CLASSIFICATION MANAGEMENT

JOURNAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XXVI-1990

ISSN-0009-8434

Published by the National Classification Management Society. Mailing address: Executive Secretary, NCMS, 6116 Roseland Drive, Rockville, Maryland 20852. Editor of Part I of this volume: Eugene Suto. Editor of Part II of this volume: Raymond Schmidt. NCMS Editorial Oversight: David Whitman. The information contained in this Journal and presented by the several individuals does not necessarily represent the views of the organizations they represent -- unless they are the head of the organization -- nor of the National Classification Management Society.

CONTENTS

PART I - PROCEEDINGS OF THE 26TH ANNUAL TRAINING SEMINAR July 10-12, 1990

Section 1. Speakers and Panelists

Section 2. Business Meeting

PART I
PROCEEDINGS
OF THE
26TH ANNUAL TRAINING SEMINAR
JULY 10-12, 1990

Opening Remarks
David A Dittmeier

NEW DIMENSIONS FOR A NEW DECADE

On behalf of the Board of Directors and the Washington, D.C. Chapter, the 1990 Seminar Committee welcomes you to the 26th annual training seminar. We all hope you will enjoy the program and your stay in the D.C. metropolitan area.

It seems impossible for anyone to talk about the new decade without using the word change. Change seems to be the key word in everyone's thoughts and conversations concerning the next ten years. Political, societal, organizational, economic, and technological change is obviously going to be the challenge of the Nineties for professionals in classification management and information security.

Dealing with change is tough. To do it with maximum effectiveness and minimum discomfort demands a substantial breadth and depth of understanding of our programs and the environments in which they exist. There are many dimensions to the real world of government and industry in which we as security professionals must operate. We hope that this seminar will prove useful in broadening and deepening your understanding of classification management and information security as they exist in this complex and rapidly changing world.

The rest--

the direction of the new dimensions of classification management and information security in the new decade

--is up to you.

KEYNOTE ADDRESS

Craig Alderman, Jr.
Deputy Under Secretary of Defense (Security Policy)

Good morning. I appreciate the opportunity to talk with you this morning; to discuss, from my perspective, some of the issues and problems which you and we have to deal with in the broad areas of information security, classification management, and security countermeasures; and hopefully to provide you a degree of intellectual stimulation for both your three days here, and for your work-a-day worlds once you return to them.

Exactly two months ago, I spoke to a seminar held on Long Island by the New York, Connecticut, and Long Island chapter of your society. At that time, I talked about the very substantial, and at times dazzling, changes taking place in the international political and military arenas. I focussed on things that change, and things that do not change -- that is, remain constant -- and the implications of each category for our national security at large, and for our counterintelligence, security, and security countermeasures activities. Change, as the principal focus of a presentation these days, has been somewhat overworked. We are, I believe, in an environment where major changes are the norm, and we are learning to cope with this environment. This morning, then, I want to focus on examples of the first derivatives of change, and look at what I think are three of the more significant, and, in some ways, more intractable tasks that we face in today's, and in the future's, information security and security countermeasures world.

In broad perspective, the industrialized nations of the world are somewhere along an evolutionary path from the nation state to a true realization of Wendell Wilkie's "one world". For a number of reasons, the industrial, commercial, and economic and financial communities are much further along in their evolution than are the political communities. This disparity results in stresses and strains, which, in our case, manifest themselves in the intelligence, counterintelligence, and security functions. However, the disparity will exist for the foreseeable future; and we must therefore learn to handle the stresses and strains to our advantage.

During the past decade, there has been a dramatic increase in the offshore ownership or control of American firms through foreign investment in those firms, or partnerships formed among American and foreign companies, or simply the outright acquisition of an American company by foreign owners.

Merger and acquisition activity on both sides of the Atlantic, and, to a lesser extent, the Pacific as well, is now taking place at unprecedented levels. Smaller, cash-poor firms, or those who have lost their market edge, are most vulnerable, but in this climate, virtually all defense contractors with established markets and needed know-how are fair game. To survive, better capitalized firms are now looking for domestic and foreign partners to team with. If they cannot find them, they simply acquire the competition, or risk finding themselves watching from the sidelines.

The impetus for this activity is largely derived from increased competition for declining defense budgets, rising developmental costs, the international competition for leading technologies, the impending economic union of Europe, and a reappraisal of all aspects of the US/JAPAN relationship. Many foreign firms believe they cannot afford not to have a presence in the United States, and many U.S. firms are positioning themselves in Europe and elsewhere to be able to compete effectively in the years ahead.

Direct foreign investment, and dependency on foreign suppliers for technology and components essential to equipping our armed forces, are inseparable issues. Foreign ownership can help or hurt the United States. In the short term, foreign investment in existing facilities helps us because the production assets remain in the United States. Moreover, there would be severe economic and security consequences if we were not able to compete effectively in areas of advanced technologies. Markets would be lost, the U.S. industrial base would erode (even further), and we would become increasingly dependent upon offshore technologies for our defense. The longer term effects, however, are more difficult to assess. I take note that some believe that interlocked economies, of which defense industries are a part, actually help stabilize world security.

Now, foreign investment, partnership, or ownership of U.S. firms, on balance, may be good things for us. But, they are not without their downside when viewed from the aspects of protection of our classified or sensitive information, or our critical technologies.

Let me say at the outset that, with rare

exception, DoD neither encourages nor discourages a potential foreign investor or owner from acquiring an interest in a cleared U.S. defense contractor. We do look carefully, however, at all foreign involvement with U.S. contractors that may have security implications. An integral part of the Defense Industrial Security Program for the past 30 years is a system that is designed to provide reasonable assurance that our cleared contractors are not affected by foreign ownership, control or influence -- FOCI -- to an extent that is inimical to our national security interests. We consider a facility under FOCI when a reasonable basis exists to conclude that the nature and extent of foreign involvement is such that they may result in the compromise of classified information, or adversely impact on the performance of classified contracts.

In the past, in general, the greater the foreign control and influence permitted to exist, the more restrictive DoD has become with respect to the company's ability to bid and receive classified contracts. Now, however, given the trend towards a global industrial economy, continued pursuit of this policy, without modification, could actually be contrary to our overall national interests.

While an effective policy to deal with foreign involvement is essential for national security reasons, it is equally important to maintain a strong defense industrial base. We can ill afford to impose security policies or procedures which are so restrictive that they act to our disadvantage from an overall national defense perspective. We are trying to strike a balance. If the case of strengthening the U.S. industrial base can be made, along with the benefits of infusing needed capital and promising technology, we will view the foreign involvement in a positive light and attempt to craft acceptable security arrangements. We are continually evaluating, adjusting, and hopefully improving our policies and our procedures to ensure that they are neither unreasonably stringent nor irresponsibly weak and ineffective.

This does not mean that we compromise. It does mean, in certain instances, that we will accept a higher degree of risk than we would if there were not offsetting gain. The challenge then -- yours and ours -- is to strike the most effective balance between these two essentially competing goals. It is a task that neither of us, DoD or industry, can master by ourselves. Each case is unique, and DoD and industry must sit down together, and openly and freely develop the security arrangements for the specific case at hand. How well we accomplish this task will, in the aggregate, significantly impact the strength and overall security of the nation -- one way or the other. I encourage you to work with us.

The second task I will call, "coping with telecommunications and AIS."

There are two subsets to this task -- one dealing with classified information, and one dealing with something we are calling "unclassified but sensitive information." Although we are not very far along in either of these subsets, in the classified information area, we do have a consensus that a problem exists and an agreement that we must solve it. I am going to talk about unclassified but sensitive information, because in this area we don't have either consensus or agreement.

Do we have a problem with unclassified data bases? I think we do. Let me give you a very simple, white world (now), example that you don't have to know anything about automated information systems to understand.

As a result of the ministerial-level START discussions in Moscow this spring, most of the western world has now heard of a missile system called TACIT RAINBOW. TACIT RAINBOW is an air- or ground-launched cruise missile being developed as an autonomous, loitering missile system capable of searching out and attacking enemy emitters, that is, radars and jammers. TACIT RAINBOW is being developed under the "competitive strategies" program. Development and testing has been under way for a number of years.

If you think that TACIT RAINBOW has been an object of hostile intelligence activity, you undoubtedly are correct. But, in this instance, and most probably any number of others as well, the hostile intelligence service would start with something like Lexis/Nexis. Lexis/Nexis is, as most of you know, an AIS subscriber service which provides searches of open source publications based on titles or key words. The stack of documents on the table beside me are Lexus/Nexus' results of a search for articles or other mentions of TACIT RAINBOW.

From this compilation, one can glean the RDT&E program description for TACIT RAINBOW; a rather complete system description; detailed operational characteristics; the newer technologies employed both in the manufacture and the operation; many of the more exotic manufacturing techniques;

costs, both aggregate and by subsystem; and a fairly complete and detailed chronology of TACIT RAINBOW'S test flights, to include the causes for most of the test failures.

Classified? It would be if we put it together! Helpful to the hostiles? You bet! It not only tells them facts they would not know otherwise without a costly and perhaps risky attack, but it also provides guideposts for espionage efforts to obtain critical information not contained in the data base. Yet all of this was assembled by computer assisted techniques from entirely unclassified sources, and now resides in an unclassified data base available to anyone with a very elementary computer, a modem, and the subscription cost.

Moving from the specific to the general, I want you to think about the security challenges posed by international telecommunications networks tied to computer data bases. If you have read anything about the recent German hacker case, you will understand that the potential for mischief is almost without limit, largely because most computer security is inept at best, and in many instances, non-existent.

The international networking of automated information systems has the potential to advance mankind's knowledge, and support mankind's well-being, far beyond their present limits. But, those same systems can be extremely vulnerable to those who see them as their toys -- to be played with, even destroyed, at will, when you stop to realize that international networks currently support university studies, multinational corporations, international law enforcement activities, the functioning of international financial and equity markets, and even the basic functions of allied governments, you very quickly understand the level of concern in this area.

As in the paper world, the security professional's challenge is to assure that valuable information gets to where it is supposed to be, but nowhere else; that the integrity of that information is preserved; and that the information is available but only to those authorized recipients. We have difficulty meeting those goals in modestly sized networks, but in ones that carry large volumes of critical information on an international basis, the level of difficulty is almost beyond comprehension. Economic solutions must be found and applied soon.

I really have raised two subjects here -- the issue of unclassified but sensitive information, and the security of automated information systems themselves. Both of these subjects are products of our times, and have been with us since the computer became an integral and indispensable element in every aspect of our lives. The revolution in telecommunications and automatic information handling has improved those lives in countless ways. But it also has created vulnerabilities -- in our national security, in our economic affairs, and in our personal affairs. These vulnerabilities are open to exploitation by hostile intelligence services, by terrorists, by criminals, by those who would seek personal gain, or by those to whom chaos and destruction are fun. The implications for all of us are significant -- implications for our security, for our resources, even for our constitutional process. The problems won't go away; they require all of us to work to find solutions that are objective, practicable, and affordable. Here, too, I encourage you to work with us.

A third major task facing us is coping with reduced resources in a time of increased threat.

One of the absolutes in the defense world today is that all aspects of the defense establishment are shrinking. Our overall strengths, our numbers of combat formations and major weapons systems, our optempo, our overseas and domestic basings, our major and secondary procurement programs, and the funding levels that support all of these, are going down.

Security, both as an identifiable item in those budgets, and as a concomitant responsibility of all commanders and managers, also will be affected by the decline in defense programs and budgets. Historically, in times of budget increases, security budgets have risen at much slower rates than the budget overall, and, as budgets fall, the resources applied to security have tended to fall at much faster rates. Now, the defense budget has been going down, in real terms, since 1985. Probably the principal reason that security funding has not yet declined significantly is the sobering education provided by the disclosure of a number of major espionage cases in 1985 and 1986. In Wall Street terms, we may be overdue a correction.

I have couched all of this discussion of security in the context of defense budgets, but those of you in the private sector know that your sector's approach to security follows the same trends and patterns. In fact, given the somewhat different set of imperatives that drive the private sector, your highs probably are

lower, and your troughs deeper, than the corresponding patterns in the Department of Defense. We both still face, however, the same array of requirements, and difficulties in meeting these requirements.

Now, there is a large body of opinion, not only public and in the Congress, but held by some in government as well, that would say, "why bother? We won the Cold War; let's get with the more pressing problems of peace."

I will not dispute that there are a host of very large, very serious problems, not directly related to security, facing this nation and the world as a whole. They are daunting, and they will require an earnest and long-term commitment by all of us, if they are to be surmounted. I also will agree that many of the factors that characterized the east-west confrontation for 40 years are now substantively and substantially changed. The threat of an attack by the combined armies of the Warsaw Pact has disappeared. The threat of a conventional attack by the Soviet Union has receded considerably; we now talk of future warning times in months, instead of days and weeks. And although the Soviet Union still possesses the capability to destroy this nation, and still continues to expand and improve that capability, there is a general sensing that the probability of strategic nuclear war has somewhat lessened.

All that having been said, I need not remind this audience that peace is not simply the absence of war. The world remains a very dangerous, dynamic, and uncertain place; and from our perspective as security professionals, the threats posed by that world are legion and are growing. Although I will not attempt this morning to catalog the threat spectrum, I want to note three general trends.

First, the Soviet Intelligence Services are more active against us now than they have been at any time in the past. These services have increased dramatically their efforts to obtain our advanced technologies and manufacturing techniques; and they are more open, aggressive, and even brazen in these pursuits than in the years past. And we, with our open society, our vastly expanded avenues and contacts with the Soviet Union, and our general naivete about espionage, are more vulnerable than ever before.

Second, the other principal intelligence threats -- led by the Peoples Republic of China -- remain as active as ever. They, too, target principally our advanced technologies and manufacturing techniques, which, like the Soviet efforts, places many of you all squarely in the target area.

And third, we are facing an increasing number of non-traditional threats, such as, the economic and industrial intelligence programs of allies and friends; the rise of state-supported terrorism; and the increased efforts of narcotics elements to penetrate our operational, intelligence, and security arenas.

All of these threats, as well as the subject areas I talked about earlier in this presentation, would lead a logical person to conclude that what we need now is more, not less, resources applied to security. But, as I have also said, that is not going to happen. We are therefore going to have to meet these challenges by working on several different approaches at once. I will propose three, although this is not an exhaustive list.

First, and this probably is more for us in government, we need to determine exactly what it is we want to protect. The world of classified information is far too large, and we classify indiscriminately. As a result, classification tends to lose its true import, and we are spread too thin trying to protect the classified universe. I believe we need a new approach to determining what should be protected, and we then need discipline in applying that approach.

Second, and this applies to all of us, we need to work smarter and more efficiently in developing and applying security countermeasures. This may sound like a platitude -- it's not. The United States is one of the world's leaders in advanced technologies and the application of those technologies. And, yet, with some notable exceptions, we are still using security practices and procedures that were the state of the art in World War II.

Finally, and this too is for all of us, we need to come up with more effective ways to convey to our leadership that good security is crucial for this nation to continue to lead the free world, and that good security requires reasonable resourcing. Again, the United States leads the world in packaging and delivering information to convince, whether it be to drink Bud Lite, or to elect a president. We ought to be able to do better for our security budgets. We should not hope to reverse the decline; we should be able to ensure that the security budget glide path is on the same slope as other priority government and private sector programs.

To bring this presentation to a close, let me say that I have looked over your program for the next three days very carefully. You have a full agenda of subjects, all of which are important to the security environment in which we function. What I've tried to do this morning is to sketch out a broader set of issues and problems to lend dimension to the specific topics you will be working here, as well as to cause you to think about where we are going -- and how we might get there -- after you go back to your normal jobs. And I hope I've encouraged you to keep an open dialogue with those of us in government on these types of topics. The challenges ahead are daunting, and we will prevail only if we work in concert with each other at every step along the way.

Thank you for giving me the opportunity to talk to you this morning. I wish all of you a successful, productive, and enjoyable next three days.

INFORMATION SECURITY - AN OVERALL VIEW

Steven Garfinkel
Director, Information Security Oversight Office

Good Morning. I know a lot of you are surprised and many are disappointed to see me standing up here by myself. You've traveled many miles, not to hear me deliver a lecture, but to see me standing beside a brightly colored game board, with a pretty blond -- like Lloyd Taylor -- serving as Vanna. Well, don't blame me. The program committee specifically decided to invite me, but not "security pursuits." Rumor has it that the Program Chairman believes that I now exceed the weight limit for American game show hosts.

However, before I begin, I do have one question that I have been looking forward to asking ever since last year's NCMS National Seminar in Tampa. Please raise your hand if you know the answer. What was the name of the comedian and magician who performed at the President's dinner at last year's seminar? (Call on pre-arranged answerer, who gives correct answer, "Carl Andrews," and offer her the standard ISOO prices -- A goo-goo baby and an ISOO security wiz magi-grip.)

A couple of months ago, a reporter was interviewing me concerning ISOO's recently issued annual report to the President. In questioning me, he asked how long I had been the ISOO Director. In my usual absent-mindedness, I asked him the date and he replied that it was the fourth of May. I walked over to a framed certificate, glanced at its small part, and, sure enough, confirmed that it was the exact date of my tenth anniversary as ISOO Director.

When you've been in the same job for as long as ten years, common wisdom might suggest that you would know what was going on from one day to another. To the contrary. If there's one thing that I've learned over ten years as ISOO Director, it's to expect the unexpected, to expect inconsistency. The agency, the organization, the person that you rely upon one day might not come through the next.

Luckily, there are exceptions. Over my ten years as ISOO Director, I have benefitted greatly from the constancy of the National Classification Management Society. I know that I can always rely upon the professionalism, expertise, cooperation and friendship of the society and its members. For that, I am very grateful.

Enough of the maudlin. With your permission, I'd like to use the occasion of my ten years at ISOO to reminisce with you somewhat. In other words, this is my tenth anniversary speech. Ushers, please bar the doors. As a kind of a twist, I've decided to examine not the highlights, not the triumphs, but some of the low points during those ten years. First of all, examining triumphs may not account for the period of time allotted for my speech. Second, I figure that in order to survive over that period of time, through three very different Presidential administrations, I have had to learn from my mistakes; to escape the doldrums; and actually to build upon what I'll describe this morning as mini-disasters. Perhaps, you, in turn, can also learn something from my experiences.

This morning I'm going to share with you ten of those mini-disasters and what I've learned from them. It would have been structurally ideal to have one mini-disaster for each year, but my top ten didn't quite cooperate -- nevertheless, they are pretty well spread out over the ten years.

Mini-disaster No. 1: Spring, 1980: As the brand new director of ISOO, I've been invited to give my first speech. The audience is comprised of about 50 employees of the Defense Intelligence Agency, (DIA). I'm both nervous and excited about this first presentation. I take a lot of time putting it together. I use my most profound material. I use my funniest material. I give it my best shot. The audience's

reaction. Nada. Nichts. Absolutely nothing. Half the audience looks like robots. The other half is doing head bobs. The speech is a disaster.

Lesson learned: Don't blame yourself, blame the audience. I learn that whenever someone from the intelligence community starts grinning or laughing, it's time to get nervous. I also learn not to be so anxious to accept invitations to speak at DIA. Luckily, that's been easy to put into practice, since DIA has never invited me back.

Mini-disaster two: Summer 1982. I'm meeting in my office with the legal affairs officer from the Canadian Embassy. We're discussing our respective security classification systems. Unfortunately, the carpet in my office is infested with little critters called carpet beetles, which, despite their diminutive size, over the past two years have proven to be immune to every toxic chemical devised by mankind. Ordinarily, these beetles limit their extracurricular activity to climbing up one of the walls. Today, an especially brave little beetle decides to crawl up the leg of my guest. As it crawls up first his shoe and then his sock, only I notice its presence. The Canadian talks on, as I silently urge the critter to turn around. The beetle stays its course and reaches bare skin. The Canadian's leg twitches. The beetle crawls on. The canadian squirms in his seat. The beetle crawls on. The Canadian jumps out of his seat and starts swatting at his leg. U.S./Canadian relations suffer from another environmental catastrophe.

Lesson learned: Conducting foreign relations is a very tricky business. I now understand why the folks at the Department of State don't have the time to learn how to mark a classified document correctly.

Mini-disaster three: March 1983. It is late in the afternoon and I'm seated at my desk reading the funnies and Jack Anderson. The phone rings and I pick it up. The voice on the other end identifies himself as a Robert Pear of The New York Times. He wants to ask me a few questions about the new Presidential directive. "Which directive is that?" I ask. "The directive on unauthorized disclosures of classified information that the President signed today," he responds. "After all, the White House Press Office stated that the ISOO Director would serve as the administration's spokesman to answer questions about it." "Oh, of course, that directive. Would you mind if I got back to you in a few minutes? Thank you." I have no idea what the guy is talking about. A few desperate phone calls to the National Security Council reveals that, indeed, that day the President had signed NSDD 84, and, indeed, I was the administration spokesman about the directive. Despite the fact that I didn't have a copy of the directive, and despite the fact that the last time I had seen even a draft of a directive on unauthorized disclosures had been almost a year earlier, when the project had been shelved.

Lesson learned: First, the most embarrassing foul-ups in implementing the Information Security Program result from the failure to communicate with one another in the most simple way. Second, the most important criterion for serving as a government spokesman is total ignorance.

Mini-disaster four: Summer 1983. I am chairing an interagency panel. The panel is drafting the nondisclosure agreements required by NSDD-84. For the third straight meeting, the panel is debating whether to include the term "classifiable" in the text of the agreements. "It's an unnecessary red flag," argues one of the representatives from the Department of Defense, and half of the panel nods in agreement. "We have to include it," retorts one of the representatives from the Central Intelligence Agency, "In order to protect against the unauthorized disclosure of unmarked classified information." The other half of the panel nods in agreement. As chairman, I ask the representative of the Department of Justice, which will be required to enforce the agreement, and the representative of the National Security Council, which is ultimately responsible for security policy, to break the deadlock. They both state that we should include the term "classifiable" in the nondisclosure agreements. The representatives from the CIA break into broad grins. The word "classifiable" goes into the nondisclosure agreements.

Lesson learned: Don't forget the lessons you've already learned. As soon as those folks from the CIA started grinning, I should have known that I was in big trouble.

Mini-disaster five: Summer, 1985. I'm about to address the class attending the two week information security management course at what was then called the Defense Industrial Security Institute in Richmond, Virginia. Professor Joe Grau, who is about to introduce me, walks up right in front of me, face to face. "Kind of drafty in here, isn't it?" He asks, with a weird edge on his voice. "I hadn't noticed," I reply. "The gate sure is open," Joe hisses. "Huh?" I grunt. I'm looking at Joe like he's lost his marbles. He almost shouts at me, "Dammit, your fly's down." I do the

proverbial 180 pivot.

Lesson learned: Security educators all too often have a habit of saying things in an obtuse fashion. Nevertheless, what they have to say is extremely important.

Mini-disaster six: May 1987. Several friendly, charming staff members from Congressman Dingell's oversight and investigations subcommittee have invited me to chat about the Standard Form 180. One of the staff members barks out, "What do you mean by the term, 'classifiable information?'" "Oh," I reply innocently, "'Classifiable' is limited to unmarked classified information like oral communications." The staff member growls, "well, it seems to me that everything is 'classifiable.'" "Oh no," I reply, "not at all. Of course, the entire information security system depends upon the good faith of its original classifiers. In the wrong hands, arguably, anything could be classified." The next day The Washington Post runs its first story about the SF 180. I have not been contacted by any reporter for the story, but lo and behold, I am quoted in the story: "Steven Garfinkel, the Director of the Information Security Oversight Office, stated: 'Everything is "classifiable".'" Ever since then, it seems that whenever the words "Steven Garfinkel" appear in print, the three words, "everything is 'classifiable'" are bound to be close by.

Let's zoom ahead two years, to April 1989. The nondisclosure agreement litigation has made its way, all the way, to the Supreme Court of the United States. And the name of the case is American Foreign Service Association vs. Garfinkel. I'm about to be immortalized. The famous "Garfinkel" decision. The Supreme Court issues its decision. There is only one reference in the decision to my role in the controversy. The Supreme Court writes: "Steven Garfinkel, the Director of the Information Security Oversight Office, has stated: 'everything is "classifiable".'"

Lesson learned: Sadly, there's only an old cliche that comes to mind here, but it's an important one to remember in dealing with the frustrations that life hurls at you once in a while. There may be a Department of Justice, but there ain't no justice.

Mini-disaster seven: Summer, 1987. I arrive at the Defense Security Institute in Richmond after driving down from my home north of Washington. I haven't stopped on route. I rush through the lounge area to a very important first stop. I burst through the door. To the extent that I can tell, there is no one else in the room. "Well, well, look at this," I think to myself. "Since it's called the Defense Security Institute now, they've gone and redecorated the rest rooms. Plants. And a sofa. Now, let's see, where are the Uri-- Uh, oh. I gotta get out of here before somebody walks in." I push open the door a crack, and try to look through. I rush out to be greeted by a hysterical mob. Ray Yamaoka has spotted me walking into the ladies room, and in the few seconds I am in there, he has managed to gather about 80% of the institute's faculty to greet me, including one or two who had retired several years earlier.

Lesson learned: Security educators may have important things to say, but watch out -- they all have a bizarre sense of humor.

Mini-disaster eight: Spring 1989. I'm sitting at home watching Robert Stack reveal the dark side of life in "unsolved mysteries." He is doing a story about flying saucers. He is interviewing the widow of an Air Force officer, who was sworn to secrecy, but who told her before he died that the Air Force had the remains of aliens from outer space who have crashed to Earth. "Please, I think to myself, "Don't mention the document. Please don't show it on TV, while millions of viewers are watching." No such luck. There it is, in Robert Stack's hands. His own personal copy of "Operation Majestic 12." And he's telling his millions of viewers, the millions of potential letter writers to ISOO, that this appears to be an official government document that confirms the existence of these aliens. For those of you who haven't been exposed to so-called "Operation Majestic 12," the document in Robert Stack's hands is a purported briefing paper, marked TOP SECRET, for President-elect Eisenhower, telling him all about the aliens who have landed or crashed on Earth, and who are currently in Air Force custody. This document has been circulating among UFO aficionados for several years, and periodically, one or the other sends copies to all interested agencies, including ISOO, asking us to confirm its authenticity or to pronounce it a fraud. While all the circumstantial evidence suggests that the document is a fraud, no agency has taken it upon itself to proclaim it a fraud. Even worse, on a number of occasions agency personnel have "declassified" the document, or marked it as "unclassified," by using official-looking stamps to show that the government is not treating this document as classified. Now the supporters of "Operation Majestic 12" are using these government "declassified" and "unclassified" stamps to "prove" that the government has verified the authenticity of this document.

