $8.00 per hour. What kind of people will apply for these jobs? I do not know about you, but this does not make me feel warm and fuzzy. Rather, I see it as a recipe for potential disaster.

Why go to an unknown outside source to provide guard service? By doing so, you must place your trust in their selection, training, and hiring of employees who will be assigned to your facility. Any guard placed in your facility by a commercial security firm is an unknown to you, a variable over which you have no control. Why not take a known, trusted, employee who has a background or training in firearms and security (most FSOs should qualify, along with many of their staff), and use them instead? Look at it this way--you're in the mood for a good steak, there is a great filet mignon in the refrigerator, and your grill is ready to go. So, are you going to fire up the grill, or go to Denny's?

I have a good friend who is a scientist and principal in a local DoD-cleared contractor. A part-time college professor, he has Doctorates in both Statistical Analysis and Oceanography. He is also a veteran of military special operations who is qualified to wear both the

Airborne and Ranger tabs, as well as the Combat Infantryman's Badge. He was awarded the Distinguished Flying Cross and two Bronze Stars with "V" device for valor in battle, along with three Purple Hearts. I have been on the range with him as his instructor, and he's good, very good. Should he hire a poorly paid, inexperienced, security guard? I don't think so. Neither does he. Most of us could easily identify people in our companies who would make good candidates for such a role.

Such a program must be voluntary, of course. It should also be one that is managed and run quietly. Those personnel who might be authorized to possess/carry a weapon in the workplace must be made aware of all others in the same position, but the general population of the company should not, or the program will become useless. In such a situation, employees bent on violence will surely target those who represent the primary threat to their actions, first. So, such a program should remain behind the scenes, on a need-to-know basis. Sounds familiar, doesn't it?

A program like what I am suggesting must have good, practical, requirements for both the initial and recurrent training of those who are participants in the program. There are a number of ways to go about this. In my area, at least one Community College offers a variety of good firearms classes for students enrolled in their Administration of Justice programs. They start with very basic classes, and progress though an advanced firearms course involving tactical training, situational judgment, and good problem solving exercises with realistic scenarios and challenges. They also offer courses to get the State Guard and Firearms cards as well, which would be a good idea for the sake of liability concerns. Armed employees who just happen to have obtained their Guard and Firearms cards makes sense too, does it not? Training and preparation above and beyond minimums will also help.

Commercial schools offer training in this field that go well beyond what is offered in any police academy setting or military training school. That is why so many of their customers are civil and military agencies. USMC Colonel Jeff Cooper's "Gunsite Training Center," now run by Dr. Richard Jee, is the one by which all others must be judged. Also providing top-notch training are such world-renowned trainers like John Shaw, Clint Smith, Ray Chapman, and armed survival training expert Massad Ayoob. Supporting attendance at one of their schools is a great idea.

I mentioned earlier that I'm also an aviator. As a long-time holder of a Commercial Pilot Certificate, and flying in two different uniforms over the years, I have always stressed in my instructing two basic ideals, which go hand-in-hand. First, the critical importance of "situational awareness" can not be stressed too heavily. The "Color Codes of Awareness," developed by Marine Colonel Jeff Cooper, simply must be understood, and made a part of your daily regimen.

There are five states of awareness: White, a state of complete relaxation; Yellow, a state of relaxed alertness that can be maintained indefinitely; Orange, the state of increased alertness in response to a specific act or situation; Red, a state of heightened alertness in response to a potentially threatening act which, if continued, will result in action on your part; and Black, a state in which emergency actions are the only correct, proper, and moral actions open to you.

Most people go through life in White, day-in and day-out. In my world, we call these folks "rabbit people." When faced with a crisis situation they freeze, just like a rabbit caught in a car's headlights. Afterwards, most people refer to them as victims. An example of Condition White most people have experienced at one time or another would be driving along relaxed and comfortable, and suddenly realizing that you don't remember driving the last ten miles you have traveled. Condition Black would be, to a pilot for example, the catastrophic failure of an engine, flight control system, or aerodynamic surface. To an armed employee in the workplace, at ESL for example, it would have been an armed individual shooting up the place. The basic truth here is one can function in White and die or function in Orange and *Live!*

The other training ideal to stress-- and I can not stress it strongly enough--is that people react the way they train. If you do not practice skills, you lose them, and, when needed, they are no longer available to you. I cannot emphasize this enough, even in the firearms classes I teach. But here is an example of what I mean.