Lesson learned: In the wrong hands, classification and declassification stamps are dangerous weapons.

Mini-disaster nine: June 1989. The crackerjack ISOO inspection team, headed by ISOO's intrepid director, is met on the bridge of nuclear attack submarine, SSN TAUTOG, by the sub's Commanding Officer. Our briefing and inspection will take place in the Commander's warroom. He invites us below, and invites me, as the senior visitor, to go through the hatch and down the ladder first. While I gaze warily down the hatch, the commander tells me to use one of my legs first. Whichever it is, I use the other leg. Within seconds of my descent, my posterior and stomach have completely plugged up the hatch. In the true ISOO team spirit, the other two members of the ISOO team come to my rescue by doubling over in hysterics. One later suggests that he only wished he had a large paddle to hand me, so that I would have looked like I was paddling a giant kayak. The submarine commander, maintaining his cool while those around him have lost theirs, instructs me on the proper manner to extricate myself, and to descend correctly using the proper leg first.

Lesson learned: Nuclear attack submarine commanders are unflappable. ISOO program analysts are flappable. Also, ISOO directors should not purport to become crew members of nuclear submarines.

Mini-disaster ten: April 1990. I'm back at the Defense Security Institute. I receive a call from my office that a reporter for The Boston Globe has a deadline to meet, and desperately wants to talk to me about ISOO's recently released annual report. I call her back and discover she wants to ask questions about the report. She has read about the report in another newspaper story, but claims that she doesn't have enough time to wait for a copy of it to read. After several routine questions, the reporter asks a series of questions like the following: "Tell me Steve," (I hate for reporters who don't know me from Adam to call me by my first name the first time they ever talk to me, thinking that familiarity will somehow get me to reveal something that I otherwise wouldn't) "What's the real story behind your report?" "What's really going on down in Washington??" "How does this crazy system of government work, anyway?" "You've got wild job, Steve. Why don't you tell the real people what it's really like." I do my best to respond, encouraging her to be more specific in her questions.

A couple of days later, what seem like hundreds of people are calling me to talk about the article about me in The Boston Globe, which appears to have been syndicated to most of the newspapers in the western world. Here is a sample of what the reporter wrote about me. "That's why we're in this mess. That's why there is often a vast canyon separating the electorate from the folks who do the business of democracy. We pay their salaries but have no idea what we're paying for. They can't speak our language and we can't speak theirs. Not that Mr. Garfinkel was being rude. He was just uncomfortable discussing his job in human terms. More than anything else, it is this terrible deadness of spirit. The lifeless voice, the dull eyes." (How could she tell my eyes were dull over the telephone?) "The person who seems to be hoping for a reversal in evolution so that he can return to the sea as an amoeba."

Lesson learned: I've got to do something about the way my eyes look while I'm talking on the phone. Also, why do organizations, including the government, hire reporters to serve as press agents?

These, then, are my top ten mini-disasters from my first ten years at ISOO. There have very likely been far worse disasters that my subconscious defense mechanisms won't permit me to recall and reveal. Like the time I almost got fired after being quoted in The Post as suggesting the administration was ambivalent about something; or the ASIS speech featuring the singing cartoon of the President-elect. I hesitate to think what the future holds in store.

DEFENSE INDUSTRIAL SECURITY PROGRAMS UPDATE

John F. Donnelly
Director, Defense Investigative Service

I welcome this opportunity to share with you my views and provide an update on the Defense Industrial Security Program of 1990 and what we can expect to see in the future.

Yogi Berra is alleged to have said:

"The future just ain't what it used to be."

What a profound statement that is proving to be as we examine the international scene today. Yogi's logic captures an idea that is central to the Defense Industrial Security Program. The hidden wisdom of his words is that change, and the challenge

that it represents, is the constant companion to those of us in industry and government who are responsible for protecting and preserving our national secrets.

Who could have imagined a year ago that the Soviet Bloc would crumble, that the old Stalinists in Eastern Europe would capitulate, that Soviet Republics would vote to become independent of the Soviet Union, and Gorbachev himself would be trumpeting the virtues of private ownership of property. Indeed, the future just ain't what it used to be.

What does all this portend for the Department of Defense, the Defense Industrial Security Program, and the Defense Investigative Service?

Is the cold war over?

Will there be a peace dividend?

Has the Soviet Union become kinder and gentler?

or

Is there a grand strategy at work - one designed to put the west to sleep? In the words of a Soviet statesman, is the Soviet Union attempting to "deny [the U.S.] an enemy."

In the eyes of many, if there is no enemy, then it follows that there is no need for a strong national defense or a large intelligence and counterintelligence apparatus within the various agencies and departments of the Executive Branch. If this is true, it would become increasingly difficult to justify expensive security countermeasure required in industry.

The pundits differ on the meaning and consequences of the events taking place today. You can formulate your own opinion. But there is one fact I think we can all agree on: that change - and with it the increasing unpredictability of future events - is the only constant denominator in current world affairs, and we must be all the more vigilant, flexible and ready to respond to whatever the future holds.

Whatever may be the course of events in Central Europe, here at home all of our counterintelligence partners report that Soviet intelligence efforts - and the intelligence efforts of an increasing number of other nations - all targeted against U.S. defense and commercial technologies - are on the rise.

And it shouldn't be all that surprising to you. While the competition among nations is shifting away from tactical battlefields, it is clear that the shift is toward the research laboratories and manufacturing facilities that are the lifeblood of any nation's future economic leadership, strength, and well-being. The KGB may now be a panda, but it's still a bear.

So it is in the context of this rapidly changing environment that I will address the status of the Defense Industrial Security Program and DIS.

Some Simple Facts.

First, the Defense budget is shrinking. This is not "news" - it has been declining since 1985. By 1995, measured either as a share of Gross National Product or as a portion of total federal spending, defense spending will be at its lowest level since before World War II.

Second, we in DIS are not immune to the Defense cuts - we're taking our share as well. However, we are hit particularly hard by the fact that 84% of our annual budget is devoted to personnel resources. Reductions in our budget can only equate to cuts in personnel and a reduction in the number of investigators and industrial security representatives available to accomplish our two fundamental missions.

The challenge that we in DIS face and, indeed, the challenge that you in industry also face, is how to adjust and adapt to an environment of reduced resources. How do we change our methods of operating to reduce spending yet maintaining a viable industrial security program?

I would like to discuss some of the initiatives that DIS is undertaking to prepare for and deal with these fiscal realities:

Downsizing of the Cognizant Security Offices.

DIS is in the process of drastically reducing the size of the staff at the COG office and transferring functions from the staff specialist to field office personnel. We expect some immediate and long term benefits from this shift:

Reducing costs and improving efficiency by moving staff personnel to operational field duties.

Delegating more responsibility to the Field Office Chiefs

and Industrial Security Reps.

Employing a phased implementation plan so as not to disrupt the lives of employees.

Enabling DIS to be more responsive to the contractor through a single point-of-contact for all industrial security matters.

Increased Reliance on Inspection Scoping.

DIS now conducts security inspections "programmatically." That is, the IS Rep selects a program or contract and reviews the implementation of your security program as it relates to that contract.

Allows the IS reps to select programs for inspection emphasis (programmatic inspections), depending upon their assessment of the company's security posture and previous inspection results.

You should do the same when conducting your facility self-inspections. We have initiated a comprehensive training program via teleconferencing to ensure that all of our IS Reps understand this important concept and related techniques. We plan to videotape this training and make this available to industry. In the near future, each COG office will have a copy of this tape.

Programmatic inspections include preinspection research and contact with government program managers to help focus the inspection and ensure that the IS Rep is aware of the security requirements and any usual situations before entering the facility.

Increased Flexibility of Inspection Scheduling.

Reductions in DIS resources preclude the traditional approach to inspections when teams of inspectors would spend 5 to 10 days in large facilities in an attempt to analyze all aspects of a contractor's security program. Fewer inspections for shorter periods of time done "programmatically" result in more meaningful, comprehensive inspections.

Inspection frequency may be adjusted up to 3 months by field offices based upon an assessment of a facility's security posture.

Increased Emphasis on Advice and Assistance Actions.

As the old axiom says, "An ounce of prevention is worth a pound of cure."

Advice and assistance visits are less labor intensive than inspections and enable DIS to have more frequent contact with industry.

Some A&A's will be "grip & grin" visits. Others will be designed to help a contractor address a security problem in accordance with the ISM. These latter actually result in a partial inspection and provide a vehicle for approvals of procedures, areas, etc.

Inspections are opportunities for advice and assistance actions as well.

Let me digress a minute and expand a little on the dual of DIS as "inspectors" and "educators." As I've said before, any good inspection is a mixture of both assessment and education. Since I assumed the position of Director of DIS, one of my goals was to eliminate the offtimes adversarial relationship which existed between DIS and the contractor. It's taken a while, but I definitely see a positive change in the way we are perceived by industry, particularly with regard to what industry now expects from a DIS inspection. To assist in the evaluation of our services, we instituted a quality assurance program within the industrial security program. As part of this program, facility security officers are interviewed by DIS Regional quality control teams subsequent to inspections. Permit me to share the results of one Region's most recent quarterly quality reviews:

31 out of 31 FSO's interviewed described their experiences with their IS Reps as "very positive, helpful, and friendly." The contractors stated that they look forward to DIS inspections because they are non-adversarial and informative.

30 of 31 FSO's stated that they observed changes in the type of inspections we are conducting. They commented how the IS Rep invests more time and effort into learning what their facility does, who works with classified information, and the extent of classified projects.

From the tone of our interviews, it appears that FSO's are not reluctant to call for help or to ask questions. Indeed, our statistics indicate that we processed 8868 A&A calls during May 1990 and conducted 1371 A&A visits.

In sum, we're trying harder to understand your problems, to make them a shared challenge, and to

solve them together. I pledge to you that this will continue.

Contracting Out.

DIS is beginning to contract out some of our personnel security investigations as well as some of our industrial security work. These contracts are non-personal service contracts.

The precedent for contracting out investigative work has been set by OPM.

Contracting out industrial security inspections is another matter. Because of the nature of the contracts, DIS cannot "train" contractors to perform the work. Bidders, therefore, must be equipped to perform the work. I prefer to have inspections in the hands of DIS personnel or former DIS personnel. So, we anticipate some difficulty finding qualified bidders. Nonetheless, we have already let our first contract and there is a resource of very well qualified former DIS employees to be tapped.

Dual Training.

We plan to "dual train" a sufficient number of our investigators to assume certain industrial security duties.

Inspect Category D and access elsewhere facilities or serve as members of a team inspection of a larger facility.

Conduct inspections in areas where IS offices are not collocated with investigative resources and IS support to contractors is currently provided through the expenditure of travel funds.

We will also "dual train" some industrial security representatives to perform limited personnel security investigative duties when visiting contractor facilities.

Electronic PSQ Program.

We continue to support and encourage the electronic processing of Personnel Security Questionnaires.

As of June 11, 1990, 454 contractors are participating in the program, with approximately 25 additional contractors joining the program each month. DIS receives approximately 365 electronic DD Form 48s weekly (or 11% of the total) and transmits approximately 1500 Letters of Consent (or 30% of the total).

The DD 398-2 is currently being programmed for electronic processing. The Defense Manpower Data Center is developing the software. Contractors participating in the Electronic PSQ Program will continue to use the software for the DD 48 until further notice. When software for the DD 398-2 is developed, it will be provided to all contractors participating in the program as soon as it is available. There will no charge for this software.

DD Form 48 (to be executed in draft for entry into the electronic program) is no longer available through DISCO. Contractors may locally reproduce the form for use as a draft.

DD Forms 48 mailed to DISCO are not being accepted any longer. Forms 48 received by DISCO will be returned unprocessed.

Contractors may continue to sign up for the Electronic PSQ Program through CompuServe and use the DD Form 48 for electronic processing until further notice.

Why electronic processing of PSQ's?

It saves money through reduced mail time and easier, more efficient form completion.

The edits and validations of the PSQ on the contractor's microcomputer have virtually eliminated the rejection of incomplete PSQ's. Approximately 19% of the PSQ's completed manually are rejected by DISCO. The rejections significantly increase the overall clearance processing time and administratively burden DISCO and the facility with processing the rejections.

Interim Clearances.

We will continue to process all requests for personnel security clearances on an interim basis. The impact of this program has been significant.

Approximately 45 days of clearance processing time has been eliminated, thereby allowing contractors to utilize their employees almost immediately on classified contracts. It is estimated that this reduction in time resulted in savings to industry of over 182 million dollars during FY89.

We have issued over 90,000 interim SECRET clearance since January 1989. During that period, we have withdrawn only 121. Bear in mind, however, that the withdrawal of an interim clearance does not necessarily indicate that the final clearance will be denied. When an interim clearance is withdrawn, the investigation is completed and the case is referred for adjudication to the Directorate, Industrial Security Clearance Review.

Expedited Facility Clearance.

Last, we will continue to refine and streamline the Expedited Facility Clearance Program.

Current processing time for new FCL's is 19 days.

These initiatives, taken together, mitigate somewhat the impact of the reduction in resources that we are experiencing. As further cuts are levied, we'll have to make other changes and tougher choices. It's a certainty that at some point the demands for our services will be reduced as Defense spending is reduced. The difficult task before us is to maintain a competent and balanced work force until the situation stabilizes.

Treaties.

Also impacting on the mission and resources of DIS are a new round of treaties with the Soviets and all that they portend.

START.

Conventional Forces in Europe.

Our role in these treaties, particularly with regard to START, is to assist industry in segregating areas not subject to Soviet inspection and, conversely, helping contractors to sanitize areas that are subject to Soviet examination. We're used to this - we do it now under INF.

To prepare for START, I have established a liaison position at OSIA Headquarters.

When START is signed and the inspection protocols finalized, DIS resources will again be taxed, especially if there are a significant number of perimeter portals as with Magna, Utah under INF.

National Industrial Security Program (NISP).

Also in the works, as you know, is the concept of a National Industrial Security Program.

There is strong senior industrial support and the highest echelons of Federal Government are also favorable.

DoD is pressing forward with a feasibility study of this important concept.

Standard Background Investigation.

I would also like to mention that in our present environment of budget cuts, treaties, and the NISP initiative, a new impetus for a standard Background Investigation has emerged. An influential member of Congress has drafted an amendment for a single scope investigation and appropriate due process in adjudications.

So, in 1990 we live in an environment of uncertainty. We all face the challenge of managing in the midst of this uncertainty. Flexibility - not rigidity - is the key to dealing with this reality. We in DIS are responding to the realities of the international and domestic environment and trying to anticipate what the future holds.

To this end, I would like to briefly address two technical areas that are of great interest and concern to all of us.

TEMPEST.

The first is TEMPEST - or more precisely our continuing effort to get contracting officers and security managers in the User Agencies to recognize that there is not a very serious TEMPEST threat within the United States.

The NTISSC - the national level policy group that guides COMSEC and TEMPEST matters - recognized this with the publication of NTISSI 7000 on October 17, 1988.

DoD C3I has recognized this with the publication of DoD Instruction C-5200.19 on February 23, 1990.

The services are now in the process of publishing their own implementing regulations in response to the DoD Instruction.

So the word is slowly getting out - that dollars

spent on TEMPEST countermeasures within the United States may be dollars wasted!

Please continue to help wherever you can by identifying to us contracts containing TEMPEST requirements that exceed DoD policy guidelines. If you have contracts with TEMPEST requirements, you can get copies of the DoD Instruction from your local DIS Field Office.

STU III.

The second technical area I would like to cover is STU-III's - and I will touch both on use overseas and the joint DIS/NSA loan program to industry.

First Overseas:

We are well aware that many contractors with overseas operations would like to use and would greatly benefit from having STU-III in their overseas offices. We hear you!

We are working with OSD to finalize policy to allow for the use of STU-III's, keyed with keying material up to the SECRET level, in U.S. contractor offices on the local economy in Europe, the Pacific Rim and wherever else U.S. defense communications require protection.

We are not proposing to extend approval to store classified material, (documents, floppy disks, etc.) on the local economy, but we would like to recognize reality and use the STU-III's to safeguard discussions between overseas offices and points here in the U.S.

Approval would be coordinated by OISI, and the User Agency that "owns" the information would also be asked to concur.

We believe the proposal is both realistic and practical and provides a reasonable balance between security concerns and operational efficiency. We hope to have this matter resolved in the very near future.

Second, the loan program:

I am also pleased to note that the cooperative effort between NSA and DIS to loan approximately 6000 of the newest STU-III models to industry on a long-term, non-contract specific basis is on track.

We expect to notify contractors who asked to participate in the program during July of this year whether they will receive terminals and if so, how many.

Deliveries of the terminals to industry would then begin in the October time-frame and continue through the third quarter of FY91.

We believe this cooperative venture will go a long way toward helping vulnerable facilities "button-up" their classified contract related communications.

International Operations and FOCI.

I wish to close by mentioning two programs with which we are having a great deal of success - Open Forums on general DISP subjects and workshops on International Programs and Foreign Acquisitions and Mergers. These are conducted throughout the U.S. under the auspices of the Regional Director of Industrial Security and the Deputy Director for Industrial Security. Contractors and government personnel are invited to attend.

Security requirements and cautions relative to co-production, teaming agreements, and joint ventures with foreign companies are stressed, as well as various mechanisms to reduce FOCI considerations brought about by takeovers, business arrangements, etc.

The open forums allow for a two-way dialogue on the status of the DISP, problem areas, changes, etc.

The international workshop increases U.S. industry's awareness of authorizing technology transfers and will hopefully result in U.S. industry remaining competitive as international business arrangements steadily increase.

Last, but not least, I want to mention our efforts in support of our cleared contractors overseas. In 1989 we planned, organized, and presented a series of Security Awareness and Threat Assessment Program briefings to hundreds of contractors assigned to Europe and the Far East. We repeated these briefings again this year. This cooperative endeavor with DIA, FBI, NSA and the services has filled a significant gap in security education within the overseas environment. With the break-up of the Eastern bloc and all that it portends for increased East-West trade, we feel it prudent to continue this vital education mechanism. The last time that I looked, there were still designated countries in existence with intelligence

organizations anxious for our high technology and national secrets - despite glasnost and perestroika.

LAA's.

Additionally, we are recommending to OSD that Limited Access Authorizations (LAA's) be allowed for foreign nationals employed by U.S. companies overseas. Under current policy, LAA's are limited to foreign nations employed by U.S. firms in the U.S. We believe such a change will enable U.S. contractors to hire qualified employees in the overseas environment.

Reciprocal Clearances.

One other example of our readiness to respond to today's realities concerns the increase in foreign investment in the U.S. The increase in Proxy Agreements and Special Security Agreements depicts this trend. The Department, of course, has in place responsible policies to deal with foreign investment when it involves a cleared defense contractor. One such policy is the reciprocal facility security clearance wherein foreign ownership and control of a cleared defense company would remain but access by the firm to U.S. classified information would be limited in accordance with U.S. foreign disclosure and export laws and regulations.

Although the reciprocal clearance is a responsible way to deal with Foreign Ownership, Control or Influence in specific situations, the fact that a firm has a reciprocal clearance carries with it a certain stigma and many User Agencies believe there is too much risk to their classified information and are therefore reluctant to enter into procurement contracts with these firms.

In reality, the additional risks associated with reciprocally cleared firms are mitigated by prudent security measures and requirements of the ISM. However, these are not readily apparent to the User Agencies and consequently U.S. classified procurements are increasingly shifted to 100% U.S. owned firms, even though prudent security measures are in place to prevent unauthorized access to the foreign interests and the management of the firm as well as its work force may all be U.S. citizens.

Because of this stigma or perception, we are working with OSD to develop a more effective strategy than the reciprocal clearance - one that assures better protection of U.S. classified information and also assuages the current anxiety of User Agencies who enter into classified procurements with reciprocally cleared firms.

In closing, I believe that DIS is making great strides to become more flexible and efficient. We have met with great initial success by taking the positive approach and looking for solutions, not problems. But partnership implies a two-way street - a "give and take" relationship. In DIS we continue to strive to strengthen our credibility with:

A balance in our inspection authority and advice and assistance roles.

Uniform policy interpretations.

Utilization of good and fair judgment when applying requirements and solving problems.

How can industry help? On a day-to-day basis there are many ways you can help make the program operate more efficiently:

Submit a complete PSQ. The manually submitted PSQ reject rate remains at approximately 19%. The average reject adds about 27 days to the process, and increases the workload for you and DISCO.

Ensure our Special Agents are provided unhampered access to all company records necessary for a thorough personnel security investigation. Help them by making copies of files when requested. Provide interview rooms that are private in terms of visual and aural access by others. Make your employees available for interviews and demand punctuality.

Access to SAP areas by investigators is often necessary to complete a thorough investigation. I am making progress in this regard, but your cooperation is necessary. Agents have appropriate investigations and the SSO's can administratively read them in. The agent is no more interested in substance of a SAP than the soda vendor.

Facilitate access to employees during inspections for interviewing purposes.

Educate other departments, besides security, as to the company's responsibilities in the area of security.

Cooperate on SAP/Carve Out issues with our IS Reps and Agents.

Arrange Entrance and Exit Briefings with your Chief Executive Officer during each inspection.

Our "new image" is not simply a public relations effort. It's a very real reflection of a change in the way we do business. Times are changing and so is DIS.

We're trying to learn more about your programs.

We're trying to listen more attentively to your questions and concerns.

We're trying to talk more personally and effectively with your employees and your customers.

We're trying to develop more innovative and efficient policies and procedures to better counter the real threats with the resources available.

Let me know how we're doing.

Thank you for this opportunity to address this group. I would like to also take this opportunity to mention that, for those of you who have not heard, Bob Schwalls retired from DIS at the end of June. Bob is moving to Dallas to spend time with his children and grandchildren and work on his golf game. Bob's dedication, vast experience, and unsurpassed knowledge of the Industrial Security Program will surely be missed.

The new Deputy Director for Industrial Security is Mr. Greg Gwash. Greg has been with DIS since 1972. He most recently served as the Director of Industrial Security in the Pacific Region. Prior to his appointment as DOIS in 1987, he served as the Chief of the Mannaheim, Germany Field Office, Office of Industrial Security - International (Europe). Greg brings to the job extensive and varied experience in the Industrial Security Program and we look forward to his joining the DIS Headquarters staff within the next several months.

I've enjoyed meeting with you today and I thank you for your attention and your support.

TECHNOLOGY TRANSFER - PERESTROIKA AND REALITY

James J. Bagley, Moderator
R. B. Associates
Dr. Oles Lomacky
Mr. Stanley Sienkiewicz

When approached about a panel technology transfer, it struck me that it would be an opportunity to place in perspective the role of classification management in a new and changing world. The world is restructuring - the meaning of Perestroika; a world that is restructuring in a spirit of openness - Glasnost. At the same time this restructuring is taking place in a world wherein the role of the United States is changing drastically.

It has been said that the role of the US is similar to that of the role of Russia in the time of Peter the Great who started a process which is going on to this date. Is the Soviet Union an Eastern or a Western Nation as it spans an area ranging roughly from the Atlantic to the Pacific oceans? With the dramatic changes in its economy, it appears that the west will win from an economic point of view but whether Russia will be western philosophically and politically remains to be seen.

The US is an island in the center between two burgeoning economies - EC 92 in the West, and the remarkable economic advances in Japan, the Pacific Rim countries and, yes, in China in the East. A major factor in the success of the US will be how it will identify, protect, and judiciously control the "family jewels" - its information, recognizing that all the information necessary to the well-being of the US is not necessarily of US origin. The role of classification management is to identify and protect that which is protectable as long as protection is warranted. The world is changing and we must change with it.

For many years it has been the policy of the US to use export controls to control the export of goods and technology which would make significant contribution to the military potential of any country or combination of countries which would prove detrimental to the national security of the US. Today we have the pleasure of hearing from two acknowledged experts in the field. From the Department of Defense Dr. Oles Lomacky, Special Assistant for Militarily Critical Technologies and Long Range Planning, Office of the Under Secretary of Defense for Acquisition, and Mr. Stanley Sienkiewicz, Associate Deputy Under

Secretary of Commerce for Export Administration.

Doctor Lomacky. I would begin by asking the questions - Do you know what the Militarily Critical Technologies List is and its statutory basis? How it is used within the DoD and outside the DoD? I will begin with a brief overview on how the MCTL is produced and the important input of industry in the production of the list, the relationship of the MCTL to the export control process and its impact on COCOM and vice versa.

The statutory requirements are the Export Administration Act of 1979 as amended in 1985 and the Omnibus Trade and Competitiveness Act of 1988 which required the DoD to establish a list of critical technologies specific enough to provide guidance to those officials having export license responsibilities. It is important to remember that the trade bills deal with "dual - use" technology, that is technology which has both military and commercial application. The Department of Commerce is responsible to work with the Department of Defense in integrating the list into the export control lists revisions. The act requires that the list be limited to that technology which has been determined to be militarily critical. While stressing that it is important for the national interest of the United States that both the private sector and the Federal Government place a high priority on exports, Congress observed that this interest should be consistent with the economic, security, and foreign policy objectives of the United States. The Act also requires that the availability of the technology outside the US be considered - that is, if available generally, it should not be on the MCTL.

Application of the MCTL. Within the DoD it serves as the basis for national security controls, especially East - West national security controls, the MCTL is also being used as the basis for establishing multi-national controls such as the COCOM. I must state categorically that the MCTL is not used to control other aspects apart from national security controls in an East - West context such as foreign policy, missile controls etc. The MCTL does not cover these subjects.

Secondly, within the DoD, the MCTL is used as a guideline for the release of technology. For example, with respect to inertial navigation, the MCTL provides guidance on what levels of technology might be released to a particular country, depending of course, on the foreign releasability of the technology. Again, it is emphasized that the MCTL is only a guide - an aid in processing export control cases. The MCTL applies only to those items which are ALREADY ON THE EXPORT CONTROL LISTS. If the items is not under export controls, the MCTL DOES NOT APPLY.

Lastly, the DoD uses the MCTL for determining technology criticality; for example, in research and development programs. The military departments frequently use the MCTL in the preparation of long range plans.

Outside the DoD, the MCTL is more and more used in the development of proposals to be submitted to COCOM for its consideration and ultimate adoption which could result in an item of technology being controlled by the COCOM countries. Similarly, it is used by licensing officers in the Department of Commerce to provide a rationale for the denial of an export license. It is also used by Customs personnel for the screening of items of hardware for determination of export control sensitivity.

The MCTL is used by the DoD as an input to the development of a Defense Critical Technologies Plan which is a strategy to determine those technologies in which the DoD will invest its R&D funds over a comparatively long time - 10 years for example. Thus, the MCTL has multiple uses.

Misapplications of the MCTL. Sometimes, people use the list as an "embargo" list - not releasable to any non-US entity. The MCTL is a guide - it is not a "go" "no-go" list providing the basis for export denial simply because the technology under export review is on the list. As an example, if the export under review is intended for the Soviet Union or one of the Warsaw Pact countries presence on the list COULD provide a basis for denial. However, if the technology were going to a non-pact country, or to an ally, it would not be justification unless, of course, there was credible evidence of possible diversion to a Pact country or other country to which the export was prohibited.

A second area of misapplication is to use the MCTL in isolation, that is without specific knowledge of the subject matter in question, of what has been published previously, or what is available in the subject area throughout the world. This becomes a particular problem in the review of papers for publication or presentation at technical meetings. Again, the presence on the list is merely an alert; there is a need for further competent technical review. Further, the MCTL does not identify basic research which is outside the scope of the MCTL. Again, foreign availability is

a key issue. If generally available export should not be denied.

Development of the MCTL. The current version of the MCTL was published in an unclassified edition in October 1989. It emphasizes that the format of the MCTL was mandated by the Congress thus not changeable.

How items of technology get on the list is another matter. In general, presence on the list means that the technology is considered to be unavailable to the Soviet Union and must also meet the following criteria:

- The technology is used by the military in the US or our allies in military systems;
- it must be critical to the performance of such systems;
- the technology is considered critical by the intelligence community;
- it is leading edge technology that is not now in our weapons system, but is likely to be.

Again, it is emphasized that just because an item of equipment may be dual-use or on the munitions list does not mean that it is militarily critical; there are items, for example, on the munitions list that are not on the MCTL, and it should be noted that those items on the munitions list that are on the MCTL are so noted in the 1989 edition.

Preparation of the MCTL. There are 12 technical working groups consisting of personnel from the DoD, DoD laboratories, other government agencies such as Commerce and Energy. The groups also include participation from industry which comprises almost 50% of the membership. When a draft is complete, it is sent out for coordination and review by those who may not have participated in its preparation. At this point, there is also an input to ensure that the policies reflected in the document are current.

I would like to re-emphasize the relationship between the MCTL and the export control regulations. The MCTL is not an export control list; it is a basis for providing an emphasis on those technologies which are important to the national security.

Further, the current MCTL is a sub-set of the current COCOM list which is now under review. (See also, Federal Register, Vol. 54, October 5, 1989, Revisions to the Commodity Control List based on COCOM review.)

Can an item approved for export be removed from the MCTL? Not necessarily. Just because an item has been approved for export in a particular case and for a particular country, there may still be justification for its retention on the MCTL inasmuch as the item may still meet the criteria for inclusion in the MCTL and should be controlled. However, if a case can be made by Commerce, for example, that the item is available in foreign markets, there is a mechanism for removing an item from the MCTL. Items can also be taken off the list if there has been a COCOM agreement to decontrol certain items of equipment. In that case, there is no point for control inasmuch as the item generally cannot be unilaterally controlled.

To further comment on industry participation in the MCTL process, the Department of Commerce has an industry technical committee to advise Commerce on what items should or should not be on the list. After all, it is industry which builds defense equipment, knows the foreign markets and foreign competition as well as the availability of raw materials and industrial processes. This committee also produces position papers which are reviewed by the government agencies and the intelligence community and then, adopted, in whole or in part.

Future plans. As one reads the papers, it is apparent that there will be many changes in the items subject to export controls. COCOM has already and will make further reductions on the COCOM list. But I would re-emphasize that the MCTL is much smaller than the COCOM list and reductions in that list may or may not have a significant impact on the MCTL. However, there will be changes and it would be prudent to keep an awareness of the changes.

Recently, the JCSA has conducted a survey of the MCTL process and has concluded that the process is sound and should be continued. Having an independent assessment of the MCTL methodology has been very useful.

Finally, I would reiterate several points:

- The MCTL is a guide and not a directive.
- The MCTL must be used together with other knowledge and must not be used as a single authority to deny an export.
- To be included in the MCTL requires that items meet a rigid criteria for inclusion.
- There is significant industry input in the MCTL process both in the DoD and Commerce.

- Over time there will be significant changes in the items included in the MCTL thus it would be prudent to keep abreast of changes.

In conclusion there will be changes. Perestroika has even come to COCOM. From what we now know, the present 120 COCOM items will be reduced to 8 core technologies each of which will have some technology subsets. Each inclusion will have to be justified on its merits. Obviously, COCOM changes will affect the MCTL, but it is far too soon to predict the final impact. My only advice is to keep an awareness of the changes and act accordingly. The MCTL is a living document and future editions will reflect, as best it can, the technical world both domestic and foreign and will also comply with the Congressional mandate that the list reflect economic and social changes. Thank you.

AFTERTHOUGHTS.

US proposals to COCOM pertaining to the CORE LIST incorporate to a large measure the 1989 MCTL. However, in some cases, US proposals are even less restrictive than would have been indicated to fully implement MCTL recommendations. This is not unexpected inasmuch as the MCTL is a living document and must be constantly updated to take into account foreign technology developments. For this reason we expect that the next MCTL draft will be considerably revised. In addition to incorporating the last COCOM revisions, the new MCTL will also deal with areas related to missile, nuclear, chemical and biological weapons proliferation issues.

Mr. Sienkiewicz.

Let me start with a brief history of export controls since World War II. Then we can cover your questions.

The export control process which exists today, was established after the war. There are a number of bodies of law which underpin the process. For example the Arms Export Control Act regulates things defined as "arms." The US incidentally does not treat the export of arms as a purely commercial activity but rather as a foreign policy instrument. The Export Administration Act regulates items that are not arms and which are under the jurisdiction of the Department of Commerce. Other statutes such as the Atomic Energy Act and the Nuclear Non-Proliferation Act regulate the export of materials which relate to the development and production of nuclear arms and the production of fissionable materials.

The control of strategic technology began when it become obvious that the US would need to develop a system of alliances even with countries which had been our adversaries, that it was in our national interest not only to aid them commercially, but to assist them in being able to provide for a common defense against our new adversaries - the USSR and its allies in the Warsaw Pact. It became obvious that those countries could maintain a numerical advantage, thus the US and its allies had to maintain a technological advantage. The US had to establish cooperative frameworks to assure that the technologies which gave us an edge would not travel eastward. The result was a coordinating arrangement, to be known as COCOM, a gentlemen's agreement among all of NATO minus Iceland, and which now also include Japan and Australia.

In the beginning the problem of controlling strategic materials was comparatively easy since the US and its allies were the principal developers of technology for military applications and in those days militarily-significant technology was less likely to have obvious commercial application. As a result, the COCOM countries were more likely able to control the technologies they were worried about. That has changed.

Increasingly, technologies of commercial origin and/or application have emerged that were of great military importance - computers, for example, have been developed largely for civilian application by industry. At the same time, of course, computers are of major importance to the development and control of military systems.

Because of the increasing rate of change in virtually all areas of technology, it has become harder to keep export controls on target. At the same time other countries have become capable of developing technologies for military and are aggressively selling their products to any buyer with the money to buy. Thus, it has become apparent that there is no point in trying to control technologies readily available throughout the world.

In fact, the Congress has mandated that we consider the issue of foreign availability in implementing export controls. In some cases we have been able to negotiate COCOM-like arrangements with other countries which have agreed with the US to control their export of critical technologies, and the US, in

turn, provides some trade benefits in exchange for their cooperation.

The recent upheavals in the USSR and the Warsaw Pact countries are leading to further changes. High level meetings in COCOM have led to the elimination of some 30 items from the current COCOM control list, and the negotiation of an entirely new approach: a core list consisting of eight categories of strategically significant technologies. The concept of a core list changes the way we do export controls in principle: We will now tell you explicitly what is strategic and may not be exported; if not on the list an item may be exported unless there are other considerations, such as foreign policy controls. This means, of course, that additions to the core list must be thoroughly justified and subject to frequent review.

You may have heard of the term "differentiation." The term means that we have treated some countries in the Warsaw Pact differently than others. Until now, this policy was one mostly of appearance because no one believed that if we sold something to Hungary, for example, that we didn't want the Soviets to have access to, we could count on the Hungarians to protect it. This situation is clearly changing.

It appears that we will be moving into an era where there will be real differentiation - we may soon deal with countries of the former Warsaw Pact with the expectation that restricted items will be kept not only from the Russians but from other countries such as some in the Mid-East.

The unification of Germany has brought on a different set of problems. It would not be reasonable to deal with one part of Germany one way and with the former East Germany in another way. Therefore, we now deal with all of Germany in another way. Therefore, we now deal with all of Germany as we did with the Federal Republic.

The emergence of the economic unification goals associated with EC 92 has begun a process by which the original concepts of COCOM are being re-examined in the light of these new realities. In the final analysis EC 92 means the abolition of trade controls such as licensing requirements between the EC countries and, therefore, among the COCOM participants.

As mentioned previously, those countries which had received preferential treatment because they agreed to COCOM-like arrangements are now watching the changes in COCOM carefully to determine the effects on their commercial positions.

National security controls will be declining in scope, however, not as fast as some would wish. Notwithstanding the fact that mutual agreements with the USSR will produce substantial agreements on arms reduction, both conventional and strategic, the USSR will remain a formidable threat, spending as it does, a sizeable percentage of its budget on military research and development and on new and improved weapons systems. The scope of national security controls will decline, but foreign policy controls, which are largely unilateral, will continue and may expand somewhat depending on the foreign policy interests of the US. The embargoes on South Africa and on some Mid-East countries are examples of foreign policy interests that are reflected on export controls. Also concerns about chemical and biological weapons are similarly reflected in foreign policy controls, as are concerns about nuclear proliferation and the spread of missile technologies.

Let me conclude by giving you something to think about. Strategic trade controls are changing. They are no longer aimed at our traditional adversaries, but at our allies. During World War II, for example, our adversaries were Germany and Japan; the USSR was an ally. The Cold War changed that, and our "enemies" became our "friends." The US spent mightily to rebuild their economies and help protect them against our former ally - the USSR, and its allies. The US provided the defensive shield, which, in part, gave those countries the opportunity to rebuild their economies and to become the economic giants they are today. Now they are serious economic competitors and, as happened in the FSX situation, for example, that competition emerges in interesting ways. That situation was not simply about the loss of technology, but, rather, about industrial competitiveness - the possible effects on the military industrial base. As of now, there are no clear policies regarding what we need to do for the US Industrial base; there is, of course, some legislation to control the foreign acquisition of US companies which are important to the national defense, and some efforts to control offset agreements. The Administration has resisted some attempts on the part of the Congress to pass obviously protectionist legislation. My point is that these efforts are in the realm of foreign policy/economic competitiveness at least as much as they are efforts to control the export of critical military technology.

As a general proposition, the way we deal with export controls today is through a virtually continuous review of our COCOM control lists. This is a process by which the COCOM countries continuously review the list to take items off, and, where justified, to put new items on. Foreign availability is an important key. Our Export Control law requires that there be a knowledge of what technology is available for export from other sources. That requires that we have the means to keep abreast of what is available from other sources. And, though the means (personnel) is decreasing overall, we must try. This approach is sensible; there is no justification for denying US companies the opportunity to make sales because of our lack of knowledge of foreign availability. Now, this concept has been recognized explicitly in COCOM. This is good.

The core list is now being negotiated in Paris. It will result in a substantial liberalization of COCOM's export controls. At the same time, IRAQ's invasion of Kuwait has further dramatized the risks to the world order associated with the spread of nuclear weapons, missile and chemical/biological weapons capabilities in the Third World. Our efforts to control and contain these technologies will require expanded regulatory processes with workable and effective enforcement mechanisms by the COCOM partners and which also must include detailed knowledge of foreign availability on a world-wide basis. No matter how concerned we are about risks, there is little point in only addressing appearances. What is clear, however, is that the world will remain a dangerous place and we must remain on guard and prepared.

Questions from the Audience.

Bagley. Before we take questions - two points of interest - the announcement in the Federal Register of the decisions of the COCOM meeting of 6-7 June, and the announcement of the President that the US will authorize the launching of satellites from Australia using USSR launch vehicles in the near future. These are but two examples of the rapid changes in export policies. And, as we know, the problems are exacerbated by the fact that many satellites are actually dual - use.

(Current Note. A good example is the use of commercial satellite photographs to illuminate "nuclear" facilities in IRAQ and shown on US TV.)

QUESTION. How can we determine what unclassified information should be controlled?

Dr. Lomacky. DoD Directive 5230.25 established the Militarily Critical Technologies List process in compliance with the Export Administration Act (EAA of 1970,(5)(d)(2) as amended in 1985 and 1988). In effect it said what was not in the list should not be controlled. However, there are and will be items not on the list which should be; new items which were produced after the list was published. The directive did say that the List was a Guide, a starting point for review. I would doubt that there will ever be an all-encompassing or totally current list. However, if a license application was made for an item not on the list, and there was a preliminary decision that the license would be denied, then, industry should insist on justification for the decision. And that justification should include, for example, industry's knowledge of foreign availability.

Bagley. It appears to me that much of the information in that category is coming from the telecommunications/communications security areas where technologies are growing so fast that there is considerable confusion, and all too often there are arbitrary decisions such as: "it's on the list therefore it is controlled." It does happen.

However, in the final analysis a decision as to whether an item of information should or should not be controlled is the primary responsibility of the originator, whether government, industry, or academia, or all of the above. The originator is in the best position to determine the worth of the information, the potential value of the information, and whether the information is worth the investment made to produce it. And that decision should be the result of rational analysis of why the work was done (at whatever cost) the possible importance of the work to the company or the government, or both, and the effects of unauthorized disclosure. Only the originator can start the analytical process and develop practical mechanisms to protect the information as long as economically reasonable which can only be done by frequent review.

QUESTION. What is the relationship between the MCTL and Foreign availability in the Department of Commerce and the DoD?

Bagley. There are three inter-related documents - The MCTL, the DoD Critical Technologies Plan, and the Foreign Assessment of the Department of Commerce. The law establishes the standards. Unfortunately however, neither the DoD or the DoC have the assets to produce the documents on a timely basis. For

example, to make a foreign assessment of a single item can require as long as 6-man months to complete, review and publish. Further, there is no established government data base of knowledge of critical technologies throughout the world. For 40-45 years, the intelligence community has devoted its efforts to technical capabilities of the Soviet Bloc, and not the rest of the world. In the final analysis however, it is industry which must, and has the capability of providing such a data base. It is industry that develops and manufactures and sells products in accordance with its perceived markets. It is industry that knows its competition, knows its market and the need for its products. Thus it is fair to say that the principal contributor of data on foreign availability to the government is industry and those research facilities, government or industry which have extensive foreign knowledge. Therefore, it is vital that industry participate in the foreign availability process through membership on the technical committees of Defense and Commerce as well as the committees of the National Academy of Science and Engineering.

INFORMATION SECURITY - A CONGRESSIONAL PERSPECTIVE

L. Britt Snider
General Counsel
U.S. Senate Select Committee on Intelligence

Well, good morning to you all. It is nice to be here. I see so many old friends I haven't seen in quite some time. You certainly look more bright eyed and bushy tailed this morning than I happen to feel. Not only did I stay up last night watching the ball game but our neighbor's kids decided to have a party. I used to come to these events almost every year when I was with DoD. I always found them to be very helpful occasions - not only to renew acquaintances but to discuss common problems, solutions, more or less get reinvigorated on the whole subject. I feel like I'm a little out of date and out of the loop on this whole area cause I have in fact been pretty much involved in another focus in the intelligence world for the last three and a half years and I may not appreciate all that is going on especially in the executive branch and defense industry in this area.

I've been asked to give a congressional perspective on information security. This is something that I found congressional staff is asked to do all the time. I've been asked to give a congressional perspective on this or that on five or six occasions since I've been with the committee and I must say I always approach that sort of task with some trepidation. Who knows what Congress thinks about on a particular subject. The only way you really know is when they take a vote and then you know what they think on that day. The next day, if they take another vote, who knows whether it will come out the same. It's not like the executive branch where it is pure middle structure, the departments and agency's funnel their comments into it and at the end you turn out an administration position on a particular topic. In Congress you have 535 little fiefdoms, men and women who have been elected by somebody to be there. They have their own prerogatives and they assert those prerogatives from time to time pursuing whatever interest they may want to pursue. They are limited only by their own endurance and their committee assignments and the rules of either body.

What is the perspective of Congress on information security? I'd have to say that probably most of them have never given it a thought. You know they know it's out there. They know there's this system of classified information. They know that there are things they don't know that they would like to know. They have a sense that things are kept out of the public domain because they're classified and therefore they can't talk about them. They have this perception that a lot of this hides things that should be discussed in public. They have this sort of general undercurrent with very little understanding of what the system is based on or how it works. But, as I've said, it doesn't take all 535 to cause problems. It really just takes a few who want to pursue their own interest in this area to cause problems for the executive branch or to lead to legislation. There is, however, a general sentiment prevailing in Congress as a whole which I think may have implications for the security business and clearly that's the changes that have taken place in the Soviet Union and Eastern Europe over the last year. There's certainly a general feeling of why can't we cut here and save there and take advantage of the peace dividend if you will. Why can't we be more open than we were before? Why are we so concerned about security as we had been before? You certainly see this attitude in discussing the defense budget and the cuts that are impending there. Nobody really knows what the size of those cuts will be but they will be substantial this year and for the next couple of years.

We also see this attitude in the debate over the export control laws now that the Export

Administration Act is up for renewal this year. In fact its going to be voted on in a couple of weeks in the Senate and you have a lot of people saying why do we have to worry about export controls anymore, even to the Soviet Union or Eastern Europe. Why don't we let American businesses take advantage of these opportunities and just lower the gates?

We see the same thing in the intelligence committee. You all have no doubt seen some of the editorial pieces. There was one in the New York Times a week or two ago suggesting that the intelligence budget be drastically slashed. One of the commentators even suggested that the CIA be disbanded and its functions be dispersed to other agencies. We see it in the counterintelligence area. A year ago we had a consensus that the embassy in Moscow ought to be rebuilt. Now we have people saying why do we need to build a new building, let's just live with the old one. Even though its bugged what difference does it make anymore? Why do we need to worry about travel controls on diplomats? Why don't we just let them do as they please? Why do we worry about ceilings on diplomatic personnel here in this country? Let's just let things rise to their natural limits. Why should we be looking at tightening the espionage laws in this period of improving relationships? Why should we be doing this now of all times?

So this sentiment is going to pose a challenge for security, for security resources, and security policy for the next couple of years. I think this whole area is going to need some very strong advocates, particularly in the executive branch, but in Congress as well.

Let me just take a minute to comment on the Jacobs panel. This was sort of an extraordinary exercise for the committee. Senators Boren and Cohen, the chairman and the vice-chairman of the committee, commissioned this effort last summer before everything happened in Eastern Europe. As it turned out, and they asked Ely Jacobs, who happens to be the owner of the Baltimore Orioles, and Admiral Bobby Inman, who you are familiar with, to put together a group of private citizens to take a fresh look at this whole area for what new legislation might be desirable in terms of improving our ability to cope with espionage. They got together an impressive group of people. They included Lloyd Cutler, who was former President Carter's counsel, A. B. Culvahouse, who was President Reagan's counsel, Warren Cristopher, who was a former Undersecretary of State and a Deputy Attorney General, Saul Linowitz, who was formally Ambassador to the Organization of American States, Richard Helms, who was a former DCI and Ambassador to Iran, Saul Weiss, who is now chairman of the Defense Policy Board, a former State Department official, ambassador, and a law professor at Columbia University, and Harold Edgar, who wrote an article on the espionage statutes back in the 70's which was sort of a definitive article on the espionage laws. These gentlemen met basically on weekends on their own time last winter. They met with people in the executive branch, getting their ideas for change. This led to additional meetings among the panel members themselves earlier this Spring and on May 23 they came before our committee in an open hearing and made 13 recommendations to the committee.

I'm not going to go through all 13 but I thought I'd mention a few of them to you just to give you a flavor for the sort of thing that's being proposed. They proposed, for example, that we establish minimum uniform requirements for top secret clearances by statute. And they suggested that such requirements ought to include providing access to financial records and travel records of government employees with top secret clearances during the period of the time they had clearances and for five years after the clearances were terminated. They recommended that government communicators be subject to counterintelligence scope polygraph examinations during the period of their access or their jobs in that area. And they recommended that the NSA director be given authority to assist problem employees of NSA once they've left the agency to prevent security problems from arising. They recommended a new criminal offense for the possession of espionage devices or equipment, where the intent to commit espionage could also be proven so that you wouldn't have to approve the transfer of classified information if you could show possession and intent to commit espionage. They recommended a new misdemeanor law for government employees who remove top secret documents without authority and who retain them at an unauthorized location. Their thought here was basically that the espionage statutes had not been used to punish such conduct and they thought a misdemeanor offense was appropriate here. They recommended that retired pay be denied to persons who were convicted of espionage in foreign courts where their crime involved U.S. classified information. As you may have known, we've had two cases I think in the last year where we've had retired Army personnel convicted in foreign courts of espionage involving U.S. classified information. They also recommended that the Attorney General be

authorized to pay rewards for information leading to the arrest and conviction for espionage similar to the authority the Attorney General already has under statute to pay for counterterrorist type information. And they also recommended that a court order process be established for physical searches done for intelligence purposes similar to the court order process that's already established under law for electronic surveillance. All of these recommendations were agreed to unanimously by the panel members.

As I said, they were presented at a public hearing of the committee of May 23. Shortly thereafter we had these recommendations put in the form of a bill as 2726 which Senators Boren and Cohen introduced on June 13th and tomorrow we will be having a public hearing on this legislation. The Justice Department will come in and testify on behalf of the administration. We're having Mort Halpren representing the ACLU and also Ken DeGraffenreid who you will remember was responsible for counterintelligence on the NSC staff during most of the Reagan administration. But as I've said, this whole effort was unusual as it has met with some degree of skepticism even within our own committee in terms of why do this now. It's also met with another kind of skepticism particularly coming from one of the Senators on our committee, Senator Metzenbaum of Ohio, who says tightening up the espionage laws and dealing with espionage is fine but why don't we at the same time reduce our exposure to this problem. I mean why can't we do something about all these classified documents? Why can't we do something about all of these people with clearances who don't need them? And in fact he made a statement that I thought was worth reading to you all, so you can see where he's coming from. This is Senator Metzenbaum, "If our secrets are truly to be protected Mr. Chairman, then our security laws and regulations must be respected. Unfortunately this is not the case today. The United States Government is in the ridiculous position of trying to protect uncounted numbers of secret documents with millions more being created each year. Roughly four million people have access to such information. Over 700 thousand have access to top secret information alone. Our current system for protecting secrets is rather like telling a park ranger to protect all the wildlife in Alaska from would be poachers. There's too much to protect. Too many people can get access. Nobody respects the system that classifies nearly everything. These problems are far from new Mr. Chairman, in 1985 the Stilwell commission that studied the year of the spy for the Defense Department concluded that "too much information appears to be classified and much at higher levels than is warranted". The government's information security oversight office (ISOO) called overclassification "a continuing nuisance that eats away at the credibility of the entire system". In 1986, this committee, referring to the intelligence committee, found that "the classification system is unduly complicated and it breeds cynicism and confusion in those who create and use classified information". I submit that the only way to truly protect secret information in the modern world is to stop trying to protect everything. There must be discipline in the classification system right from the start. People must be required to think before they classify and there must be sanctions for overclassification just as there are now sanctions for underclassification. Once the material to be protected is limited to that which truly merits protection, far fewer people will need access to that material. There will be more respect moreover for the need to protect the information. There will also be more justification for the inconveniences and invasions of privacy that we are asked to impose upon people with access to such secrets. As useful as the suggestions of the Jacobs panel may be they will achieve little without such a complete overhaul of the classification system. Mr. Chairman this committee must call on the administration to develop within sixty days and to share with us plans for significant classification reforms that can be enacted by the end of the year. Our national security cannot wait another five years. At the same time Mr. Jacobs and his panel should examine this issue and bring their influence to bear on the executive branch to reduce substantially both the amount of classified information and the number of persons with access to that information. Finally if the administration cannot revamp the classification system this year, I propose that this committee and other interested committees report out legislation to enact this needed reform. Several of the legislative proposals to be presented today place special burdens on two thirds of a million loyal americans who have access to top secret information. I firmly believe that the administration must share those burdens by reforming its own system. Until it does so I will be very concerned over proposals to make so many Americans give up more of their privacy or to create new criminal offenses that are easier than ever to prosecute."