Remember the "Newhall Massacre" I mentioned earlier? In the aftermath of that tragedy, CHP Officer Pence, killed while trying to reload his revolver, was found with six empty shell casings in his front pants pocket. He had developed the habit, on the firing range, of dumping his empties into his hand so that he would not have to pick them up off the ground, then putting them in his pocket. When his life depended on a quickly reloaded weapon, he reverted to deadly habits developed during his training and wasted precious time he did not have to put his empty cases in his pocket. He paid the ultimate price for doing so. I repeat, you react the way you train.

A second part of this is that you absolutely must train for worst-case scenarios. As anyone who is a pilot can tell you, whether you are a ten-hour Student

Pilot, a four-thousand-hour F-111F Aardvark driver, or a ten-thousand hour Airline Transport Pilot, most of the training time spent with an instructor is spent preparing for that one fateful moment when absolutely everything goes wrong. Like Forrest Gump says, "[--]It happens."

In an act of workplace violence, what happens is a small, violent, and very personal war. You will have only a few moments to fight that war, and you will have only the tools and skills you have prepared in advance and brought with you. If you wait until you face the situation to think about it, it is way too late. People are going to die.

I will try to put this all together. What we have are well-trained, mature, responsible, experienced, capable personnel. They are in-house, trusted, and ready to act immediately to meet whatever threat may surface. We have a good legal basis for our actions and our crisis management methodology, and we have effectively minimized our liability exposure. In short, we are now prepared to save lives.

When faced with a fire in a trash can, do we have a fire extinguisher that is ready at hand? Sure we do. We do not simply wait for the fire department after we dial 9-1-1. From where I sit that is what this is all about.

I will close this with another short story. On 11 April 1986, two murderers on an extensive bank robbery spree took on eight agents of the FBI in what has come to be known as the "Miami Massacre." Seven agents were shot, two were killed, and two left permanently crippled. The real hero, and a hero in every sense of the word, was Special Agent Edmundo Mireles. Agent Mireles was shot in the opening moments of a four-minute long gunfight that saw more than 140 rounds fired. His right arm was hit by a 5.56mm rifle round that rendered his right arm useless, and resulted in a tremendous loss of blood.

Despite the pain, the fear, the death and injury all around him, Agent Mireles was somehow able to use the one good hand he had. Despite his injuries, he was able to fire his shotgun, operating it with one-hand, learning how to do so as he went. When it was empty, he put it aside and used his one good hand to draw his issue revolver. Walking toward the two killers in a pain-induced daze, he shot and killed them both at what was conversational range. When asked how he was able to do what he did, he answered that he owed his actions to a line from a Dylan Thomas poem that kept going through his mind over and over, as the situation developed, and after he'd been shot. He credits it with giving him the strength and will to do what had to be done.

I truly hope that each of us never sees the day where we are faced with deadly violence in the workplace. If you do, do not give up and do not become a rabbit person. Remember Edmundo Mireles and his story of survival, and this line from the pen of DylanThomas: "Do not go gentle into that good-night; ***rage, RAGE*** against the dying of the light!"

Mark O. Hamersly is Facility Security Officer for Access Research Corporation in Carlsbad, California. While stationed at Headquarters, United States Air Force Europe in Ramstein, Germany, he witnessed destructive terrorism at first hand. He also promotes saving lives as a search and rescue pilot in the Coast Guard Auxiliary.

Executive Order 12937 of November 10, 1994

Declassification of Selected Records Within the National Archives of the United States

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. The records in the National Archives of the United States referenced in the list accompanying this order are hereby declassified.

Sec. 2. The Archivist of the United States shall take such actions as are necessary to make such records available for public research no later than 30 days from the date of this Order, except to the extent that the head of an affected agency and the Archivist have determined that specific information within such records must be protected from disclosure pursuant to an authorized exemption to the Freedom of Information Act, 5 U.S.C. 552, other than the exemption that pertains to national security information.