That's Senator Metzenbaum on information security. He's one senator but as I mentioned before one senator can push things a long way when he gets motivated and this senator happens to be particularly motivated on this subject. He requested and obtained from Senator Boren, the chairman of

the committee, a commitment to follow through on this whole area at the hearing. We subsequently followed this hearing with a letter to Steve Garfinkel, who we knew was chairing an interagency effort to do just precisely what I think Senator Metzenbaum has in mind, which is looking at the sunshine dividend we might be able to glean from all that's happening here. We haven't been pressing Steve for a response to our letter and I can't recall what the deadline was, but I don't think this is going to last forever. I think the point is that there is interest on the hill on this subject, whether Steve's group is able to come up with ideas or innovations that would satisfy the concerns of Senator Metzenbaum and others I simply don't know. I sat in on enough of these interagency panels to know that I'm not particularly sanguine about the ability to push innovative ideas through the bureaucracy on this particular issue, but certainly I look forward to reading what Steve's come up with. Could there be legislation? It wouldn't surprise me at all if in fact the committee reports out the Jacob's panel legislation, if it goes to the floor it wouldn't surprise me at all to see Senator Metzenbaum offering amendments on the floor to deal with his particular concern. I'm not quite sure what they might be but this is certainly a possibility.

Incidentally I think its an area that NCMS, probably as much as any organization I can think, of would really be in a position to help. You have the expertise, you have the experience. I think this is an area your organization really ought to think about. I don't know whether Steve has engaged you all or not in his project. I know the committee would be very interested in getting the views of the professionals in this area in terms of what might be done that would make a difference but would still not prevent us from protecting that which still needs protecting, not withstanding all the changed circumstances in the world. I think there really is sort of a new imperative here that's driving this and I think you could help. What sort of things ought to be looked at and should there be higher thresholds for classification? Should we think again about automatic declassification for certain categories or even certain types of information? Should we be thinking about going back to automatic declassification? Should we think about phasing out confidential? Do we really need a three tier system? Sounds pretty radical and I know it would present a lot of practical problems but is it really beneficial to continue to maintain three tiers? Should we think about downgrading classification guides or automatic downgrading and declassification guides? Are there categories of information that in fact we are not concerned about protecting any longer? Has anybody attempted to make this analysis at all on a decentralized basis? Would it help to decrease the number of people with original classification authority? Would that make any dent at all? Are there any sorts of checks or limits you can realistically put on people who apply derivative classifications without bogging down the system completely? We need more oversight and we need more federal mechanisms for challenging improper classifications that won't interfere with carrying on the business of the departments or companies.

I don't know what the answer is here. But I do think it is a good time to think about it. Things do seem to be gelling here and we could very well see legislation in this area. Would it pass? I don't know. I think that's rather doubtful particularly if the administration were to oppose it and they have always opposed any legislation in this area. But it might nonetheless tap into this sort of reservoir of congressional skepticism about the whole program that I mentioned at the beginning. You know that people feel like there is a lot out there that they're not being able to see and the system is being used to protect things for the wrong reasons. I even hear this from the members of the Intelligence Committee who in fact are exposed to the real secrets. So it's a very widespread conception up there that just strikes me that if legislation were to be proposed, it may very well trigger this reaction in people. It's not really partisan. It's more institutional than anything else and it's not very well informed either. As many of you have heard me say before, I happen to be a proponent of legislation in this area, that is, to create a classification system by statute. If I'm not mistaken, didn't NCMS take this position itself several years ago? Is that right? I think it makes sense, I think a law can be passed that respects the President's constitutional prerogatives. It allows him enough flexibility to deal with situations under this statute but I think it would help to have a statutory basis for this whole program so that it covers not just the executive branch but it covers the legislative branch and the judicial branches. I have always been bothered by the fact that there is nothing that binds the legislative and judicial branches to the classification system. They accept it, they don't know what else to do but accept it. But you know they are not bound by executive order. It just seems to me that there ought to be a stronger legal underpinning.

The classification system really forms the basis for a number of other statutes. The espionage statutes are premised on the transfer of classified information.

The Freedom of Information Act exempts classified information from public disclosure. The Privacy Act, ditto for that. But these are all fenced statutes that are based fundamentally on an executive order and on determinations made under an executive order. And finally I think that having it in a statute would increase respect for the system even within the executive branch, and it would lead to greater discipline within the executive branch.

I happen to think this is probably a good time to look at this whole area while in a time of decreasing tensions rather than a period while you have a lot of passion and heat applied to the process. I think we actually may do something more sensible in a time when there is less concern for the international environment. Stay tuned. I think that we'll see over the next year whether this is going to materialize or not but I think there is still a lot left to be done even within our committee on this subject. I wanted to leave plenty of time for questions and I'm not sure how much time I have left but before doing that I wanted to say a few words about information security or security in general in the Congress. I don't think there is anyone else in your program who is going to cover this and you ought to know about it so I'll just take a minute or two to let you know about some of the developments.

Congress has of course been a very much maligned institution in terms of its ability to do things securely, perhaps with a lot of justification. But things are improving, particularly in the Senate. As you all probably know, the Senate a little over two years ago created its own office of security. They have now issued a Senate security manual which is binding on all offices in the Senate. The problem before was particularly bad with respect to Senator's offices and committees who did not deal in the national security area and weren't used to handling classified information. All of those offices are now covered by the new manual and the new system. This Office of Senate Security processes all the requests for clearances. It serves as a repository and clearing house for classified documents coming to the Senate. They are all delivered there, logged in there, stored there, if the office getting it doesn't have a storage facility, and they check the documents out during the day to the cleared staff and they check them back in in the evening for storage and that sort of thing.

They have also now appointed security managers in each senator's office as an additional duty sort of thing. If classified information shows up one day in an office, there will be someone there who knows what to do with it. We've all heard stories. I remember Congressman Bennett telling Dave Whitman and myself that he had a classified document at his office and the staffer didn't know what to do with it. It was late in the day and so the staffer took it home with him and slept on it, put it under his pillow, and returned it in the morning. No harm done. But that's not the way to operate obviously. Hopefully we won't see that anymore.

They have also tremendously improved the technical security up there. I saw a telephone directory the other day of every senator that had a STU III. It's amazing, I would bet 50 senators probably have STU III's in their personal offices now. These are senators who deal with either the chairman or ranking members of committees in the national security area and the senate leadership, all of whom now have secure telephones in their personal offices. Committee offices too have STU III's. The intelligence committee used to have one and now we probably have twenty. It makes a big difference. It helps a tremendous amount I think in terms of keeping our work secure. There's also been new technical monitoring systems that have been installed by the Senate Office of Security that give them a real time capability to monitor technical intrusions and hearing rooms that are used for closed hearings. Senators' personal offices are now covered by this sort of thing so there is a far greater capability now in the senate than there used to be. All this I'm sure you have lived with for years and sounds pretty rudimentary. For the senate its a big step forward over how things used to be. The house has not yet established its own office of security but I'm told that they intend to do so whenever they can figure who should be in charge for the effort. So perhaps we'll see the same thing there.

I'm not sure how much time we have left but let me invite any questions about anything you want, whether on things I've said or other things you're interested in.

Question: Clearances in the office of security. Has anybody been denied a clearance?

Answer: I don't have an answer to that. This raises an interesting problem because its not all decided the same way. Some committees like the Intelligence Committee insist on adjudicating the clearances of their own employees. Other committees will ask the Defense Department. In fact it turns out to be OSD Security most of the time adjudicating clearances for

their committee staff and they simply just accept the determination made by the executive branch. It varies from office to office. The Intelligence Committee has an unusual procedure. The FBI does background investigations on our staff, the results are sent both to OSD and to the DCI for their comments and they come back and tell us whether they have any objection to clearing this particular employee and then the chairman and vice chairman of the committee will actually make the decision. Since I've been there, we have turned down several people who were okayed by the DCI and OSD for clearances. The committee is very rigorous as to who they will accept from a security standpoint. But as I said it varies and some committees leave it in the hands of the executive branch and some people insist that they have to make the adjudication determination themselves. The office does not make the adjudication decisions. They might comment on it but they don't make it.

Question: What Senator Metzenbaum seems to be complaining about, which is how to reduce the amounts of documents and security clearances and this sort of thing, is a different issue than establishing by statute a basis for the classification system, and I think that's right. The question is why can't it all be done together?

Answer: Well I guess it can be done together. Particularly if you can think of ways to deal with Metzenbaum's problem when you create the system. In other words you could imagine putting into a statute restraints on what could be classified. You already have that in the executive order. You could take that and perhaps even expand upon what should not be classified. I haven't thought this through but it does seem like that would be something you could put into a statute if you were so inclined. You might even establish some sort of procedure by statute or requirement for challenging improper classifications and that sort of thing. You could require that by law if you wanted to, so there are things that I think could be done to satisfy Senator Metzenbaum's concerns if the will is there to do them.

Any other questions? If not, let me just say that I've enjoyed being with you and wish you a very successful conference. Thank you.

DECLASSIFICATION IN THE NATIONAL ARCHIVES

Edwin A. Thompson
Director, Records Declassification Division
National Archives and Records Administration

Please cast your memories back eighteen years to 1972. The Eighth NCMS annual seminar was being held in Palo Alto, California. The Society's president that year, Gene Suto, had invited me to address the seminar. The emphasis of that seminar was to be a wide-ranging and carefully crafted review of the new Executive Order on the Government's Information Security Program (E.O. 11652). The program also had a workshop on training classification managers. This was followed by Jack Robinson's examination of the British Official Secrets Act. The DOE interests were conveyed by a luncheon speaker from Lawrence Livermore Labs and a session on AEC's Restricted Data declassification program. Finally there was a press panel. A very typical NCMS program.

But the real emphasis of that seminar was the fall-out of Watergate and the Pentagon Papers -- the new Executive Order E.O. 11652 was the first major overhaul of the classification system since President Eisenhower signed E.O. 10501 in 1953 (19 years earlier). Much of our discussion -- formal and informal -- at the 1972 Seminar was proper classification under the new information security program.

My presentation eighteen years ago was part of the seminar's examination of the Order and was entitled "Effective Declassification at the National Archives." I pointed out that by this new Order my boss, the Archivist of the United States, was given a new responsibility vis-a-vis the management of classified records. That responsibility focused on the declassification of information in order to make it more readily available to the public -- a public which wanted it and needed it to understand the workings of the Government in our democracy.

I briefly described how the National Archives -- first established in 1934 -- was created to receive, preserve and make the permanently valuable records of the Government available to the Government itself and to the public. How World War II changed the character of records transferred into the National Archives -- an explosion in the quantity and most notably, a change in the character of the records.

Most of the World War II and many post-war records were security classified resulting in new storage and public reference problems.

Until 1972 there was no national program which would readily lead to public release of this vast valuable hoard of classified documents. Demand for access was restrained by the requirement for agencies to themselves review the limited number of documents a researcher was permitted to request or for the researcher to obtain a security clearance. To quote my 1972 paper,

To the National Archives the requirement of these orders (E.O. 10501 as amended by E.O. 10816 and President Kennedy's E.O. 10964 of 1961) meant that large quantities of classified records acquired from war-time emergency agencies and similar records originated by the military and other departments were effectively closed except to the most persistent non-official scholars who convinced the responsible agencies that their access was in the best interest of the government and that they were trustworthy.

All of these Executive Orders stated the principle that the originator of classified records was the final arbiter of what was to be declassified.

Modifications of the system between 1945 and 1972 had little effect on making access easier for the public. The staff of the National Archives facilitated the procedures embedded in the various orders by making still-classified records available to approved researchers in secure reading rooms and transferring any notes taken to the agency for approval. Alternatively we submitted photocopies of the identified and requested documents to the originating agency for a release determination. The bottom line was that in 1972 relatively few classified records dated through 1945 had been examined and released. The quantity of World War II records already in the National Archives was staggering -- my estimate in 1972 was approximately 260,000 cubic feet of records or approximately 50 miles of paper. I further estimated that the classified record items scattered among these amounted to about 49,000 cubic feet of paper records and some 18,500 rolls of microfilm or about 160 million pages of classified material.

Having provided that background, I then proceeded to describe the efforts taken by the Archivist to implement that section of E.O. 11652 which said,

All information and material classified before the effective date of this Order (1972) and more than 30 years old shall be systematically reviewed for declassification by the Archivist of the United States by the end of the thirtieth full calendar year following the year in which it was originated. In his review the Archivist will separate and keep protected only such information and material as is specifically identified by the head of the Department. In such case the head of the Department shall specify the period continued classification.

While I had estimated that under the previous orders and directives it would take about five years and 1,136 man-years at a cost of about $11 million to review the 160 million classified pages, by the 1972 Order the National Archives was faced with a requirement to complete the entire declassification review in just over three years to meet the thirty year deadline.

But the new Executive Order also provided new authority to the Archivist and obliged agencies to develop and provide systematic declassification review guidelines. Consequently, we expected to be able to "bulk declassify" large quantities of less sensitive records and quickly label entire containers of declassifiable records rather than cancel markings and stamp declassification authorities on every document. We revised our estimates and launched our effort. This effort included getting 19 key agencies involved -- through meetings and consultation -- in providing useable declassification guidelines while at the same time recruiting, clearing and training staff.

In concluding my 1972 presentation I expressed this thought: From our point of view, E.O. 11652 is a decided improvement over the earlier E.O. It shifted the burden of proof from the researcher, who wants to see the document, to the agencies, who must justify their continued classification. We see it as an attempt to strike a new and better balance between the Government's need for confidentiality and the people's right to know -- a balance in favor of greater access.

Now, reporting to you in Washington eighteen years later, let me briefly describe the present situation regarding the declassification program in the National Archives. I am focusing on the National Archives because that's where declassification of records most clearly equals public release. This is a progress report. The declassification requirements have been modified several times since 1972 but the essence of the program has remained largely unchanged from

President Nixon's E.O. 11652 through President Carter's E.O. 12065 to the present Reagan E.O. 12356.

By 1976 the National Archives had reviewed over 160 million pages of records which were previously classified -- one year later than hoped for, but given the start-up problems a rather remarkable achievement. By the end of this fiscal year (1990) the National Archives will have reviewed and made available to the public about 475 million pages of previously unavailable records.

Nearly all of the World War II and most of the Korean War era military and civilian agency records have been systematically reviewed. The small amount of World War II era records that still contain classified information are records recently accessioned into the National Archives including some Office of National Intelligence and other Navy records still being transferred from the Navy's classified historical records holding area in the Navy Yard. Also large quantities of still classified World War II era microfilm which because of the nature of these records -- largely message center files -- and their high cost of review will only be reviewed for declassification on demand.

Since 1982 the National Archives' declassification program has concentrated on reviewing post-World War II foreign relations documentation in cooperation with and in part financially supported by the State Department and the Agency for International Development. With this financial assistance and through the provision of expert assistance and the preparation of carefully wrought and very detailed declassification guidelines, the National Archives has systematically reviewed nearly all of the State Department's records through 1959 (except overseas embassy and consular records after 1954) and the records of the predecessors to the Agency for International Development through 1954. These are some of the most frequently requested records in the possession of
the National Archives.

But not everything is being reviewed as it becomes 30 years old. One of the most significant changes in the declassification program in Executive Order 12356 is that it no longer requires that all classified records accessioned into the National Archives of the United States be reviewed for declassification when it reaches a certain age. Instead, we are asked to review and declassify only those records in greatest demand by the public and where there is good return on our effort. This change in approach is simply a recognition of two facts we faced in 1982.

First, the resources were never going to be sufficient to continue on the old basis. Budget cuts in 1982 resulted in a staff cut for the declassification effort to the National Archives from a high in 1981 of nearly 89 to a present staff of about 50.

Second, the quantity of more sensitive classified holdings in the National Archives has increased tremendously. In 1984 we estimated there were over 53 thousand cubic feet or about 134 million pages of classified records. In the following three years (1985-87), the volume grew to 127 thousand cubic feet or over 317 million pages, an increase of 137% despite the declassification review of about fifty million pages during those same three years. We estimate that approximately 40% of all the permanently valuable records being accessioned into the National Archives can be expected to contain classified information. This rapid growth results in a growing backlog which far outstrips our present ability to review about 15 million pages a year. Our ability to devote effort solely to systematically review records is also severely affected by the increase in demands for declassification review -- by researchers making requests under the Freedom of Information Act (FOIA) and the mandatory review provision of the executive orders. This impact I did not foresee nor address in 1972. It only began to really adversely affect our systematic review program after the staff reduction (RIF) in 1982 when the staff plunged from 89 in fiscal year 1982 to 48.5 in fiscal year 1983. As fewer series of records were systematically reviewed, researchers reacted by demanding reviews of larger and larger blocks of records. We spend a great deal of time trying to persuade researchers to refine and reduce their requests.

Not only have we never recovered the staffing level we require to keep up with the incoming records, the proportion of effort absorbed by these special demand reviews has increased to a point where nearly 20% of the staff is devoted exclusively to meeting these requests. This leaves us with too few resources to tackle the really significant records which we would like to review systematically.

Everyone involved in declassification review -- the leadership of the National Archives, the Director of the Information Security Oversight Office, and the agency experts working with us -- appreciate that

systematic review is a far more efficient and cost-effective approach to making historical records of real significance available to the public. How much more cost-effective? A 1987 study by a task force in the National Archives determined that it cost the National Archives 56 cents to systematically review a classified page compared to $17.80 for a FOIA or mandatory review of that same classified page. Clearly we need to increase our efforts to conduct systematic reviews.

While I will always advocate a larger systematic review program for historical records in the National Archives I must also tell you of the impact of a very aggressive systematic review program. Reviewing especially significant records often results in withdrawal of a great many individual documents. For example, nearly 20% of the 1955-59 State Department central decimal files are withheld. This often results in increases in mandatory review requests from the public for those same withdrawn items. As a FOIA attorney from the Department of Transportation once stated, "The community of requesters typically don't know that they want, until we tell them what they can't have." As more records are reviewed and withdrawn from high-research interest record series, more targets are created for mandatory/FOIA review and the volume of requests grows accordingly. The most recent and the higher the level of subject interest, the more immediate the public reaction. The result is an ever greater requirement for additional resources. Clearly we need to focus our efforts to gain the most from the dollars available.

Several years ago the National Archives -- after consulting with historians and the knowledgeable reference staff within the Archives -- identified a priority list of systematic declassification. It came to over 45,000 cubic feet or about 35% of the classified holdings at that time. A plan was proposed -- largely involving a substantial increase in staff -- to attack this priority list of records. The plan acknowledged that about 65% of the holdings of classified records would only be reviewed in response to demands. But attempts to increase the staff through additional hiring have run up against delays in obtaining clearances, transfers-out, reductions in the amount of reimbursable funds from the Department of State (after eight wonderful years of this cooperative effort) and now an absolute hiring freeze in the National Archives. A depressing situation, indeed. We know what needs to be done and how to do it. But we apparently never have the resources necessary to meet the objective.

The declassification program in the National Archives has had a roller-coaster ride during the past 17 years. We experienced a steady climb in the staff available from just 20 percent in 1974 to the high point of nearly 90 in 1981. Then a steep plunge to 48 in 1982 and a further fall off to just 37 in 1983. While we have recovered somewhat since then, we seem unlikely to see the staffing levels attained in 1982 again. Unless there is a great outpouring of researcher - public concern and consequent executive and legislative branch attention and interest in declassification there will be no appreciable increase in appropriations. Consequently we must find other ways to obtain the objective. From our prospective, therefore, we need to change the rules of the game since we can't change the number of players.

We must look for a great sharing of the burden of declassification through a substantial renewal of declassification effort by agencies on the permanently valuable records retained in their custody before they are transferred to the National Archives. Agencies should also be obliged to provide real declassification assistance to the National Archives by assigning expert manpower when needed or by providing reimbursable funding assistance to the National Archives.

We should also demand some new thinking about what requires continued security protection after the passage of time. Changes in the political and military situation in Europe and elsewhere during the past few years, consequent changes to strategic plans, changes in the tactical situation, changes in weapon systems used and scrapped, changes in relationships with former "enemies" and changes in the role of the U.S. in international organizations such as NATO and compromises of our "secrets" all suggest an urgent need to reconsider our thinking as to what exactly requires protection after 30 years. The impact of these changes on classification and declassification is a challenge we must all weigh and consider carefully. New thinking about classification guidance and revision of agency declassification review guidelines is urgently required.

The objective remains as it was when this program began in 1972; To make more of the government's formerly security classified records available to the public sooner rather than later -- or never. I've told you something about how that is being done (and can be better done) in the National Archives. I have also suggested that federal agencies must play a much larger role in meeting this same common objective. It cannot all be left to the National Archives!

You in industry who originally created and are often holders of older classified records should be concerned too that continued classification of these historically valuable records is costly to you to safeguard and costly to you as taxpayers after they reach the National Archives. I invite you to join us in challenging the need for continued classification of older records and in pushing for increased systematic declassification review by agencies and increased staff resources for the National Archives.

At the same time we in government must be imaginative and bold in the revision of the prevailing declassification guidelines and deadlines for keeping information classified. If we do this we might once again return to the days which we enjoyed in the early 1970's of bulk declassification of significant portions of our records. We can hope for and fight for acceptance of the concept of automatic declassification of most categories of information after a reasonably short passage of time. Maybe not the General Declassification Schedule of the Carter Order, but a new approach that recognizes the real impact of our post-Cold War world on 3 to 5-decade old classified information. Without this change of thinking we will never catch up and the public's trust in the efficacy of the Government's classified system may be lost forever. Such a loss none of us in this room can afford or tolerate.

NOTE: The views expressed are those of the author and do not necessarily represent those of the National Archives and Records Administration. Mr. Thompson retired from government on September 3, 1990.

CLASSIFICATION MANAGEMENT AND THE DEPARTMENT OF DEFENSE

Arthur E. Fajans
Director of Security Plans and Programs
Office of the Deputy Under Secretary of Defense (Security Policy)

On the door of my refrigerator at home I have magnetically stuck an AT&T advertisement which simply depicts an artist's rendition of a dinosaur. The caption is equally simple and direct to its point: history is full of giants who couldn't adapt.

I put it there in a vain parental attempt to communicate something useful to my eighteen year old son. But sometimes when I come home from a particularly frustrating day at the office, I wonder whether I put it there for him or, subconsciously, as a reminder to myself that change often requires adoption of a different point of view.

I try to be responsive to my environment and sensitive to changes in perception or even reality. Just recently, for example, I gave a speech locally and during the coffee break that followed I engaged in conversation with some in the audience. It's a good time to receive feedback and generally find out what people think and how they perceived your presentation.

(That was a very boring speech. I would have been embarrassed to deliver a speech like that. That was the worst speech I ever heard. That's all right, he's old and senile and he just goes around repeating what he's heard other people say.)

You've been at this conference for over a day now and I'm sure that the mindboggling events of the past year in Eastern Europe have and will be given more than just a passing mention.

Did I predict such radical change? No. Do I know what the next ten years will bring? No. Do we need new criteria to define who we work with and who we work against? Yes. Are current security policies supporting decision makers and the overall objectives of the Department of Defense?

Do we know enough to deal with the rapidly changing world environment and are we, unlike the dinosaur, flexible enough to entertain new ideas? We must adapt to change.

The advent of a new decade brings a time of heightened expectations to the American people--expectations of a peaceful and stable world.

The collapse of the Iron Curtain and the political developments in Eastern European nations have seemingly reduced the military threat in Europe.

Yet, it has been the traditional role of the military to concentrate on potential adversary's capabilities, not intentions. That has not changed. Intent is the silent operation of the mind. I cannot know your intent, I can only make judgements based on actions, what you do, and what you are capable of doing.

The objective still remains to provide for the

defense of the nation and it remains defense policy to ensure that security resources are expended to protect only that which truly warrants protection in the interest of national security.

Basic security concerns remain the same. In fact, our secrets may be more vulnerable in times like these when "loose lips, sink ships" sounds inappropriate.

We all understand that the security disciplines should inter-relate, but it all starts with information security. What is it that requires protection? Once information has been identified as classified, all of the other safeguards, physical, personnel, industrial, should come into play. Although protection of information has been a fact of government life since the earliest days of the United States, the "birth" of the information security program as we know it may be considered the issuance almost thirty years ago of Executive Order 10290, which provided for protection of information in the interest of national security in the military and non-military departments of the government.

Since then, we have seen a succession of executive orders that changed and re-changed the program. Since then too, we have seen dramatic and far-reaching changes in a wide variety of factors which influence our needs and ability to protect national security information.

Some of these are the information explosion since the mid-60's, the constantly changing threat, changes in the operation environment as we seem to be moving toward a paperless workplace, the computer networks of the 70's and 80's, increasingly constrained resources, and fragmentation within the information security program itself.

Are these issues tactical or strategic? Are they rooted in the basic policies and approaches of the program, or are they primarily problems of implementation? How will open skies, Conventional Forces Europe (CFE), or START treaties effect the total security environment? None of these questions can be answered quickly or easily, but will we learn the answers in the next few years ahead.

I believe in order to understand or predict where security policy development is going, we need to have a better understanding of where we've been. We need to analyze, evaluate, and just plain think about factors that influence the security business generally. But we don't have to do a 200 year historical analysis to gain valued insight.

Experience is the best teacher and our own experience is there for the taking. It takes but a moment to recall the decade of the spy, the 1980's and to look quickly to what we may expect in comparison in the 1990's particularly with the realignment of political forces in Eastern Europe.

In the past, significant increases in emphasis and resources in security required emerging technologies ripe for application and public alarm and consensus within the security community and the perception that hostile intelligence services were exhibiting provocative behavior.

In the 1980's, essentially all of these factors existed. Retina eye prints and hand geometry for area access systems, intrusion detection devices, infrared and motion detection alarm systems, automated document control systems the polygon and a continuing vast, array of physical security systems marked examples of technology applied to security disciplines in the 1980's.

Media coverage of the Walker spy case and others, the Soviet bugging of the newly constructed U.S. Embassy in Moscow, and Admiral Inman's initiating concern that there was a hemorrhage of Western technology loss to the Eastern Bloc markedly raised the public's consciousness of the threat to our nation's security.

In response, the government security community became more closely aligned with the intelligence and counterintelligence community and there was consensus for a more proactive stance and protection services became security countermeasures.

And it took like imagination when you saw a photograph of the Soviet space shuttle to see what the hostile intelligence services were doing in terms of information and technology they were gathering and how it was being immediately applied.

But what about these four factors, emerging technologies, public alarm, consensus within the security community, and the provocative behavior of hostile intelligence services, in the 1990's.

Technological developments continue their rapid pace but there is growing concern that we are not keeping up. Automated information systems and the digital processing of huge volumes of data are

raising serous security dilemmas concerning unauthorized access, tampering, logic bombs, and the very integrity of data networks on which we are becoming rapidly and increasingly dependent.

Public alarm has virtually evaporated and has been replaced by growing expectations of peace dividends, information access dividends, and in general, a more benign stable and peaceful world. While some members of the public remain uneasy over present developments, others are questioning the continued paranoia of the security community and are asking where's the treat?

Security policy makers within government no longer share general agreement on how to face the challenges of the future and in my opinion, security policy development and implementation is returning to an environment marked by rice bowls, special and parochial interests, and competing disciplines.

We see special access programs, operations security, computer security, emanations security, (TEMPEST), and a call, born of contractor frustration, for a National Industrial Security Program.

Finally, the Soviet Union seems to have seen the error of its ways and the face of Europe is changing. The hostile intelligence threat will change and I believe we will increasingly see that term falling into disuse and replaced by the foreign intelligence threat.

CNN's Ted Turner recently circulated a memo to his staff that directed them to no longer use the adjective foreign in reporting the news and to substitute the adjective international to more accurately reflect what's going on in the world.

Using that anecdote as a point of departure, when you use the term foreign threat, you presume a single nation state. When you use the term international threat you've broadened the scope of concern. An international threat does not necessarily owe allegiance to any one political philosophy, is less encumbered by the forces of a nation state, and is more difficult to define and therefore more difficult to defend against.

How shall we react in the 1990's? How should we as security professionals prepare ourselves? How should we adapt to the changing environment?

Efforts are underway to insure that security policies are in tune with today's realities and tomorrow's challenges. But as these policies develop, I am sometimes reminded of what the snail said when he went for a ride on the back of a turtle--wheeee!

Internally, we have developed a plan for increasing the effectiveness of information security and special access program oversight. Over the past several years, we have accomplished numerous oversight activities but the actual processes have been uneven.

We have embarked on a more aggressive, more comprehensive, and more cohesive program of oversight of defense component programs. I see my oversight responsibilities as something more than just making sure that defense activities are in compliance with security requirements.

I have placed a high value on the feedback that oversight visits provide for without that input from the various activities. I cannot be as responsive as I feel I should be in trying to resolve security policy issues and improve the overall effectiveness of the various programs. I cannot and should not establish security policies in a vacuum.

There also has been considerable activity within the Office of the Secretary of Defense in recognition that revolutionary change is needed in the way we manage security within the acquisition process.

Project managers and systems acquisition personnel have a unique, highly critical and pervasive security responsibility. They make a vast number of key decisions on what DOD will and will not protect as national security information.

They have a profound effect on the amount of classified information produced or present at any time within the Department of Defense and the Defense Industrial Security Program.

They also decide or heavily influence the added security requirement necessary in special access programs. Consequently, their work determines, in large part, the resources that DOD must commit to protecting national security information. The very nature of special access programs, for example, can dictate an extraordinary expenditure for security support.

Management reviews have noted that operations security needs to be enhanced at RDT&E

facilities; that the supporting counterintelligence and security apparatus has not always been used to best affect; and that many programs lack an overall security concept.

The failure to integrate security countermeasures into a coherent "system" has resulted in unacceptable program vulnerabilities.

As a result, the effectiveness of the supporting security disciples in aggregate has been less than it could be, and the competitive edge afforded by our latest weapons systems is less than it could be.

An acquisition/policy/military department review group on protecting the U.S. technical lead in systems acquisition recommended;

- The formulation of a comprehensive system protection plan for each major system prior to milestone 1,

- and the use of C1 and OPSEC surveys to monitor information loss for each major acquisition system during its development.

The analogy I like to use is a comparison of security to total quality management, until program managers and acquisition executives accept that security like quality is a management responsibility, we will have problems implementing the program.

One classification management anecdote involves the statement by an acquisition executive that when reviewing the classification guide for a weapon system to discern what was more sensitive about the project, it was like trying to discern the size and shape of a city from reviewing a telephone book.

We need to consider what management tools are needed by our executives and program managers to make informed decisions about the level and quality of security afforded the product involved.

As the security experts, we need to do a better job of communicating these requirements so that management decisions are appropriate.

Also, we need to begin using time-phase classification guidance, keyed to the milestones of the acquisition process, so that we can afford the level of security needed during each phase, and that the tailored countermeasures are effective for the system and the technologies involved in the environment that they will be used.

Another necessary step involves implementing controls available to limit distribution of unclassified but sensitive program information.

Finally, I believe that we will see specific requirements in the new major system acquisition directives to be issued later this year including integrated protection planning, or a system security approach.

In a closely related effort on 23 May 1990, the Deputy Security of Defense signed a memorandum requiring immediate implementation of a technology assessment/control plan (TA/CP) for application by the services and defense agencies.

The TA/CP describes a program's scope, identifies the technologies and sensitive information involved.

It evaluates the foreign technologies or other benefits the United States is likely to acquire, assesses the risk to U.S. classified and unclassified sensitive information, establishes foreign disclosure guidance and prescribes specific requirements for the protection of classified and unclassified sensitive information during the course of the program.

A working group has been established consisting of service and OSD acquisition and foreign disclosure representatives to develop a game plan for the systematic and judicious implementation of the TA/CP.

The goal is to require security and foreign disclosure planning early in the acquisition process (milestone 0) so that the security controls and disclosure decisions can be applied systematically in order to apply our security resources where they are most needed.

But these initiatives will take time to be fully implemented to be fully effective. That is a cultural change; it gets at the very basic ways we've done business in the past. But we must change and we must change now.

I mentioned earlier that security disciplines should interrelate. The great unfortunate fact is that this is not always the case. There is too much fragmentation in the government's development of security policies and program implementation and

much well-intentioned work results in conflicting requirements or worse yet, counter-productive requirements.

But, in facing the time ahead, it is necessary to continue to seek ways to integrate security into the programmatic activities of our respective employers. Too often the security professionals sees himself or herself as a specialist and not as a part of the whole.

This is not only self-defeating, it may also be self-destructive. If security is viewed as a separate entity, which often it is, and there is need to save money or cut resources, security is too highly vulnerable.

If, however, we strive to create the notion that security is an integral part of the on-going activity or operation, not only does that contribute directly to the overall success and integrity of the effort, it also provides some greater degree of protection against losing necessary resources.

Tack-on security is both costly and inefficient. Tack-on security in an environment of shrinking resources could be disastrous. Our potential losses are two-fold.

We could lose technological advantage and our systems may be countered before we even field them or loss of our technology allows the production of similar systems by other nations.

The cost of our failure to properly safeguard our systems during the acquisition process is too much for us to ignore.

We must fully integrate security into our systems as they are developed and institutionalize security considerations at the start of the acquisition process and continuously provide security throughout the system's life cycle.

I started this presentation with reference to my refrigerator bulletin board and the picture captioned "history is full of giants who couldn't adapt". If we are to be successful as security professionals in the 1990's we had better adapt to the changing national and international security environment.

Even in rural Virginia you'll find those who while holding to useful and proven ways are keeping up with the times by being flexible. I was reminded of that fact while driving through Patrick County, the southern most county in Virginia. I passed a rural mailbox on which was printed: S. W. Jones - veterinarian and taxidermist - either way you get your dog back.

INFORMATION SECURITY - A JOURNALIST'S VIEW

John Martin
National Correspondent, ABC News, Washington

Good Morning. members of the seminar committee, members of the society and guests. I appreciate the opportunity to speak with you today.

You play an important role in the country's security. Not just in the obvious way of protecting secrets, but in a less recognized way, one that is not widely understood. Yet it is vital to the future of this country.

Best of all: You make the system. I've learned from visiting these meetings yesterday and this morning, that you are the system.

I want to talk about that in a moment, but if it's alright with you, I'll keep that a secret for the moment.

First, I want to tell you that when your program chairman, Joe Grau, called some time ago to ask me to join you, I was a bit surprised.

National Security is not my beat. I dabble in this area. I tangled with the CIA on a matter some years ago -- more on that later -- but it's not what I do for a living.

John McWhethy of ABC News is your man, or David Martin of CBS News, or Jim Bamford, who works for the ABC News and wrote "The Puzzle Palace," the unauthorized history of the NSA.

But not me.

Joe was gracious enough to make me think I was the one he wanted and that I could contribute something today.

I hope I can, because I'm very aware of the perils of mistaken identity. Some of you may remember that about 20 years ago in San Francisco,

there was a killer called Zodiac. There seems to be a new one in New York just now. In the bay area in the early 1970s, people were abducted off the streets, taken to a remote area, and murdered by a killer who left signs of the zodiac around.

The San Francisco Chronicle assigned a veteran reporter, Paul Avery, to write about the murders.

Avery did an interesting thing. He went to a renowned psychologist and asked what would motivate a killer like that. The psychologist had some revealing observations. Avery wrote a story that was pretty good.

It was so good that the Zodiac read it and started writing to Avery. He would send letters with sentences constructed out of newspaper headline letters. This was sensational, because Zodiac had terrorized the bay area for a long time and now he was actually communicating with somebody.

The Chronicle thought it was great: everybody was reading the Chronicle to find out what the Zodiac would say or do next.

The staff was really excited for Avery: This was Pulitzer prize stuff. Still, the more they thought about it, the more they began to worry.

What if this lunatic turned on Avery? He might try to kill their friend. That worried them. They started worrying about something else.

What if the Zodiac mistook one of them for Avery? No telling what he'd do. He might pick off one of them by mistake. This was serious. They decided they had to do something.

So they went out and bought dozens of these little metal buttons; the kind the politicians give away in election years? They put them on all their trench coats. When they walked out at night, the buttons were very visible. They said: 'I'm not Avery.'

Now they wanted to play a prank on the city editor, so they had one more button made and stuck it on his trench coat. It read: "I'm Avery."

Well, I feel a little like the city editor here today. I'm wearing a button that says, in effect: "I'm Avery." I'm one of the journalists. You know, the people who publish secrets and jeopardize national security, to quote the late William Casey.

I guess I'm one of those guys Alan Thompson was talking about who doesn't know what he wants from the National Archives until you tell me what I can't have.

You probably think I'm the kind of reporter who would call Steve Garfinkel and ask: "Steve, what's the human story down there, what's really going on where every life seems like just a series of small defeats. Inside ISOO?"

Well, I might.

But I swear to you that I would never suggest that anyone really rather return to the sea as an amoeba.

Honest, Steve.

In the spirit of Steve's speech about disasters, I want to mention one of my own. Partly in the spirit of George Orwell, who wrote once that "autobiography is not to be trusted unless it reveals something disgraceful, because somebody who gives a good account of themselves is probably lying. Seen from the inside, every life seems like just a series of small defeats.

Some years ago, six, seven, I can't recall, I was plowing through some documents, the lists of World War II War Criminals, the Crowcass Lits, they're called. I don't recall what the acronym means. But as I was looking at the documents, somebody said, "Oh, look at this!". I looked. There was the name of Kurt Waldheim. I said: "Nahh, it couldn't be." Sure enough, four years ahead of time, I had the Waldheim story. Well, easy come, easy go.

Actually, journalists are only the messengers. And there are two messages that I want to bring to you today. The first is one that we all recognize:

It is, simply, we won.

The Cold War is over.

The United States and the Eastern Bloc are no longer enemies.

Competitors, perhaps. But not enemies.

It's not all worked out. But it's getting there.

And that leads to a second message that may not be so obvious here. But let me say it anyway: Now that the Cold War is over, let's open up the Government.

Big surprise, eh? Journalist wants to open the files.

But what I'm trying to say is let's trust each other again. Not with the most vital secrets that must be kept, but with the workings of government that must be understood.

I think we all recognize the necessity of this. Craig Alderman conceded yesterday just how indiscriminate and excessive we've been when it comes to classifying information.

George Carver, formerly of the CIA, writes in the current issue of Foreign Affairs: "Security classification (has) run amok."

So today, I'd like to:

Review some of the abuses of the past,

Suggest some ways we can improve the situation right now, and

Offer a broader concept of security for all of us now that the Cold War is over.

To start off, let's consider the state of tension that still exists. Not in the world, but within our own country.

It's a tension between branches of government, between agencies of government, and between people and their government. It is damaging.

So much of what we spend so much money to learn is being kept from those who need to know it. I'm not just talking about the public's right to know. I'm not just talking about the need for reporters to get the news so the public can make informed decisions.

I'm talking about what the left hand of government keeps from the right hand of government. What one agency keeps from another.

Example: Congressional staff members are denied information by the Drug Enforcement Agency. The people whose job is to help Congress intelligently debate issues, can't get the information unless they agree to a classified briefing.

Example: The State Department has just declassified the list of high-technology products that can not be sold to the Soviet Union and the East Bloc. That was 11 years after Congress said the list ought to be generally available.

Many of us on the other side of the fence -- that is, the reporting side -- have discovered a system that is arbitrary, capricious, and sometimes so cumbersome that it seems to defeat itself.

Almost every journalist who's ever tried to get documents declassified under the Freedom of Information Act has a story to tell: Getting the same docuemnt from different agencies and discovering what was blacked out on one document was left uncovered in the other. That kind of confusion seems understandable, and just a little hopeful. The system is human.

But some practices are highly questionable.

Some years ago, when he was writing NSA, my colleague Jim Bamford filed a request for his file at NSA to see what the agency might have been collecting on him.

The law says records kept on somebody must be kept under their name.

But the reply came back from NSA: No file on James Bamford.

Well, this was suspicious. The agency had done a lot of things to stop Jim from writing about NSA. It even tried to force him to give back a document it had already released to him. Bamford was puzzled. Then he spotted a notation on some other documents he'd requested. A handwritten reference to something called 'Esquire.' Sure enough, when he asked for Esquire, he got his file.

The agency had tried to hide his file by giving it another name. Clever, but according to Bamford, who knows the Freedom of Information Act far better than I do, it is a violation of the law.

Here's another example of what journalists face.

Several years ago after Mike Deaver left the White House staff, questions arose about just how

much access he still had. As you know, it is illegal to lobby your former associates in the executive branch for a time after you leave.

Then somebody leaked the word to William Safire of the New York Times that one of Deaver's Korean clients had been given a face-to-face meeting with Mr. Reagan to deliver a letter.

Now, this was certainly an extraordinary favor for an ordinary "consultant." The kind of favor that would have helped Deaver justify all the money the Koreans were spending to have him represent him.

As you may know, White House photographers take a picture of virtually everybody who meets the President in the Oval Office, literally thousands of them every year. I thought it would be a good idea to get that picture to illustrate Mr. Deaver's lobbying, which he had been denying.

I called the White House photo office. Yes, there had been a photo taken during the meeting. No, the White House press office would have to release it. The White House press office said no, it wouldn't release it, and reminded me that the White House is exempt from Freedom of Information requests.

A former State Department official told me that State routinely gets a picture of every foreign visitor to the White House. The State Department is subject to FOI requests. So I filed one. The answer, after several weeks: Sorry, not in our files.

Was somebody playing games? I don't know. Did the picture exist? I'm convinced it still exists. Did people get to judge for themselves whether Mike Deaver had gotten special treatment? Well, all I can say is that a picture is worth a thousand words.

So, what I'm trying to say this morning is that despite our claims of openness, there is still plenty of secrecy that has nothing to do with security.

The prospect for improvement is pretty grim: As Alan Thompson has just told us: We're building bigger and bigger vaults."

You know, It's been 20 years since the Pentagon Papers case. It's hard to believe that that was half the Cold War ago.

Just to see how young we all are, how many people remember the Pentagon Papers case?

Let's see your hands.

Okay. Just to refresh a few memories:

Daniel Ellsberg was a former pentagon official who worked for the Rand Corporation in California. He made copies of a secret history of the Vietnam War. It was a calculated effort to end the Viet Nam War. He shared the information with the New York Times, The Washington Post, and other news organizations.

Now, the government claimed that publishing the classified documents would damage the national security. Actually, it claimed that Ellsberg and his friend, Joseph Russo, stole the documents, stole the information.

Of course, this case was never decided by a jury. The judge declared a mistrial. The government had broken into Ellsberg's psychiatrist's office. And the judge had met privately with a presidential aide during the trial to talk about a possible appointment as head of the FBI. There were unauthorized wiretaps. Unfortunately, the legal issues of security classification were not resolved at the time.

I looked back over the legal briefs the other day. I was struck by one defense claim. Under the Internal Security Act of 1950, it said, the government had to show that Ellsberg meant to harm the United States. It's certainly not what he intended, he said, but I suppose some would argue that that's exactly what he did.

But maybe we could agree, 20 years later, that knowing the truth about Indochina was better for both sides in America: Those who opposed the War and those who believed in it.

The truth was told: The United States had been involved there far more deeply and far longer than we had been allowed to know. But the government didn't want us to know.

For many journalists working in Washington today, that was the case that first convinced us that the government could and would try to classify documents for political protection rather than national security. It taught us that it was important to try to get documents classified properly and declassified regularly.

Another example: Diplomatic records. And a question: Why do we have to wait 30 years for

them?

And perhaps I got some of the answer from Alan Thompson and Steve Garfinkel at the break. But I'm still not sure it is an adequate answer.

The same year the Pentagon Papers were published, Idi Amin came to power in Uganda. I went to East Africa to report for six weeks. Through a member of the Kenya Parliament, I arranged in advance to get an interview with Amin. When I arrived, I talked to one of his advisors. He wanted to know what I wanted to know. I told him I was interested in the usual questions: The problems he faced in running a poor country. His goals. And so on.

But also about a journalist who had been reported missing. The adviser said he didn't think Amin knew anything about that, but I was free to ask.

The interview was several days away, so I went up country, as they say, to a remote area to look around.

To my surprise, I found villagers who had been arrested without charge. People were disappearing. Everyone was afraid.

Then I got a radio message: "Field Marshal Amin cannot see you after all, but the Foreign Minister will see you on Friday in Jinga." I got out a map. Jinga is a tiny town at the edge of Lake Victoria. This sounded strange. Why would the Foreign Minister see me in Jinga? Driving back toward Kampala, I came upon a concentration camp being build -- literally -- by its inmates, under guard.

I went to the American Ambassador, Clyde Ferguson, and told him what I had seen. He said he didn't know what was going on in the outlying areas, but that things were bad.

I spent a few more days trying to get to see Amin. Finally, I left.

Two years later, the Minster of Health defected in London and wrote a book, called "State of Blood."

In it, he said that "when we were worried, in the fall of 1971, that we were about to be exposed for the mass murderers, we would arrange for people who were suspicious to go to small towns, Jinga among them, where they would be taken into the custody by the Army and taken to the barracks and hammered to death."

Did the United States Embassy know about this? Was something else going on? There have been reports that the CIA had a hand in bringing Amin to power.

Would the Embassy's cable traffic help clear this up? Maybe, maybe not. But we won't know anytime soon. Clyde Ferguson is dead now. And the documents are still classified, still not available 19 years later.

What I'm suggesting here this morning is that in the Cold War, to counter the National Security States of the Soviet Union, and China, we became a National Security State. The two blocs -- East and West -- became National Security Blocs. The Brazilians, incidentally, had a written doctrine defining themselves as a national security state.

We were so worried about what the Soviets were doing, we didn't spend a lot of time worrying about what it was doing to us as a country.

We always had the grim satisfaction of knowing that the Soviets were suffering more from excessive secrecy that the United States. It was true.

Looking back at Chernobyl, Grigorii Medvedev, a Soviet expert on nuclear power, says: Secrecy is "especially dangerous because of the absence of openness (Glasnost) about negative experience is always fraught with unpredictable consequences. It breeds carelessness and thoughtlessness."

But my question is: How can we as Americans feel smug about that here this morning?

Recently, a determined civil servant in the Department of Energy declassified 16,000 documents dealing with nuclear weapons plants in the United States. Now we learn of pollution and carelessness at Hanford, Washington and elsewhere. Here, too, the secrets were kept: American workers suffered accidents and failures, created terrible pollution -- all behind the stamp of secrecy.

Both countries are still secretive. Recently a high-ranking former KGB official came forward in Moscow. He warned that the KGB is everywhere in Soviet security. He said it even opened a rock music club in Moscow to spy on Soviet musicians. He said he could not reveal the classified details of his life as an undercover agent.

Sources and methods. Even so, two weeks ago, President Gorbachev stripped him of his rank and all his medals. Secrets are secrets.

But that's not all. Last Friday, the Moscow City Council denounced his treatment. It said the government was using "Stalinist methods."

Well, wait a minute: Joe Stalin was our villain, and now they want him back.

I guess the point here this morning is the legacy of secrecy lasts a long time.

For a reason.

We need intelligence. We need security. Yes, even secrecy. The capacity to defend ourselves. Every country needs it.

But let's not forget that in the last year of the Cold War, with our adversaries virtually on their knees, we still created 6 million 7 hundred 96 thousand new secrets. That's how Senator Daniel Patrick Moynihan of New York put it after reading Steve Garfinkel's yearly report.

True, many of these "secrets" were derived from other "secrets", but Moynihan asks another question.

If an envelope is marked top secret, does that make a spy's work easier? I guess the answer is yes. In the latest scandal, three generations of American GI's stole the secrets at the Eighth U.S. Infantry Division Headquarters in West Germany. One of them got more than 5 million dollars for NATO battle plans, Air Force operational plans, the locations of all the nuclear weapons.

President Reagan once said of Grenada, we got there just in time. In this case, it sound like the Cold War ended just in time.

With so many secrets, it seems to me as an outsider, that we created the illusion of security without the reality.

Senator Moynihan writes about the illusions of the Cold War in a recent article:

"Errors became a distinctive feature of the system," says Moynihan, who was Vice Chairman of the Senate Select Committee on Intelligence. "This is easy enough to explain," he says. "As everything became secret, it became even more difficult to correct mistakes. Why? Because most of the people who might spot the mistakes were kept from knowing about them, because the mistakes were classified.

"Of all the big mistakes," Moynihan writes, "The biggest was our failure to spot the exhaustion of communism as a world force that had become unmistakable by the 1980s."

Now, these are big issues. Not the kind of thing that comes to your mind as you scan a Form 254. But it's worth having in mind as we decide what the future should be.

So, what are some of the practical steps that could be taken to reform the process? First, let's be clear about what we're discussing. By most objective measures, the United States is guilty of massive over-classification of documents.

By one highly informed estimate, 80 to 90 per cent of all the classified documents in the United States could be released tomorrow without damage to national security.

Instead of protecting the crown jewels, we built a moat around the entire palace.

So as a first step, I think it is time to reverse the assumption that when in doubt, classify.

Yes, let's protect the ten percent of secrets that are truly vital: the codes, the stealth technology, the crown jewels.

But then let's turn our official government records back to the service of the country.

How can we do that?

Some of you may know of Scott Armstrong. He is a former Washington Post reporter who helped organize the National Security Archive here in Washington. Armstrong makes this point:

Instead of being forced to cut the Federal Budget blindly with the Gramm-Rudman axe, why not examine the secret projects, so that intelligent choices can be made.

Art Fajans has talked about efforts in the special access programs.

Almost nobody knows the full extent of special access programs. By 1987 there were some 110 special access programs and inside of them more than 10,000 compartments. According to Armstrong, and others, these are self-perpetuating: No auditors can examine them without, in effect, being cleared by the people they're auditing. Nobody in Congress can learn without clearances whether these programs are failing or whether they're still needed.

Now, some argue that it's the executive branch's responsibility. But under the constitution, it is the Congress that is supposed to regulate the Armed Forces. If they're corrupt or abused or just wasteful, who tells Congress? Armstrong points out that Oliver North was a compartment all to himself.

There's another practical step that would help immensely, more careful marking of these documents.

The practice of portion marking.

If classifiers take the time to pull out the key secret portion and make a single paragraph out of it, the secret stays secret, but the accompanying information remains open to discussion if the rest of the document is declassified.

Another useful step: classify fewer documents with an indeterminate status. Steve Garfinkel reports that over a four-year period, only three percent of the documents reviewed were marked with a date or event beyond which they could be declassified. That's a tremendous amount of information left locked away.

Truth is the first casualty of War, but trust is the first casualty of secrecy.

Trust.

People stop trusting when they can't get the truth. Truth slips out. Nobody thinks it will. But it does. My wife reminds me, it's in the bible:

St. Luke, Chapter 8, verse 17:

"For nothing is secret, that shall not be made manifest; neither anything hid, that shall not be known and come abroad."

Have we learned anything over the years? A great deal. The Congress learned that if the public was going to understand what it was being asked to pay for, there would have to be some access.

The Freedom of Information Act, written by Congressman John Moss of California, was drafted over nearly a decade of hearings. It is a unique instrument. Today, says Moss, it has been virtually destroyed by amendments and subsequent legislation. But the premise was a good one:

Open up the government.

Despite the abuses, we have many things to be proud of. So I'd like to leave you today with a final story about something that makes me proud of the United States.

In 1983, a German Catholic woman named Beate Klarsfeld hounded a Nazi fugitive, Klaus Barbie, out of Bolivia. He was sent to France to stand trial for the murder of Jean Moulin, the head of the French Resistance in World War II. He was responsible for the deaths of thousands of people in Lyon.

A few days after Barbie was returned to France, I got a phone call from a woman in Chicago who was a friend, so help me, of Leonid Brezhnev. Not a close friend, but a friend, actually a beautiful Dutch woman who had caught his eye. That's another story. She told me she had a friend in Canada who knew Barbie quite well. It turned out her friend was an international jewel thief -- reformed, he said -- who had fallen in with Barbie in Bolivia.