Sec. 3. Nothing contained in this order shall create any right or benefit, substantive or procedural, enforceable by any party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

/S/ William J. Clinton

THE WHITE HOUSE
November 10, 1994

Records in the following record groups ("RG") in the National Archives of the United States shall be declassified. Page numbers are approximate. A complete list of the selected records is available from the Archivist of the United States.

I. All unreviewed World War II and earlier records, including:

A.	RG 18, Army Air Forces	1,722,400pp.
B.	RG 65, Federal Bureau of Investigation	362,500pp.
C.	RG 127, United States Marine Corps	195,000pp.
D.	RG 216, Office of Censorship	112,500pp.
E.	RG 226, Office of Strategic Services	415,000pp.
F.	RG 60, United States Occupation Headquarters	4,422,500pp.
G.	RG 331, Allied Operational and Occupation Headquarters, World War II (including 350 reels of Allied Force headquarters)	3,037,500pp.
H.	RG 332, United States Theaters of War, World War II	1,182,500pp.
I.	RG 338, Mediterranean Theater of Operations and European Command	9,500,000pp.
	Subtotal for World War II and earlier	21.0 million pp.

II. Post-1945 Collections (Military and Civil)

A.	RG 19, Bureau of Ships, Pre-1950 General Correspondence (selected records)	1,732,500pp.
B.	RG 51, Bureau of the Budget, 52.12 Budget Preparation Branch, 1952-69	142,500pp.
C.	RG 72, Bureau of Aeronautics (Navy) (selected records)	5,655,000pp.
D.	RG 166, Foreign Agricultural Service, Narrative reports, 1955-61	1,272,500pp.
E.	RG 313, Naval Operating Forces (selected records)	407,500pp.
F.	RG 319, Office of the Chief of Military History Manuscripts and Background Papers (selected records)	933,000pp.
G.	RG 337, Headquarters, Army Ground Forces (selected records)	1,269,700pp.
H.	RG 341, Headquarters, United States Air Force (selected papers)	4,870,000pp.
I.	RG 389, Office of the Provost Marshal General (selected records)	448,000pp.
J.	RG 391, United States Army Regular Army Mobile Units	240,000pp.
K.	RG 428, General Records of the Department of the Navy (selected records)	31,250pp.
L.	RG 472, Army Vietnam Collection (selected records)	5,864,000pp.
	Subtotal for Other	22.9 million pp.
	TOTAL	43.9 million pp.

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

NCMS Viewpoints, Volume XXVI, 1990 (Published June 1991)

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

NCMS *Viewpoints*, Volume I, 1992 [Published February 1992]

TITLES AND AUTHORS
OF PREVIOUS *VIEWPOINTS* ARTICLES

NCMS Viewpoints, Volume II, 1992 (Published October 1992)

Almost Everything You Need to Know About Computer Security....
but didn't know whom to ask!
by John R. McCumber . . . . . .

Classification of Compilations of Information
by Arvin S. Quist . . . . . .

The Declassification Dilemma:
Are We Heading in the Right Direction?
by Robert J. White . . . . . .

Defending Contractor Employees in Security Clearance Revocation
Proceedings: A Guide for Defense Counsel
by Jack Thomas Tomarchio . . . . . .

A Prudent Approach to Industrial Security:
The Background and Promise of the National Industrial Security Program
by Maynard C. Anderson . . . . . .

Kurt's Laws of OPSEC
by Kurt W. Haase . . . . . .

Oversight: A Means to an End--Not an End in Itself
by Ethel R. Theis . . . . . .

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

NCMS Viewpoints, Volume I, 1993 (Published February 1993)

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

NCMS Viewpoints, Volume I, 1994 (Published May 1994)

Guest Editorial: Information Security Program: Is the Future Behind Us?
by Maynard C. Anderson . . . . . .

An Engineer Looks at National Security Policy
by David B.Fell, Jr . . . . . .

National Industrial Security Program Impact on Information Systems Security
by Gerald L. Kovacich . . . . . .

Security Policy for International Programs: Releasing US Classified Information to Foreign Governments and Protecting US Security Interests
by Charles C. Wilson . . . . . .