I went to see him in Vancouver. He told me Barbie claimed he'd been very friendly with the Americans after the war. And that he had visited the United States many times while hiding in South America. If that was true, I wanted to know, how did he do it? Did we help him? Was he still under our protection?

With the Freedom of Information Act, I got the immigration records of some of Barbie's visits. But the CIA declined virtually all requests for documents.

Did this mean Barbie was a source? An informant? An intelligence asset?

We went to Bolivia to try to find out. Two U.S. Justice Department officials were on the same track. We talked to people. They talked to people. We came back. They came back. We knew from sources that Barbie had been furnishing intelligence information to the CIA, indirectly: We were told his reports were to Bolivian Intelligence and then were

passed on to the CIA.

What we didn't know and couldn't get from the Pentagon or the CIA was Barbie's work for the U.S. in Europe after the war.

The documents existed, but the government did everything it could to keep them from us.

Why?

Well, it said it was because these were investigative records, part of an ongoing investigation. We argued that they had not been generated as part of an investigation. That didn't work. So we sued the CIA and the Army.

Finally, the two agencies offered an unusual deal:

If we would agree to drop our suit, we could go to Langley and sit in a small room with people who had the documents in their hands and we could ask them questions.

If they could answer the questions, they would. If they couldn't, they wouldn't.

Pin the tail on the intelligence donkey. Actually, I began to feel that I was the donkey.

I hate to say it, but I missed the tail completely. I didn't get a thing I could use.

As it turned out, the government was keeping the Barbie information for itself.

And in a sense, it was doing a remarkable thing: carrying out an investigation to set the record straight.

Finally, Alan Ryan of the Office of Special Investigations delivered his report to the attorney general. The United States apologized to France. The U.S. had hidden and spirited away a man wanted for murder. Justice was delayed and denied -- and kept secret. But in the end, the United States performed an act of courage. As a great nation: It apologized.

I said at the start I was keeping one thing secret. Let me finish by saying there is a second way you can fulfill your important role in the security of the country.

The first is that you protect the secrets. The second is that you preserve the public's ability to know those things which need not be secret.

Armed with the facts, there can be broad agreement in America about what needs to be done.

Supplied with information, there can be intelligent choices of goals and strategies.

Provided with the facts, there can be informed judgments about what really needs to be cut from the budget.

So my message to you today is:

Despite the abuses of the past, the mistakes, the problems, we can help reopen government. And you can do it by not only protecting our secrets but protecting our access to the information that should not be secret.

If you will do that, you will truly serve all the people of the United States. Thank you very much.

UNAUTHORIZED DISCLOSURES

M. J. Levin
Special Assistant to the Director of Policy and Senior Classification Officer National Security Agency

Good morning everybody. I have discussed the topic of unauthorized disclosures before, again and again and again. I'm a little bit afraid that you may be hearing a broken record. As a matter of fact, gathering a few papers together to see what I might talk about, I found one that you might recognize. You can't see from where you are what the date is on it. It's the journal of the NCMS in 1979. In 1979 I spoke to the Washington Chapter of the NCMS on a topic that I called, at that time, problems of intelligence and security in a democratic society and I addressed among other things the problem of unauthorized disclosures. I said, "where do the Soviets get their real good stuff?" Do they get it from the recon aircraft ships, satellites, KGB, counselor officials in New York, San Francisco, San Diego? Do they get it from tass correspondents?

Yes, they get a lot of stuff from those sources, but these are costly, dangerous and fragmented.

What's their good sources. Cheap, prolific, safe and authoritative. Washington Post, New York Times, Aviation Week and Space Technology, Defense Electronics, Armed Forces Journal, ABC, NBC, CBS and a number of other places. What I'm specifically talking about I indicated was the frequent appearance in the open of details of intelligence programs for which we have spent years of planning and millions of dollars, details of foreign relationships and foreign basings that are thereby put in serious jeopardy. Details of some of our most fragile sources and methods. Sources which can be forever lost to us if they become known.

I postulated at that time three fixes for this serious problem. The first was some proposed legislative fixes. We haven't gotten very far with that. The most prominent legislative fix that I've been proposing for a long long time we apparently don't have the political will to institute, although there are some members of the Congress, notably Senator Bradley, who are very much in favor of it, and that is legislation which would simply criminalize the unauthorized disclosure of classified information. At the time I spoke that eleven years ago there was a bill to that effect in the House, HR1837, but apparently it went nowhere.

Second, I said we must establish a dialogue with the press. I'm sure you'll recognize that this is a painful recommendation coming from someone whose standard comment has always been no comment, but I believe it's necessary. While there are some radical newsmen and some disaffected former employees who seem intent on doing us in, most members of the force of state are loyal Americans doing what they believe to be right and in the best traditions of the free press. They publish secrets when they don't believe they are true secrets. Many are apparently convinced that we employ idiots to stamp top secret on everything.

The third fix that I discussed at that time was policing up our own act. These are things that we on the inside can do. I indicated that our security is poor both physically and personnally. We have to improve that. I spoke about what it was that allowed this classified information to get out. Was it a desire on the part of officials to curry favor with the press, a desire to curry favor with industry, weaknesses in the contractual process, disaffected employees, malcontents, misguided whistle blowers, politics, senior officials doing what they thought they had to do to let everybody know what the bad guys are doing, or just plain stupidity. Actually it's some of all of them.

I indicated that we have to make a concerted effort to review our practices and procedures and strengthen the weak links. We shouldn't be dissuaded by pessimists who say that nothing can be done. Start with an education program. Make sure everyone understands the potential damage in the exposure of sensitive intelligence sources and methods. Check your distribution lists. Do all those people really have a need to know? How about your information officers. In their zeal to publicize your mission, your capabilities, your product, are they giving away the family jewels faster than you can publish them. Are you sure it's always in that other place where the leak took place and a very high level one when somebody decides to release some information for what he believes to be valid political purposes. Are the procedures crystal clear? Does he have the authority to do it? He always thinks he does, generally he does not. Has the material been officially declassified or at least sanitized? Has he consulted with the appropriate senior intelligence officer?

At the end of that little talk I said by the way you know those newsmen who think we have a lot of crazies running around with top secret stamps, I said and by the way we do have some, let's go get them. The situation, the problem between the requirement to have good intelligence and to keep it secret and the public's right to know has been a problem since the founding of this country. In 1777, George Washington wrote to Elias Dayton discussing the need for intelligence in these words.

"The necessity of procuring good intelligence is apparent and need not be further urged. All that remains for me to add is that you keep the whole matter as secret as possible. For upon secrecy success depends in most enterprises of this kind, and for want of it they are generally defeated."

It was only three years after that in 1790 that secret funding for foreign intelligence activities was formalized by Congress in the form of a secret contingency fund for use by the president.

So the recognition was there from the very beginning. We have to have good intelligence. We have to keep it secret. And failing to do that we're in deep trouble. There have been leaks recorded throughout history. The earliest one that I happen to have a record of at the moment is in 1800. Wasn't exactly an intelligence leak but it was an interesting

one. On March 18, 1800, Thomas Dwayne, editor of the Philadelphia Aurora, was cited for contempt of the Congress for having failed to appear as ordered to explain how he had obtained the text of a controversial but secret senate bill and caused it to be published. Mr. Thomas Jefferson was Vice President and leader of the Democratic Republican Party. His supporters feared a plot to deny him the presidency in the upcoming election and so they apparently leaked a copy of this particular bill to William Dwayne. An offended federalist demanded an investigation of Dwayne and his illicit sources. Vice President Jefferson, as the Senate's presiding officer, was directed to read Mr. Dwayne a list of prepared questions about who had given him the bill. Mr. Dwayne asked for additional time to seek counsel, a request Mr. Jefferson quickly granted and that was the last anybody from that Congress said of Mr. Dwayne. He hid out for the remainder of that particular congressional session.

Now throughout history presidents have complained about leaks. I have some quotations from some of the most recent that are interesting. Harry Truman in October 1951 said that "95% of our secret information has been revealed in newspapers and slick magazines and that's what I'm trying to stop". Dwight Eisenhower in 1955 said "Listen from now on if I'm going to make any announcement I don't want it told to anyone on the hill. I don't believe that the president should be in any position of making an announcement that has already been leaked". I think he thought these leaks were all from the hill. He might have been surprised to know where some of them really came from. John F. Kennedy said in 1961 "stop everything else you're doing, I want the name of the person responsible for this and I want it today. This has got to stop." And you may remember that some wag during that same period said of the Kennedy administration "This ship of state leaks from the bridge." Lyndon Johnson in his typical fashion said "This god damn town leaks like a worn out boot." Richard Nixon as you all know had a little bit of a problem with the leak and plumbers and he tried to find them to stop them. He said "I don't give a damn how its done, do whatever has to be done to stop these leaks and prevent further unauthorized disclosures. I don't want to be told why it can't be done. This government cannot survive, it cannot function if anyone can run out and leak whatever documents he wants to. I want to know who is behind this and I want the most complete investigation that can be conducted. I don't want excuses, I want results. I want it done whatever the cost." The cost was pretty high for Mr. Nixon. Even Gerald Ford said "I'm damn sick and tired of a ship that has such leaky seams. We're being drowned by premature and obvious leaks." Finally, Jimmy Carter one day speaking to a group of State Department officials said in 1979 "This leaking has got to stop. If there are any leaks out of your area whatever the area may be I'm going to fire you. Whether or not that's fair and I can see where some of you might not think it fair, this has just got to stop."

The last DCI expressed his perception of the problem of leaks. And you'll notice that I'm going to be quoting some unclassified speeches, unclassified articles. I'm going to read from a few newspaper items, scrupulously avoiding all classified information. It's extremely difficult to discuss serious leaks of intelligence information at an unclassified level so you'll have to bear with me. The last DCI said "In recent years publication of classified information by the media has destroyed or seriously damaged intelligence sources of the highest value. Every method we have of acquiring intelligence, our agents, our relationships with other security services, our photographic and electronic capabilities, the information we get from communications has been damaged by the publication of unauthorized disclosures. Stories in both the print and electronic media have shown sometimes in great detail how to counter capabilities in which we have invested billions of dollars and many years of creative talent and effort. This time and again has enabled those hostile to us to abort huge investments, to conceal and otherwise deny us information critical to our defense, and to deprive us of the ability to protect our citizens from terrorist attack. Leakers are costing the taxpayers millions and even billions of dollars and more important putting Americans abroad as well as our country itself at risk.

Some interesting insights a few years ago came from the distinguished owner of the Washington Post, Mrs. Kathryn Graham. She was trying to emphasize the extent to which the press is willing to withhold potentially damaging information and she added "tragically however, we in the media have made mistakes." You may recall that in April of 1983 some sixty people were killed in a bomb attack on the U.S. Embassy in Beirut. At the time there was coded radio traffic between Syria, where the operation was being held, and Iran, which was sporting it. Alas one television network and a newspaper columnist reported that the U.S. Government had intercepted the traffic. Shortly thereafter the traffic ceased. This undermined efforts to capture the terrorist leaders and eliminated

a source of information about future attacks. Five months later apparently the same terrorists struck again at the Marine Barracks in Beirut and 241 servicemen were killed. Now this was a tragic media mistake that Mrs. Graham knows about. What about all those that she doesn't know about, and there are many.

The DCI again addressed this question in recent weeks and months when he said a flood of information has appeared in print and on the airwaves. Before the president spoke to our people and told them about the conclusive evidence that we had about Libyan direction of the attack of allied soldiers in the Berlin nightclub, you'll remember that as the LaBelle Discotheque, major newspapers and news magazines published that Libyan communications were being read. The Libyans stopped using those communications and this is bound to put other peaceful citizens in jeopardy. This is a severe problem we must address if our fight against terrorism is to succeed.

Incidently on the way down this morning I was listening to the news in the car. I heard that it was just discovered that the East German government had known about this projected attack on the LaBelle Discotheque and did nothing to tell us about it.

Let me pick up on some more recent leaks again by some quotations from odd cases if I may. Here is an article from the Washington Times, Thursday September 15th. U.S. says it monitored Iraqi messages on gas. If this sounds like a serious leak when you hear it maybe it is but I'm just going to read it to you and you decide. Reagan administration officials said today that the United States had intercepted Iraqi military communications indicating that Iraq had used poison gas against Kurdish gorillas. The officials said the communications by the Iraqi air force were one source of evidence for the United States assertion last week that Iraq had used chemical weapons against the Kurds. Iraqi officials have repeatedly denied the charges. Sounds like someone leaking intelligence. American officials declined to discuss details of the intercepted communication other than to say that they included references to chemical warfare. The officials said that the United States had routinely monitored Iraqi military communications particularly since May 1987 when an Iraqi war plane flying over the Persian Gulf fired two missiles at the American Frigate Stark, killing 37 members of the ships crew.

You know this bit, where American officials decline to discuss details of the intercepted communications, reminds me of an occasion recently when I heard a high official at the State Department was briefing some people on some information that we knew and he said I can't tell you what the source was though. And someone afterwards got a hold of him, button holed him, and said tell us a little more about this intelligence you have. We have to know how valid it was. This State Department official was very well briefed not to talk about intelligence matters and he said you know I can't talk about intelligence matters particularly when it has to do with intercepted communications.

On the same problem of Iraq and Iran gasing Kurds, Pat Tyler in the Washington Post on May 3 this year wrote "A Defense Department reconstruction of the final stages of the Iran-Iraq war has assembled what analysts say is conclusive intelligence that one of the worst civilian massacres of the war in the Iraqi Kurdish city of Halabja was caused by repeated chemical bombardments from both belligerent armies. A little later on the study's authors would not discuss the highly classified sources that allowed them to reconstruct the battle. But U.S. officials and western diplomats are known to have had access to intercepts of battlefield communications as well as accounts from participants and witnesses that reached western intelligence agencies.

Here's an interesting one. NBC Nightly News, January 12, 1989, it has to do with the Libyan chemical weapons plant. Tom Brokow was at the desk and he said "For the past several weeks the Reagan administration has been trying to persuade the world that it has solid evidence that Libya is prepared to produce chemical weapons. Moreover the U.S. accused West German companies of helping the Libyans build the plant. Much of the world, however, including the Soviet Union doubted the American claims. And the West German Government was especially critical of the U.S. charges. Now NBC's Pentagon correspondent Fred Francis has learned details of the U.S. case against Libya and the evidence has impressed the Germans. NBC's Fred Francis has gone to Frankfurt, West Germany to pin down this story. Fred, how was the United States able to persuade the West German government that it had the goods on the Libyans? Fred Francis said Tom, U.S. intelligence sources have told NBC News that they were certain more than 18 months ago, certain because of electronic surveillance that Khadfi was about to produce mustard gas and nerve gas at that secluded site in the Libyan desert. Furthermore the

Reagan administration has evidence that eight months ago Khadfi ordered the plant into a limited test production and gave some of the poison gas it produced to the government of Somalia and on and on and on.

Let me divert for those of you that are not familiar with the intelligence business. Let me point out that there's a difference, a big difference, between revealing that the United States knows that something has happened, knows about what a certain country has done, or about what certain terrorists have done. The big difference is between that and telling the whole world precisely how the United States got that intelligence. Because when you tell the whole world precisely how we got that intelligence, you permit the individuals to fix the system and prohibit us from getting it the next time.

Now I can tell you that these cases that have come to public attention represent the tip of the iceberg. In most cases we can't publicly describe either the leak or the damage for fear of causing further damage. The intelligence community, the defense community, the diplomatic community must often suffer in silence. There you have millions of dollars, painstakingly developed sources and methods, human lives, intelligence critical to the national security, all lost because of careless, often criminal leaks of classified information.

Let's talk a little bit now about specifically what we mean by an unauthorized disclosure. We're talking about the unauthorized disclosure to the media of validly classified intelligence or other national security information. If the same information were disclosed to a foreign agent it might well be espionage. The damage could be precisely the same. I'm a little later going to talk at some length about the case of Samuel Morison wherein there was a big argument as to whether he really should have been convicted under those statutes which were a part of our espionage statutes. It made a big difference, didn't it, whether he released it to a publication or whether he released it to an enemy. The result was all the same. Now we're not talking about information which might be politically embarrassing. Those are a different bag altogether. We're not talking about disclosures of fraud or waste. We're not talking about whistle blowers. Again I'm not even talking about the disclosures in the Department of Justice about a possible investigation of Representative Gray. What we're talking about is the disclosure of validly classified national security information.

Who leaks information and why? The Congress frequently blames the administration. The administration blames the Congress. The executive branch blames the media and the media blames the government. There apparently is plenty of blame to go all around. But lets get the culprits in the right order. First is the irresponsible government official who leaked the information in the first place and then the second is the irresponsible newsmen who prints or broadcasts it. But let's not give away the basic responsibility for this sad situation. For the responsibility is ours, ours in the executive branch. It's our responsibility because we have allowed our classification system to operate without sufficient supervision and oversight. Because we overclassify, because we distribute too widely with too little control. It's our responsibility because we do a poor job of indoctrinating officials and they frequently are not aware of the great sensitivity of the classified material we give them. It's our responsibility because we continue to allow the media free reign to roam the halls of the State Department, the Defense Department and the executive office buildings without adequate control, regulation or recording of contacts. It's our responsibility because we have not fully supported those congressmen who are prepared to legislate needed controls. It's our responsibility because we have not instituted a government-wide system to assure proper coordination of authorized releases.

Who is doing the leaking? Well of course we can't be sure if we haven't caught them and unfortunately we've caught very few. It's my judgement that the leakers are generally middle to upper managers in the executive branch including people at the assistant secretary and ambassadorial level. While there have been some leaks from the Congress, I believe they are minimal, and the house and senate intelligence oversight committees have good security often alerting us to damaging leaks.

Why do people do it? While the underlying cause is generally failure to appreciate what damage will be done, they do it for any one of several reasons. There is of course the ego trip. Well you know I can tell you the real facts that guy down the hall that told you what happened, he really doesn't know the whole story. Now don't use my name but let me tell you what really happened. Don't put my name in there though. The person who has to get his program approved by his department or the Congress. The only way to get it approved is to let the people know what the other side is doing and that the other side already has a program like this that cost more rubles

than what we're asking for. The person who has an important advocate role and must tell the world what the bad guys are doing so it's position will be understood and supported. And finally the person who gives information away accidentally, not knowing or noticing that the material is classified.

And this of course gets back to the basic problem of education. In each of these cases the individual does not intend to harm the United States. Where an individual does intend to cause harm to his organization or to the country, he's not a leaker but he is a traitor among us.

About five years ago Samuel Loring Morison, grandson of the famous naval historian Samuel Elliot Morison, was employed at the Naval Intelligence Support Center. He had been for about ten years. He was arrested, tried, and convicted of providing Janes Defence Weekly, that's a magazine put out by the same people in England who publish Jane's World Fighting Ships, World Aircraft and so on, you've all seen these great big tomes, with classified overhead photographs concerning Soviet ships under construction. The newspapers screamed foul. The freedom of the press was threatened. The Washington Post asked in its editorial, Yes but is he a spy? Tom Wicker in his column in the New York Times on 6 December 85 said "The Morison verdict is dangerous, Mr. Morison is not a spy, he's a whistle blower who thought Americans needed to know more about a Soviet naval buildup." That's why he sold it to an English magazine for bucks, because he thought the Americans needed to know more about the Soviet naval buildup.

Well, nobody said he was a spy. He was convicted of violating a section of the law which prohibits disclosure of classified U.S. Government information to unauthorized persons and that's exactly what he did. It so happens that the section of the law that he was tried and convicted on is in the general category of laws which we refer to as the espionage statutes but again nobody said that he was a spy. The Federal District Court judge in Baltimore, Judge Joseph Young, ruled that officials who make unauthorized disclosures of military or intelligence secrets can be prosecuted under laws barring espionage and theft of government property. He found quite correctly that disclosure of sensitive information to a magazine can be just as damaging to the national security as giving it to a foreign spy.

The guilty verdict was appealed to the U.S. Court of Appeals for the fourth circuit. And I can tell you that at that time those of us who were concerned about this and who had for some time been pushing for that legislation to criminalize the unauthorized disclosure of classified information all went into a quite state, worried about what might happen with this appeal. Because the defense really put together a team. One of the lead lawyers was one that I had tangled with a few years ago, Mark Lynch, who at that time was from the American Civil Liberties Union, and now is with a prestigious law firm in downtown Washington. He sued my agency on something I had done in connection with the Marshall Library Case. Some of you might remember that, so I got to know Mark Lynch pretty well. He's a very good lawyer, on the wrong side of my issue, but he's a very good lawyer. Mr. Lynch was joined on his appeal by 32 news organizations and other groups in an interest in the dissemination of information about the inner workings of government. These groups including the New York Times, this happens to be a New York Times article that I'm reading from, argue that to permit such a prosecution would cut off an important conduit of information that is in the public's interest. Crocodile tears at this point.

The decision of the court of appeals was most interesting and I'd like to read from the concurring opinion of Judge J. Harvey Wilkinson III. Bless his heart, he's down at the fourth circuit court of the United States Court of Appeals for the fourth circuit at Richmond and Judge Wilkinson said "Morison claims he released photographs revealing construction of the first Soviet nuclear carrier in order to alert the public to the dimensions of the Soviet naval buildup. Although this claim is open to serious question, the undeniable effect of the disclosure was to enhance public knowledge and interest in the projection of Soviet sea power such as that revealed in the photographs. The way in which those photographs were released, however, threatens a public interest that is no less important, the security of sensitive government operations. In an ideal world governments would not need to keep secrets from their own people but in this world much hinges on events that take place outside of public view. Intelligence gathering is critical to the formation of sound policy and becomes more so every year with the refinement of technology and the growing threat of terrorism". Boy if he ever loses his job as a judge I can get a job for him. "Electronic surveillance," he continued, "prevents surprise attack by hostile forces and facilitates international peace keeping and arms control efforts. Confidential diplomatic exchanges are the essence of international

relations. None of these activities can go forward without secrecy. When the identities of our intelligence agents are known they may be killed. When our electronic surveillance capabilities are revealed countermeasures can be taken to circumvent them. When other nations fear that confidences exchanged at the bargaining table will only become embarrassments in the press our diplomats are left helpless. When terrorists are advised of our intelligence they can avoid apprehension and escape retribution. The type of information leaked by Morison may cause widespread damage by hampering the effectiveness of expensive surveillance systems which would otherwise by expected to provide years of reliable information not obtainable by any other means. Public security can thus be compromised in two ways. By attempts to choke off the information needed for democracy to function and by leaks to imperil the environment of physical security which a functioning democracy requires." He finished by saying that "the tension between these two interests is not going to abate and the question is how a responsible balance may be achieved."

One of the best judgements that relate to the protection of sensitive classified information that I'm aware of.

Well what can we do about this and what can we say about that balance between the need of the people for information and the need for secrecy to protect valid national security information? There are a number of things that can be done if we have the will to do it. Unfortunately, we don't always have the will. We must develop respect for our classification system by insisting on observation of all the rules. We classify too high, we disseminate too broadly, there are much too many secrets. To a certain extent there is truth in this claim. We have to get after those people who stamp the information top secret when it's barely confidential. Apply the proper administrative sanctions where appropriate. Work towards improving discipline among holders of classified national security information. We must improve our investigative techniques and provide our investigators the best tools that are available, and I specifically include the polygraph here.

Let me divert a moment and talk about the investigation of leaks. Typically when there is a serious leak of classified information, the Department of Justice is asked to initiate an investigation and they require a report with the answers to eleven questions, one question of which I have consistently told them is the craziest question. It says are you prepared to declassify this information for purposes of prosecution? Well heck if I can declassify it, it isn't sensitive and there's no use you going to look for anybody. We have consistently refused to answer that question. In place of answering that question we have said that we are prepared in the event of prosecution to assist you with sufficient information to sustain that prosecution. I'm not going to guarantee in advance to declassify all of it.

The Justice Department will ask the FBI if they think the case is serious enough and warrants it, to initiate an investigation. The FBI will look at the basic information. Who reported this leak? What organization considers that their information has been leaked? And they traipse on down to that organization and they say was this your information that was leaked, Yes. Now did you publish it? Did you put it in a report? Yes. Where did that report go? And so they are shown a list of the distribution of that report. Here are these thirty locations that got copies of this report. Aha. Top of the list, Central Intelligence Agency. Next, Department of State. Next, Defense Intelligence Agency, Air Force, Army/Navy Intelligence, so on and so forth. So they go to these others and they say you got this information in this report. What did you do with it? Did you report it yourself, did you put it in one of your documents and they add up the list of places that might have gotten these reports and they might end up with a list of some several hundreds of locations that might of ended up either with the original report or subsidiary reports that were put out. And with that information they go back to the Chief of Internal Security at the Department of Justice and they say here is what we have so far and typically he will say we can't investigate that. There's too much distribution, it went over too far, there's no way we can investigate that, drop the investigation. The investigation is terminated.

Now I have been trying to preach that that method of investigation is wrong, dead wrong. It's my view that we forget about the distribution. Go to the organization that originated the information and say now what people in which organizations are most concerned about this kind of information. Which elements within the Department of State really go for this stuff or within the Department of Defense. Who is working on this subject? Who has a special interest in publicizing this kind of information and with that you get two, three, four maybe five leads and you go to each one of those leads and speak to those people. Focusing in closely on the people that really had the

special interest.

Now with that sort of approach and further with an indication of where the newspaper man or television journalist hangs his hat, you can focus in on where that leak might have originated.

We must do a better job of developing mutual trust with the media so that they'll more readily accept the government statement of potential damage if certain information is disclosed. Typically right now if you try to tell most newsmen don't publish that it will be damaging, their reaction is wolf wolf, you've been telling that for everything, I'm sure it can't be damaging.

We must establish a system mandated by the chief executive for the coordination of proposed disclosures so that instead of unauthorized disclosures we'll have controlled executive disclosure. And again I repeat by legislation we should criminalize the unauthorized disclosure of classified information.

Now what of the claim that the government is squelching first amendment rights. Nothing could be further from the truth. We not only respect those rights but are actively working for their preservation. Let's not fudge the real issue though. Just as freedom of speech does not allow one to yell fire in a crowded theater, so freedom of the press does not allow one to publish this nation's secrets for the enemy to see. If the media will act responsibly, and if we act responsibly, we might all keep our freedoms and if we don't first amendment rights and other attributes of a free society will all be in serious jeopardy.

Now just let me finish with a few minutes about the most recent efforts of your executive branch to develop a national security directive covering this subject. I spoke earlier that I'm not sure that we had the will to do what has to be done. I'm sorry to say that I think that's true at this point. In late 1988 the DCI issued a new directive establishing an unauthorized disclosure committee. At the first meeting early in 1989, the director of Central Intelligence, Mr. Webster, conveyed to us the importance with which the president views this problem, he wants something done about it, and he wants something done about it soon, and we were directed to prepare a national security directive to attack some of the very problems, fix some of the very things that we thought were wrong.

After several months of discussion it was decided to establish a working group to draft this new national security directive and yours truly got the task of chairing this working group. About a month later we submitted our draft national security directive to this DCI's unauthorized disclosure committee and it took us about a year after that of discussion and argumentation between some departments who thought we were going a little too far, some departments who thought really this wasn't necessary, some departments who thought maybe this was treading on their toes a little bit too much, a little bit too restrictive, so on and so forth, but about one month ago the DCI signed off on this national security directive and sent it to the National Security Council for implementation.

I regret very much to have to report that we now understand that its not likely that there will be a national security directive on unauthorized disclosures at this time. I'm not quite sure why that is, but it may have to do with the fact of political embarrassment in connection with some other cases. But in any event what are we going to do about it. Well we can't just give up and quit and what we are recommending is that a lot of these things that were put into the national security directive can be implemented by the director of Central Intelligence who has statutory responsibility for protection of intelligence sources and methods. And we hope that will be done. This is an important fight that we can't give up on. Some of you are aware that I've been fighting this fight for many years and to quote somebody, I can't remember who it was, I've had it up to my keister in leaks too. Thank you very much.

INFORMATION SECURITY IN THE DEPARTMENT OF STATE

Kenneth L. Lopez
Director, Office of Procedural Security
Department of State

I was reviewing some of my comments that I was going to make and I decided to go into my scrapbook, we all have a scrapbook of our careers and everything, and I pulled out a 1982 NCMS Bulletin and I knew that that would be significant. It was a May-June 82 edition because it followed the 1982 Orlando Annual Seminar. I looked there just to see if anything was said that I didn't want to repeat or I should repeat. In flipping through, I was astounded. I saw the metamorphose of myself and also there were a couple of other humorous pictures in there,

and if you want to see those afterwards I'd be glad to share them with you. It's eight years ago and maybe in eight years from now I'll still have my hair, but it will probably be pure white.

I do appreciate the opportunity to come and address this group. We have a lot of common interests, common career field. When Dave Dittmier and Jacklyn Baker asked me if I would be interested in speaking, of course I was caught off guard a little bit. I hadn't planned on any presentation, but then again I thought this is going to be a good opportunity to try to put a focus on what State Department security is like and look at it from a perspective of our common interest, information security directly and indirectly. A lot is going on and I'd like to just cover some of these points and give you some insight into some of our current activities that certainly are not totally in the Information Security arena.

In the early 80's American citizens serving abroad were literally under siege by terrorists bent on bombing and killing. In 1984 and 1985, 40% of terrorist incidents and a large portion of all threats were aimed at the United States, our diplomats, members of the armed forces, and our business people. In the summer of 1984, then Secretary of State George Schultz named a special panel to sort out what could be done to fight back. The advisory panel on overseas security headed by retired Admiral Bobby Inman presented the State Department with over 90 recommendations and suggested a monumental build-up of security with a new organizational entity to manage it.

The Inman panel's recommendations received strong support from Congress which appropriated millions of dollars for strengthening overseas security. The Inman panel investigation pointed out the urgency of the problem in a very dramatic way. Nearly half of our diplomatic facilities overseas did not meet minimum standards for physical and technical security. The department was told it should replace or substantially modify 126 of 262 overseas missions. A large number of our embassies continue today to be extremely vulnerable to bomb and small arms attack. Embassy staff and our diplomatic facilities were easy targets for violent destruction.

Many of our embassies were also vulnerable in the area of espionage. Our most sensitive information was at considerable risk of loss to hostile intelligence services. We see in the headlines today daily what's happening in the Philippines, Korea, Columbia, Liberia. Although the threat of terrorism and crime against our diplomatic community remains high, the department considers equally important the need to protect our nation's secrets. With the impetus of the omnibus diplomatic security and anti-terrorism act of 1986 and some unfortunate lapses in our security procedures, highlighted by the Moscow Embassy's discoveries and the Lonetree/Bracy cases.

The Department of State has aggressively put into place numerous programs designed to safeguard our information. The Diplomatic Security Act of 1986 placed responsibility on the Secretary of State to develop and implement policies and programs to provide for the security of U.S. Government operations of a diplomatic nature. One of the principle purposes of the Diplomatic Security Act was to strengthen security measures at our diplomatic functions overseas as well as domestically. The act put into place the basic foundation of our present day diplomatic security program. The act established the Diplomatic Security Service within the Bureau of Diplomatic Security which was created in November 1985 as a result of Inman panel recommendations. The size of the Diplomatic Security Organization doubled to about sixteen hundred employees worldwide and now operates on an annual budget of nearly 185 million dollars. Don't be deceived by that amount, $90 million dollars of that is for guards overseas, local guards, supporting the marine guards and domestic guards. The act provided authority to strength certain security programs related directly to the protection of information. The act also provided for a diplomatic construction program which permits only U.S. persons to design and build U. S. overseas diplomatic facilities requiring physical or technical security measures. The act required the Department of State to issue regulations to strengthen the security procedures applicable to contractors involved in any way with diplomatic construction or design projects.

Later the 1989 Foreign Relations Act required that the Secretary of State certify to Congress that adequate security measures have been implemented to insure new construction or major renovations are carried out in a secure manner. Soon after the enactment of the Diplomatic Security Act, the department was faced with the difficult task of balancing the Congressional mandate to strengthen security programs with substantially reduced funding levels brought on by Graham-Rudmann-Hollings. Like other government agencies, we had to weight competing needs against limiting resources.

One method to achieve our objectives has

been through the establishment of comprehensive, minimum standards for physical, technical, personnel and information security programs applicable to U.S. overseas missions. A wide range of minimum standards have been established and are applied to each overseas post based on existing threat level. For example, I think there are at least two dozen. We have standards for TEMPEST, physical security, residential security, RF shielding, countermeasures program, personnel security, storage.

The State Department publishes quarterly an update of a composite threat list covering four threat categories; terrorism, counterintelligence threat, the technical threat, and criminal activity threat. Each overseas post is assigned a threat level of low, medium, high or critical. I won't go into specifics of those because that is a protected list, but you can draw your conclusions where the criticality would be the highest in the counterintelligence area or the technical threat area. We were driven to this because of the dwindling resources. No longer could we work towards correcting the problems by pouring money into solutions. The money was not there. At the direction of the Undersecretary of State, we have been working feverishly to develop these standards and put them in place. The standards are developed within the State Department through the overseas security policy group which consists of all the major government agencies who have activities overseas. All considerations are taken into place and resources and threat.

Let me give you some examples of where minimum security standards were established with the principle focus of protecting sensitive national security and foreign relations information. Classified information processing equipment, and I'm going to elaborate on a couple of these. Classified Information Storage, a particular area I work with daily, secure conference rooms, and controlled area access restrictions. Using the classified information processing equipment as an example, let me just describe how this minimum standards program works. Since each post has a categorization of low, medium, high or critical threat in the four categories that I mentioned, counterintelligence, criminal, technical, and terrorism, some of the standards apply where others don't. In the case of classified information processing equipment, it will vary from low and medium posts to critical threat, where in low and medium we require that all equipment that's used for classified processing be approved by the Bureau of Diplomatic Security and that it be located in controlled access areas. Controlled access areas are those areas of the embassy where classified information is processed, stored, handled, and uncleared foreign service nationals are not permitted without an escort. Classified information process equipment also is under a continuous accountability program where it is shipped from warehouses in the United States or transhipped to warehouses in Europe under 24 hour protection. All the classified information processing equipment must be maintained by cleared American personnel. There are accountability requirements, inspection requirements, maintenance logs, etc. Now the difference in a critical threat area, we just expand the equipment, and any program you have you have a balance of risk that you're willing or you have to accept because of cost things and naturally in low and medium we accept a greater risk because we feel the threat is less in the area that we're concerned with. In critical threat areas, all equipment, copiers, printers, micro-fiche readers, everything is under the classified information protection program.

Let me discuss a little about the classified information storage standards which my office manages. We've had 87 that were published and we've had two revisions since. Basically, to try to address the changing environment, that again, the driver of available resources. What we have in low and medium threat posts is storage of classified material must be in GSA approved safes and they must be secured in secure rooms. This information can only be up to the secret level. All top secret information must be stored in approved containers in alarmed vaults. At critical threat posts, things change quite a bit. In order to store top secret information at critical threat posts, there must be a 24 hour cleared American presence. At non-24 hour manned posts, no top secret is allowed and all classified storage must be in containers within vaults with supplementary intrusion protection systems.

The third example of our minimum standards I want to talk a little bit about is controlled area access restrictions. At one time the State Department had to rely a lot upon the Foreign Service National Employee Community and they still do to a great extent, and we've had to re-look at that for many reasons. And I think it was evidence of problems we had in some of the critical threat posts. We've established within controlled access areas, restricted areas and core areas. Criteria have been established as to who can enter, what escort requirements, and what the minimum investigative level must be. In Moscow, and this was publicly stated in the papers, in 1986

when we got into it with the Russians about expulsions of diplomats, if you recall the Russians retort to what we had done with some of the diplomats, they pulled all their foreign service nationals, some 150 out of the embassy. So there was a time there when there was no help. So that was the impetus to begin and the Secretary of the State pushed to have Congress support replacement of the foreign service nationals with American contract personnel and currently in Moscow we have that. There are approximately 90 employees there now and they do everything from translation to office administration, drivers, cooks, etc. Efforts were underway to extend that in Eastern Europe. Of course with the changing environment in Eastern Europe that is being re-looked. Particularly in terms of the money it is going to cost. I think I've been told it cost about $150 thousand dollars a year to maintain a cleared American in the work force in an overseas embassy.

Let me discuss some other programs involving protection of information directly or indirectly.

Counterintelligence. Recent events have shown us how aggressively the foreign service has been targeted by foreign intelligence services. The department is committed to having a strong CI program. Five years ago I think there were ten people in the counterintelligence programs, now there's 50 and it's interagency staffed. We don't conduct counter-intelligence investigations, the FBI has that authority overseas and domestically. What we do is two areas in counterintelligence. We have a beefed up screening program, and I'll explain a little bit of how we're doing that employee screening program and also have increased our CI security briefings. What do I mean by the screening program. When a person is nominated to be assigned say to a critical counterintelligence threat country, whether the person be a foreign service officer or contract employee or a marine security guard, they're subjected to a very thorough screening program. The records are vetted by a panel consisting of a security representative, a CI specialist, a personnel specialist and a medical specialist. They look at all pertinent elements, the background investigation, particular vulnerabilities that may appear in the person's background, the health of the family, whether a person has ever been overseas by themselves or overseas in a hostile environment. After all these checks are made and there's a pass off, then the person's approved for assignment. We found in the counterintelligence arena that there was not adequate coverage in making people alert of the hostile threat in overseas environments. Now we have requirements that before deployment from the U.S. all persons undergo very thorough briefings. We have specialty briefings for groups of contractors that are going over such as construction, security people and foreign service officers. Than at post they also receive initial briefings of the CI threats unique to that post and are accorded refresher briefings. We have at all the posts in the world counterintelligence working groups, which is a representation of all the agencies that are tended at the embassy and they meet regularly to discuss the various CI issues, awareness programs, and the threats that may have come about. We're in the process of establishing three regional counterintelligence centers around the world that will be in a position to deploy to those areas where there are particular problems in the counterintelligence arena. A recent happening in the counterintelligence area happened in 1989. The department implemented NSDD 197 reporting foreign contacts and security awareness, through the issuance of our 1989 relationship contact reporting policy. This policy imposes reporting requirements whenever U.S. citizen employees assigned to an overseas mission have other than official or casual contacts in conversations with nationals of particular countries and organizations.

Let me touch on a couple of other areas that have an impact on protecting information that the Department of State is entrusted to protect.

Industrial Security Program. In mid 1985, the department had many contracts, and procurement actions that were classified, but that was at the very beginning of the overseas construction program. Once we developed the procedures to strengthen our construction security program, it drove the need to have classified contractors. We are a user agency in the Defense Industrial Security Program, and we now have over 500 classified contracts dealing mostly in overseas construction related matters. The architects and engineers that design our embassy's, contractors who construct sensitive parts of the embassy involved in communications facilities installations, our cleared American guards, and our construction surveillance technicians, all from the private sector, are all under the Industrial Security Program. Computer Security. Protecting information in an automated mode. We all know what the rapid growth of automated information systems has done to the information security world. We're in the process of developing a multi-million dollar telecommunications network which will link Washington with all overseas posts. Minimum standards have been established for the use of automated information systems and the use of personal computers. We

have information systems security officers assigned to posts around the world where classified automation is a large program.

Emergency planning. A fallout of the Inman report certainly focused on what happened in Iran and what to do with classified information during times of emergency. Since then we've established an emergency planning function which is well staffed and have periodic crisis management exercises. There's a world-wide program of information management specialists who visit the post and provide the post guidance on reducing classified holdings. There are minimum destruction times established for classified information and prioritization of what information must be classified. It's been very successful in reducing the amount of classified overseas.

Let me talk a little bit about the implementation of EO 12356 in the Department of State. The office that I head is responsible for administering information security in the Department of State. In 1986, when I came to the department, I was well aware of the status of information security as this group knows it, which includes classification management, safeguarding and protection if classified information and could see the challenges there. The Inman panel and other outside audits and evaluations recognized that there was a problem in information security management within the Department of State. It suffered from low visibility, fragmented responsibilities, poor oversight, and really a lack of an effective program. Information security took a back seat to counter-terrorism measures, physical security upgrades, and counter-espionage programs. We understand that those programs are still important, while we have killings and kidnapping and assaults on American citizens. But what's happened over the years, and we're reversing that now, is that information security took somewhat of a back seat. It fell off the screen of the security mosaic where information security was one of the pillars. After four years I think we're now on the right track.

State Department Management, based on recommendations and what was presented to them by outside oversight organizations, supported the information security program by increasing the staff from 5 to essentially 20 personnel. Organizational changes were also made by moving the information security program out of information management into the security apparatus. We've done a lot of things to progress towards where we want our objectives to be in security awareness briefings, classification guides and stepped up oversight. There's certainly a lot that needs to be done. We're competing for the attention of resources and management support, commitments from management, commitments from personnel, and commitments from the foreign service. We're getting it but it's not easy. We're all sales representatives, just like you are in your firms and your agencies. Information security has never been recognized as a glamorous activity, particularly when you put it in the context of today's contemporary issues of terrorism and counter-espionage programs.

We need to increase our efforts to train and educate folks in the foreign service community and our professional security officer corp. Many people who recently had come from the law enforcement community, were not ingrained in information security responsibilities. I can see that at some posts, such as Manila, probably information would be down on your priorities right now, but it's our job to put that on the same plateau as the other programs. It's a challenge and it's not going to be easy, but I think I can stand here and say that many of you face the same situation in your organizations, but I think there's a willingness to do that and I believe there's a commitment. I know there's a commitment to support our efforts in this direction. We want to institutionalize the information security program. There's a lot going on in the State Department and I think I could speak in many areas that relate to protection of classified information but I wanted to give you an overview of where we stand in information security, where we've been, where we're competing with other interests, and where we need to go. We've made improvements but we must keep up the momentum.

The decision has been made by the administration to raze the new office building in Moscow that had the problems with the technical penetrations and that's on public record. The problem is the funding. The existing embassy building is under a multi-year programmed upgrade to make that more secure for the period that it's going to take to fund and rebuild the new embassy complex. We figure another five or eight years perhaps in the old embassy. The Administration is solidly behind razing the new embassy complex and rebuilding.

INFORMATION SECURITY - A MILITARY PERSPECTIVE

Col. James R. Linnen
Director of Counterintelligence and Security Countermeasures
Office of the Deputy Chief of Staff for Intelligence
Department of the Army

I'm very happy to be here, it's always a pleasure talking to security professionals. It's a little bit like preaching to the choir in some cases. I don't have to convince you of the need for security, but it's a different choir so I'm happy to be here at this choir. I see a lot of familiar faces here and a lot of people I haven't had the chance to talk to before. So what I want to do today is go over my perspective on how we protect information in the Army, basically how we are trying to secure the Army in the 1990's.

It's a very rapidly changing world. I work as Mr. Reynolds said for the Office of the Deputy Chief of Staff for Intelligence. This is the old ACSI, if you remember from the old days. We are now Deputy Chief of Staff which means that the two star became a three star which I think is a good reflection, at least General Eikelberger, my boss, thinks so, of the importance of intelligence and security in the Army. It puts us on a co-equal basis with the personnel community, with the operations and logistics community. So it's very important to us.

What I'd like to do is run through a few slides. It's part of a review we're doing right now on security in the Army. This is not an official DA position but this is basically what we see. It's kind of my view of the Army from my foxhole. I'm a product of the Army. I've been in the Army for twenty eight years. I worked security since my second job in the Army. I was a security officer of a 24th Infantry Division in Augsburg, Germany many years ago when the Mark was four to one and the wall had just gone up. I was there in 1963. The world has changed a lot and our Army is getting smaller and we're trying to sort through how we are going to do that.

I am aware of the challenge I have in talking to you today. I used to teach at old Fort Holabird. Some of you remember that. During the Vietnam era we had a lot of soldiers going through there. To get all the soldiers through we would teach classes on Saturday and I had the unfortunate honor of teaching a class at 6:00 on Saturday morning. That reminds me of being the last speaker at a conference like this. We had a class called 97 Deltas in the old days. They were the counterintelligence typists and they had a room of 50 typewriters and 50 bloodshot eyes sitting behind the typewriters because everybody had been downtown on East Baltimore Street the night before. No one was thinking too much of the block of instruction I was giving which was something fascinating like the organization of the corp support command or something like that which is kind of hard to teach.

At any rate there was one young man sitting right about where Dave Keene is sitting and he was trying hard to stay awake. You know he wanted to be good but he was losing the battle and what he did is he got his elbows up on the carriage of the typewriter and he got his chin underneath it and he was going to stay awake. Well he lost the battle, fell asleep, and his arm hit the little lever. For those of you who are young, you don't remember this. Typewriters used to have levers on them and when you hit them the carriage went this way and the bell rang. There he is laying right there in the aisleway. I'll never forget that. If I get boring and Dave is laying there in the aisleway, I'll know I've got to change my pace a little bit.

I'm going to run through basically five things. I'm going to talk about some of the background we've had in the Army in our security business and counterintelligence business. I work both sides of the house; counterintelligence and security and the Army does that institutionally. I think it works very well. I'm going to tell you what we've tried to do with the resources we have, what we see as our developing needs and a few comments on cost and security and what's cost effective and what isn't cost effective.

First of all I'd like to go into a little background of what the Army has been through in the past five years. Now this is not all Army, in 1985 there was the year of the spy, that happened to be a Navy production. We can't take credit for that but the Walker case was the event that really hit the Department of Defense and the American public right between the eyes. We have serious, serious problems and what brought this on, how can we fix this. We went through a lot of soul searching. In 1986 a very important event, General Stilwell, a very respected figure, ran what I still consider to be the best review and survey of what is wrong with security and what we can do to fix it. He came out with a little red book which I still keep on my desk and it listed many many things that we have to do to try to fix security.

The Senate and House Committees got interested in it after that and did some very good work. I saw Britt Snyder was here to talk to you. I would like to say to you that their work and their investigations and our interactions with them have been very very useful to security. I came into my job without having had contact with Congress before and with the committees. They've done a very good job, the professional staff and the Congressmen and the Senators. They're very interested in it. They're very smart people and you don't have to give me any idiot lessons. They ask me very good questions and I think that's been a very very useful relationship and we value that. But anyway they put some reports out. Other things have been published.

All of these things I would like to point out have resource impacts. All of these things told us that we ought to do more things. At the same time we were losing people to do things because of cutbacks here and there and so on and so forth.

For us 1988 was the year of the spy for the Army. The Army got hit very very hard. Clyde Conrad was an operations sergeant in a division in Germany. A trusted agent. A clean record. A model NCO at least on the surface and Clyde Conrad sold the farm. Did it very cynically, did it very effectively. We had tried to find Clyde Conrad for about eight years. All we knew was stuff was getting out from a unit in Germany. We have a lot of units in Germany and in an investigation we found Clyde Conrad and as you've heard recently brought him to justice in West Germany. West Germany gave him a life sentence. By far the strongest sentence they've ever given anybody. The day the Germans arrested Clyde Conrad was the day I learned of the next individual there, James Hall, who was a signals intelligence soldier, also a trusted agent, also a clean background, also a good man on the surface.

At the same time we were hit with INF treaties. We had Russians coming to see us and we were going to go see the Russians. We were having barbecues with the Russians. Where did the threat go, big challenge. This continued through 89 and into 90.

We participated in National Security Review 18 which was directed by the President and is now going through the National Security Council process. This is a broad description which shows where we should be going. Concurrently with this the Senate Select Committee on Intelligence asked Mr. Jacobs, former Army intelligence by the way, I'm proud to point out, respected business man, owner of the Baltimore Orioles, to head a panel which has some very good people on it and they looked at security. Retired Admiral Bobby Inman, former boss of Mike Levin here, I'm sure was a key member on that panel. So we've had a lot of help to point out what we've known all along. We have some serious security problems. Problems that are of a magnitude different than the problems I worked with in the 60's in Germany.

So what are we going to do about them? We haven't been sitting on our haunches. We haven't been just doing nothing. Some of the things that we have been trying to do in the Army and that we've been working hard on are to tighten up our policy and reduce work intensive procedures. We have been and we're going to continue to take a very hard look at things we do in the Army in the security field that don't really add value, such as bookkeeping things, report submitting and reports that cause a lot of work for security people in the field. We'll also look at industrial security things, across the board, things that are work intensive that require people to do them which may not be the most important things that they ought to be doing but because somebody's demanding that report or checking to see if they initial something or other it's being done.

Moving ahead to CI operational capabilities and counterintelligence operational capabilities. The Army has put a lot of effort and a lot of money into training, making sure our counterintelligence people are doing a good job. I am personally convinced that one of the best tools that we have to improve security in the Army is to penetrate the enemies intelligence effort and that is what we are trying to do and have done successfully in the key cases that I talked about earlier. Army and other other national agencies have done a good job and we intend to do a better job through classified operations which I can't talk about at the Hyatt but they are very effective jobs. I'm talking double agent operations, I'm talking penetrations, recruitment of the bad guys who want to become good guys, who want a change in jobs, let's put it that way. That's very effective. We found out recently in a case that we had a young soldier who was about to follow in the footsteps of one of those earlier spies, the Conrads and the Halls, and we gave him a chance to make some money and he said oh no no no, I'm not going to do that. He said Army intelligence will catch me and I don't want to go to jail and I think we made a point there. A good point. We

can't keep all of America honest by fear or by some kind of a PR campaign that Army intelligence is going to catch you. But I feel we can make a lot of inroads and we can do more and more with some of our good counter-intelligence operations which enhance our security. It's a two sided street, a double edged sword.

I want to also highlight polygraph. We have put a lot of time and money into polygraph. Polygraph is the most contentious issue and the most emotional issue I've had to deal with in my three years as the Director of Counterintelligence and Security. We live in a free society and when we ask somebody to come in and strap up to a machine and basically answer four very simple questions a lot of people say what's the problem. What's the problem with asking somebody are you in contact with hostile intelligence. On the other hand, where you have the potential for damaging somebody's reputation, where you have the potential for doing something wrong to somebody, we have to make absolutely sure that we do that absolutely right. Security in the Soviet Union is much simpler. We don't have to balance individual rights against the security needs of the Army or of the United States or of the Soviet Union. Security always takes first place. It has to be balanced here in our constitutional government and that's why we have the freedoms we have. That's why we have a security force to protect those freedoms. So it's a lot harder but we are doing a lot of work on that.

The opinion of the community that I work with is that polygraph is by far the most effective deterrent from somebody going in and selling their country out. When you're trying to stop somebody who has no standards and no morals, who on the surface is a very good soldier or civilian, if he states that with a polygraph that's the only thing they say would have stopped me. They all say that unanimously. So we're continuing to push on that working closely with the Department of Defense, working closely with Congress to make sure that we do it right, that we don't get the right to do that polygraph taken away from us, but the counter-intelligence scope screening polygraph is a very important tool and we want to continue using it.

Some of the other things we all do in the industry, the awareness things, they're very important. We are quite proud of the call spy hot-line. I think that was a very innovative thing. It's a good safety valve for somebody who doesn't want to go see the security manager about something. Dial 800-CALL SPY. It's on everybody's phone. I was briefed on this and I said does it work and they said well sure it does. I picked up the phone and punched in 800-CALL SPY and sure enough there is Miss so and so on the other end of the line. So it works. We do get lead material out of that. We haven't caught a spy with it yet. It doesn't cost us much. 800 numbers are quite cheap so it's a good source of leads and we're going to continue to do that.

I want to talk about where we feel we need some priorities and where we feel we need some help in the Army. I talked to my leadership about these and I don't have to beat down doors. When I worked security 20 years ago you had to fight your way into the boss's office to get him to listen to security. You don't have to do that anymore. The boss is calling you. They're saying hey G2, hey security guy, what are we doing to improve our security. So that's good. We have a ready audience. We are asking our leadership to endorse security, METL is an army term. I hate to confuse you with acronyms. It's mission essential task list. These are the things that all commanders put on their list of things to do and the things that they're grading on. We're adding security to that. It's going to be as important as logistics or as important as reenlistments or as important as some of the other things that they're doing. It's hard to grade people on security. It's important that it be on their list of things that are important so we're adding that.

We don't have enough security training in the Army. Training has been salami sliced over the years and cut back, cut back, and cut back to the point where I am ashamed to say that right now we don't have a security manager course in the U.S. Army. That is not a happy state of affairs, so we're getting that turned around, that has to be turned around. We cannot expect Mr. Ev Gravelle in the DoD Security Institute to pick up the slack for the whole Army. I'm not saying there isn't security training in the Army. There is quite a bit of security training, but there's no centralized security manager course for our people in the Army so we're getting that pushed back in.

The Army is going through a lot of cuts right now. We're getting cut, everybody's getting cut. That's not all bad but when you're getting cut and you're cutting security forces in the Army, a lot of the security element, security offices are small already. And when you cut them even further you reach the point where they're ineffective. We are convincing our leadership and we have willing ears that we not take a proportional cut of the cuts that are coming around in the Army.

This is painful because if we don't take our share as they call it, they being the other people, somebody else has to and who is that somebody else. You all go through this in your lives too but this is something that we fight daily and we have receptive ears to this. We're asking for a lot of other things that I think are important. I won't go through any of these details as a lot of these things are still in a staffing process. We were putting more people into our counterintelligence effort. More training in the polygraph area. We're working hard on that. Research in polygraph, we're getting more money for that.

Something that a lot of us tend to overlook is that security is a people business. Quality people are absolutely essential to securing any organization. The Chief of Staff for the Army has a list of about six priorities. Number one on his list is to maintain the quality of the people in the Army and he is willing to spend dollars that he was going to spend for tanks. The Army went to Congress and said we're going to cut back on tanks. In fact we're going to stop building them in 1992. Congress went crazy. They said you can't stop building tanks. Somebody from Michigan said that of course. Maybe he had a parochial view about that but that fight is still ongoing. But what we are doing in the Army is that we are continuing with every program we have to ensure that we recruit and maintain and train a quality force. That makes my job and my people's job and the Army intelligence and security command's job a lot easier because they don't have as many investigations to run that go derogatory. They don't have as many concerns about people. When the Army had to go out and really sell the Army to make the volunteer work, we had a quality problem that was pretty severe for a while, measured by traditional measures of quality. We had people coming in who had police records. We had people coming in that could not be granted a security clearance. Overall that effects the quality of the force. So we don't have to make those compromises anymore. So in cutting back the Army we can keep the good people and we can only let in the people that we want to let in across the board, be they military or be they civilian. So that's the plus side of a smaller army.

Everything we do in the counterintelligence and security world to maintain the quality people and find the people who aren't quality is value added and that's why I'm very much in favor of a lot of the efforts PERSEREC is doing. Trying to determine how we determine if somebody is quality and if we want to keep them or if we don't want to keep them. What type of investigations bear fruit and which are a waste of time. How investigators write up their reports. PERSEREC just did. I just got the draft of a very interesting report on how investigations are done and how they should be done. These are very worthwhile things. I haven't seen Dave Keene fall over into the aisleway yet so I think we're home almost free.

A few thoughts on cost. Security costs. Good security costs some money. It isn't all that much in the overall scheme of things, but it costs some money and we have to sign up for that. We have to bet our bosses to sign up for that. We have to make sure we give them value for their money. They see the security office as just a bunch of negative people that sit around, who are interested in just putting in eight hours a day, and not accomplishing anything or not being proactive. They don't see what they are getting out of security and they say hey it doesn't do anything for me, you know I'll put that money into something else. We have to be able to tell our leadership this. Smart security and good security can also save some money. One of my people got a very nice phone call yesterday. We went to an Army installation north of here. Some good security work had saved millions of dollars in new construction that was going to be done. Whoever was designing the things said you need this, you need this, you need that. We got in before the place was built and said you don't need that. That's not necessary. That standard doesn't apply anymore. You need this but here is a cheaper, equally effective way of doing that and we've got a commander up at a major army installation north of here who thinks that army security is okay. These folks helped him save some money and were there pro-actively, before he sank all that money into new construction. What we normally do is come around after they do it and say no, no, no, you did that wrong. The door isn't supposed to be three quarters of an inch thick, it's supposed to be an inch thick. You know, take the door off, put a new door on, so on, and so forth. These are very important things.

We've done a lot of review of the bidding on TEMPEST. Where we're going to apply our TEMPEST money. Where it's cost effective to apply TEMPEST money. We save millions of dollars on that. We're not saying that money shouldn't be spent on TEMPEST, it's where you spend it, where it's smart to spend TEMPEST money. We've had good interaction with the National Security Agency and the national committees that do that. We've saved the Army that way. Money that goes into other things that provides security in other areas that are

desperately needed. Computer security is a humongous problem and humongous challenge. So there is where we're going to be putting some money.

My bottom line there is inadequate security is cheap up front. You can probably spend nothing on security and maybe get away with it. But in the long term from the Army's perspective, it degrades force protection, it can present unacceptable costs on the battlefield. I'm very gratified that Joe introduced me by talking about security of Army weapon systems. I've worked for over ten years on securing army weapons systems. Black programs. I've been involved with that deeply, trying to pick out the crown jewels, the weapons that are really going to make a difference, that will deter the Soviets, when they see or hear or learn, which they will eventually, that we've got this wonderful weapon system they're going to say, hey, we can't match that. We could spend billions and I think that thought process went through Mr. Gorbachev's mind. We could spend billions trying to catch up with the M-1 tank; and the other services, what they've done with the Trident, with the new strategic missiles and things of that nature, but it wouldn't be worth it. Our country would be bankrupt and I think that went through his mind when he decided to say hey, enough is enough, and start building down. So money spent on good weapons system security is money well spent and we're going to continue to be doing that. Money that is not spent in that area is penny wise and pound foolish and we can't afford to do that.

Those are the things I wanted to talk to you about. Those are the things that keep me busy. I don't have a huge staff to do the things I do, none of you do. I can assure you that we're working hard on it. I brought along Mr. Jim Passerelli who runs my security countermeasures division. We're busy people. We're out there trying to find out how we can do the job and do it well and I appreciate very much the opportunity to talk with you.

INFORMATION SECURITY - A MANAGER'S VIEW

Richard A. Black
Director, Corporate Security
SRI International

I've been asked to deliver the keyhole address to our convention. The other guy says you must mean the keynote address. It's for the National Association of Security Officers. Now I've also been told in my days at the Pentagon, Jim, that no briefing was complete without a pie chart. And so I brought a pie chart. Yesterday, those of you in this room heard Art Fajans, a very dear friend. And I told Art after his presentation yesterday that I wanted to take a couple of ideas that he presented to us and sort of use those as the initiation of my presentation. I'm paraphrasing from Art because he was speaking so rapidly that I couldn't call up all the words but he did say that security is seen as a separate entity and not a part of the whole. When resources are reduced, security will lose resources. How many of us have experienced that factor. He also said, tack on security is counterproductive, inefficient, and unacceptable. But that's how we've been doing security traditionally, tack on.

Security must be integrated into systems from inception and throughout the life cycle. How many of you have read Mil. Standard 1785? Well, both of you are in good luck, because that is going to be the future standard and all of you would do well to read that epistle. Trying to find something that I could use as an image to sort of hang the ideas that I'm going to throw at you this morning, I was sitting at my desk thinking about a present for my son's birthday and I thought I would go down to the local railroad shop and pick up an electric train. And so I went, I was walking around, and do you all recall in your youth an unguarded railroad crossing somewhere in the vicinity of your home and there was this big pillar with the crossed arms that said railroad, stop, look, and listen. And so if you can carry that image in your mind this morning, this presentation will be based upon stop, look and listen.

First of all, stop apologizing for being a security professional. Security is a company asset, like all the assets, it costs money to get and to maintain. Don't be ashamed or apologetic about it. It's a fact people are an asset that costs money. Facilities and equipment are assets that cost money, real estate is an asset, so it is with security. In most organizations security is an overhead activity. What is your company getting for its investment in security. Stop keeping your staff locked up. A security staff is a support organization providing an essential service to management and the rest of the company's population in meeting their responsibilities and in fulfilling their roles. Security is a service industry. And the management and employees of your company are the customers of their service. It's essential to the success of a security program that our customers be

involved in both the development and execution of that program. The result of this effort will be a larger security staff. Keep your staff up to date. Many of your companies have in-house training and development courses. Seriously consider enrolling security staff in computer courses, stress management, time management, effective writing and how to deal with irate customers. It will cost you some time in the short run but the long term benefit gained will more than make up for it in the improved productivity and in customer relations. When was the last time a security staff member attended a professional workshop? Send them. But a quid pro quo. Send them with the understanding that on their return they have to conduct a meeting, class or workshop to pass on the information gained to others on your staff. That's your return on investment for having sent them. Stop to dream, to contemplate the what if. All of us get tied up in the day to day ongoings of our jobs. We frequently miss reading sign posts, we frequently don't understand things need to change.

Stop, sit back, think. Stop the do it myself syndrome. You cannot do it alone. We're frequently thought of as short sleeved managers. The connotation is that we pitch in to get the job done and I realize that in companies with small staffs that is essential, but how many of us do it because we are reluctant to delegate. How many of us still think that if I want it done right I need to do it myself? You are doing yourself and your subordinates a disservice. First, your depriving yourself of time to dream, contemplate time. Time to sit back and look at what you're doing and how you're doing it and contemplate how to do it better and more efficiently. How much more could you do with the same resources? Second, your depriving your subordinates of opportunities to enhance their professional and personal skills. The best learning experience is hands on. Actually having to do something. Give them the opportunity to grow. Use the opportunity to train and develop your staff. If you delegate, two things will happen: 1) the skill and professionalism of your staff, whatever its size, will increase; and 2) you will find yourself with more time to find creative ways to add value to security services for your companies. Stop using the N word. No. No customer wants to hear the word No. Take it out of your vocabulary. You are security professionals. You belong to the National Classification Management Society. That says you are a professional. A few of you out there said you also belong to the A Organization. You may or may not be professional. Stop the faceless name society. Every day in our offices we accept telephone calls, we talk to these people for years. We never meet them, we could pass like two ships in the night, never knowing each other. When you have the opportunity, personally go and see the person to whom you are talking. Do not send memos through interoffice mail, go personally. You have two opportunities. 1) So that you are recognized; 2) You show them that you want to help. and there is a third corollary, you get to do a little security education. Stop using a negative philosophy. In the old days we did security by check list. We carried our four and a half bible with us and checklist after checklist after checklist. We walked in, did our jobs, left the deficiency report sitting on someone's desk, and said we'll be back in ten days to reinspect. Well folks, if we have the capability to find those deficiencies, we have the capability to fix them. So do it then.

Change the negative philosophy, get positive about what you're doing. Stop talking about challenging requirements. I know that the ISM now has a thing that charges us with the responsibility to challenge classification. When you challenge, what you are telling whoever wrote that document is that they are wrong. You just set up a lose lose situation. Don't challenge it, discuss it. Perhaps bring some factor to their attention that could make it a win win situation. Try to change the way things are done by being positive about it, not being negative. And stop griping about stupid government policy. It isn't stupid. The people who write this policy have good and cogent reason for why they are doing what they are doing. There is however a missing factor. Many people who write policy do not have experience down where the rubber meets the road, where all of you come from, so it is incumbent on each and every one of us to bring to the attention of the people who write policy how that policy should be written so that we can properly implement it.

I move to look. Look. Look at the areas within your responsibility. Human resources. Hiring, firing, promoting, demoting, drug testing, applicant prescreening, pay equity issues, finance and accounting, budget preparation and implementation, purchasing, cost benefit analysis, capital funding, health and safety, hazardous materials handling, toxic waste disposal, emergency systems, and the list goes on and on, security engineering, facility engineering, telecommunications and data processing issues. All of these things fall within the responsibility of the current security staffs. Look at your security policy. Know your corporate culture. What is acceptable and how can it be implemented.

Start with your security policy. This policy statement is your charter. It tells you what the company wants done, review it periodically, ensure that it says what you need it to say. Does it specifically designate you as the responsible individual to implement security policy? Does it include all of your responsibilities? Does it grant adequate authority to accomplish those responsibilities? Look at your mission statement. Review or write one if necessary. This mission statement translates the policy into action. The mission statement tells the organization how you will do what the company says it wants done. Review your company mission statement or charter purposes. Your security mission statement must be congruent with the overall mission of the organization that you serve. The formulation of the mission statement should answer the questions. What function does the organization perform? For whom does the organization perform this function and how does the organization go about performing this function? Look at how you look. What's the image that your security staff portrays to the customers you support internally and externally. Would a uniform change make a significant improvement? Would a coat of paint on the guard shack out there make a difference in your image? What's the image your company wants to portray? Is the first person you meet when you walk into a new company a guy in a plain brown uniform with a pointy star tin badge on his shoulder with an eight pointed hat. Or is it a sharp looking young lady in a blue blazer and a gray skirt with a white shirt and a nice logo tie. There is an image you wear of how you look.

Look at where you are. Where the security organization is placed on the organization line and block chart says a lot about how your company perceives security. Are you an ABC organization with security sitting down here as the foundation holding up the entire superstructure? Or are you XYZ company with exposures at the highest level of management within your organization. I have the dotted line security director of the CEO because that is ideal. Most of us are in the second category where we report to the next line management. Take a look at where your organization is. It says a lot internally and externally. Where are you physically? How many of you on the installations of your company are out in the back 40 someplace? How many of our offices are in the basement with little or no visibility? Where you are physically says a lot both internally and externally.

Look at what you can do to support your company goals. Some of you may have heard me, I think it was Tuesday, in the PERSEREC section, where I made the comment that I have said publicly and privately, it is not possible to me as the Director of Corporate Security for SRI International to provide security to that international organization with a staff of 40 people. It is impossible. But if I can get the people whom we support to buy into the security program, its a very easy matter to provide security to SRI International with 2800 security staff. When you convince the staff to buy into your programs, you want to be sure that you understand what their goals and objectives are because they must become yours. Look at your personal management style. Do you beat people about the head and shoulders to get things done? Do you talk to them? Are you consistent with how you deal with your own security staff and the people that represent you in the operational staff? Take a look at your personal management style. Listen. Listen to your company.

Now I've been on this one for quite a while. Do you really know what your customers think of security? Security in general has historically had a negative image. The enforcers, not team players, merely an extension of the Department of Defense, security always says no. These are quotes from responses to a security survey questionnaire. These are extractions from another security questionnaire. Does this tell you anything about how the security staff is perceived by people whom it supports? What's the other side of that coin? The other side of that coin is how your security staff feels about itself. Everybody treats us like cops, nobody tells us anything until its too late. Nobody consults us until its too late. People are always trying to break the rules. Nobody wants to understand the rules. They only ask my opinion when they're really in trouble. Well friends, I have to tell you that those of you out there who are in security management at any level have a massive job because it's to change those perceptions, both your staffs and the people you support.

In conclusion, the effective security manager of today, is one who knows what his or her company wants done, fully understands the cultural environment, clearly specifies how the company's security policy will be accomplished through a coherent and acceptable mission statement, listens openly and attentively to both customers and security staff members, stays attuned to the needs of customers and the modulations of national security policy, takes advantage of state of the art technology and recognizes both the need and the benefit of change.

So stop, look, and listen.

Thank you very much.

Q. What's the single most valuable thing you've done to turn around the perception of security in the office?

A. Get off my butt and go walking. It is absolutely essential that security has positive visibility. I think it was Hewlett Packard or I believe the Apple Corporation that started the MBWA, management by walking around. I'm a firm believer. Get out there, it's amazing what you'll find out cruising the halls of the institute grounds, 72 acres and 43 buildings on site, stopping in a strange office some place and just sitting down and saying, hi I'm Dick Black, what is it that you do? It's amazing what you'll find out and it's amazing what you will find out about how they perceive your security operations. I mean there are 2800 people on that site, I don't know them all and most of them don't know me. So it's nice. The other thing is get visibility. In most of your companies you probably have supervisor counsels or management counsels of some kind, you may have staff advisory working groups. Get involved. Show the corporation that you are indeed a team player. If you hide down in the cellar, if you're sitting in a shack in the back 40 someplace, you are not going to be able to impact positively in a visible role. You've got to get involved. Get out, get visible. I think probably that's the best thing, the easiest thing to do to turn around the perception.

Thank you very much; its been a nice conference.

SECTION II
Business Meeting

THOMAS J. ADAMS

Tom's first career began with the Air Force. In the course of 20 years he enjoyed assignments in Texas, Hawaii, Florida, California and the Philippines. Tom's former employer also provided him with exposure to Lockheed. His final assignment involved duty as the Senior Security Specialist for the Lockheed Strategic Reconnaissance SR-71 Aircraft Program. Tom takes great pride in the fact that he was associated with the Lockheed Skunk Works Team when the SR-71 established the world absolute speed and altitude records (New York to London; London to Los Angeles). His other Air Force assignments included flight duty as an Airborne Command Post team member and other classified tasks.

Tom began his second career with Lockheed Missiles and Space Company in the Special Access Program arena. Presently Tom is the senior Security Manager for all DoD SAP/SAR activities at the 23,000 employee facility. He has over 20 years experience in the DISP and Special Access Programs. Tom has been active with Aerospace Industries Association CODSIA Cases; is the Chairman of Contractor SAP/SAR Working Group Personnel Security Committee and the National Management Association.

Tom's hobbies include reading, photography, golf, baseball (former Little League/Babe Ruth baseball president - 10 years). Tom was born in New York City on January 19, 1940 and has an older brother.

CRAIG ALDERMAN, JR.

Mr. Craig Alderman, Jr., currently is serving as the Deputy Under Secretary of Defense (Security Policy), a position he has held since April 1985.

Mr. Alderman was born at Fort Benning, Georgia. He attended the United States Military Academy and graduated with a Bachelor of Science Degree in 1952. He also has earned a Master's Degree in Political Science from Auburn University.

During Mr. Alderman's early military career, his assignments were principally to troop units in Europe, the United States, and Asia (including combat service in Korea and Vietnam). He also gained research and development experience with the Royal Armoured Corps and the U.S. Armor Board, and served as his branch's representative and senior instructor at the U.S. Military Academy. He is a graduate of the Army Command and General Staff College and the Air War College.

In the late 1970's, Mr. Alderman was international military marketing manager for an American defense producer, before joining the Office of the Secretary of Defense as the Director for Emergency Planning in 1981.

Mr. Alderman is married to the former Rene Goodlet of Melbourne, Australia. They have a son, daughter, and two grandchildren. The Alderman's reside in Fairfax, Virginia.

JAMES J. BAGLEY
(Life Member)

Mr. Bagley was born in Boston, Massachusetts, December 6, 1915. He has been educated in Financial and Business Management, Social Sciences, Law, Economics, History, and continuing education since 1933. He entered the continuing education since 1933. He entered the military service in 1940 and continued military and civilian service until his retirement in 1975.

Mr. Bagley established R.B. Associates, Inc., which provides consultation in: Management and systems analysis; technical information systems; technology transfer; information security systems; export; systems for identification; and contract management. He has served as a consultant to U.S. and Foreign governments and U.S. and Foreign companies. He has published and/or presented over 100 technical papers.

Mr. Bagley is a life member of the National Classification Management Society. He also is a member of the National Security Industrial Association; Foreign Policy Association/World Affairs Council; American Defense Preparedness Association; Armed Forces Communications and Electronics Association, New York Academy of Sciences.

JACQUELINE F. BAKER

Ms. Baker is the Program Manager for Security Education and Awareness for all Department of State employees worldwide. The program is currently located with the Bureau of Diplomatic Security, Office of Procedural Security and entails coverage with the industrial, physical and information arenas. One accomplishment this past year, has been the

development of a "New Look At An Old Theme" in designing and implementing an information security briefing (refresher) for all Department of State employees. In addition, Ms. Baker is the Department's representative to the Security Awareness and Education Subcommittee's "Security Briefings Course". Her career in security spans sixteen years, with the initial thirteen in the industrial community. She was awarded the James S. Cogswell award in 1986 for superior performance in the conduct of the industrial security program and has been an active member of NCMS since 1982.

RICHARD A.BLACK

Richard A. Black is the Director, Corporate Security for SRI International with Headquarters in Menlo Park, California. Before assuming those responsibilities in 1984, Dick spent over 22 years in Army Intelligence and Security. He has been the Contractor Special Security Officer for the Department of the Army and Chief of the Security Survey Division of the 902d Military Intelligence Group, responsible for providing both advice, assistance, guidance, and interpretation of government security regulations to both the military and industry. He is a member of ASIS and NCMS, a member of the steering Committee of the Research Security Administrators of California, and a member of the Security Subcommittee, National Security Industrial Association.

IRV BOKER

Irv has spent the last 12 of this 35 years with GAO as the Evaluator-In-Charge of reviews of the protection of national security information. During that time, his group has issued 25 reports of information, personnel, and physical security, covering subjects such as classification management, special access contracts, faster processing of personnel security clearances, and polygraph use and training. He has been a member of NCMS since 1979 and was on the Board of Directors for 7 years, serving as Treasurer, Vice-President and President.

MICHAEL BROWN

Mr. Michael 'Mike' Brown is the head of the Information Security Policy Division of the Office of the Chief of Naval Operations Information and Personnel Security Policy Division. He is responsible for all Navy security policies dealing with industrial security, physical security of classified material, classification guidance, security markings, protection of classified information during preparation, reproduction, storage, transmission and destruction; security review of information proposed for public release by Navy personnel and Navy contractors, security requirements for provision of classified material to Congress, protection of NATO classified information, assessments of damage resulting from compromises of classified information and the policies for control of unclassified critical technology, and unclassified controller nuclear information.

Mr. Brown served as an intelligence specialist in the Air Force Security Service; following his discharge from the Air Force he worked for the Center for Naval Analyses for thirteen years as a security and classification management specialist. From there he joined the Office of Naval Intelligence as a security review specialist and subsequently became program manager for promulgation of Navy classification guides. When Navy security programs oversight was transferred to the CNO Special Assistant for Security and Investigative Matters following the Walker espionage case, he was assigned in his present position since 1987. Mr. Brown represents the Navy on the Defense Information Security Committee, the Information Security Committee of the Advisory Group/ Security Countermeasures and is the Navy liaison to the Information Security Oversight Office.

KENT S. CRAWFORD

Degree/Field: Ph.D. Management and Organizational Behavior, University of California, Irvine.

Functional Research Area: Continuing Evaluation and Defense Industrial Security Program.

Dr. Crawford has worked at PERSEREC since November 1987. He has over 16 years of experience in conducting and supervising applied research in the DoD. He has authored numerous technical publications, journal articles, and conference papers on industrial and organizational psychology, productivity improvement, and personnel security. He is a member of the Academy of Management and received the 1985 Professional Publications Award at the Navy Personnel Research and Development Center.

JOHN F. DONNELLY

John F. Donnelly is the Director, Defense Investigative Service. Mr. Donnelly is a native of Glenolden, Pennsylvania. He is a graduate of St. Joseph's College, Philadelphia, where he received a Bachelor of Science Degree.

Mr. Donnelly served with the Naval Investigative Service from 1951 to 1981. His 30 year career with the Naval Investigative Service culminated when he transferred to the Office of the Deputy Under Secretary of Defense for Policy in September 1981, where he managed the Department of Defense investigative, security and counterintelligence programs. Mr. Donnelly was appointed Director, Defense Investigative Service on August 4, 1988. In 1985, President Reagan awarded Mr. Donnelly the rank of Meritorious Executive.

Mr. Donnelly is married to the former Therese Scott of Collingsdale, Pennsylvania. They have five children.

ARTHUR E. FAJANS

Arthur E. Fajans became the Director, Security Plans and Programs in the Office of the Secretary of Defense on January 1, 1989. He has almost twenty years continuous experience at the operational and policy levels in all the security disciplines, with emphasis on information security, industrial security and international security.

While Acting Director, Information Security, in the Department of Defense in 1982-83, Mr. Fajans served as Chairman of the National Disclosure Policy Committee and the U.S. Representative to the NATO Security Committee. In more recent years, Mr. Fajans completed the Foreign Service Institute's Executive Seminar on National and International Affairs at the Department of State, participated as the DoD international security representative on the U.S. delegation that negotiated international agreements on Cooperative Research in the Strategic Defense Initiative with the United Kingdom, the Federal Republic of Germany, Italy, Israel, and Japan, as well as negotiations leading to implementation of Patent Secrecy and the Scientific and Technical Agreements with the Government of Japan.

Prior to joining the staff of the Deputy Under Security of Defense for Policy, Mr. Fajans served in the Office of the Assistant Secretary of Defense for Public Affairs as the DoD Freedom of Information Staff Specialist. Mr. Fajans also has been employed by the Navy Department and the Defense Intelligence Agency as an intelligence analyst.

MARTIN FERGUSON

Mr. Ferguson is the Security Manager at the U.S. Naval Research Laboratory in Washington. He is responsible for all phases of security at this important DoD research facility and its 14 field sites located in 5 states. His security responsibilities include information, industrial, personnel, physical, operations, ADP, security force, fire protection, health physics and occupational safety, SAP, SSO, technology export, and security eduction, and he is the Deputy Inspector General. He has held his present position for 10 years. He has over 25 years in government and industrial security. He holds a Bachelor's Degree in Business Management, has done related graduate level work, and has been a member of NCMS for 8 years.

STEVEN GARFINKEL

Steven Garfinkel is the Director, Information Security Oversight Office. He was born on June 18, 1945 in Washington, D.C., and attended the public schools of that city. He currently resides in Silver Spring, Maryland with his wife Tillie, and their children Kenneth and Laura.

Mr. Garfinkel attended both George Washington University and its Law School as a Trustee Scholar. He received his J.D. (with Honors) in 1970, three years after receiving his B.A. (with Distinction, PBK).

Mr. Garfinkel has served as Director of the Information Security Oversight Office since May 1980. In this position, his is responsible to the President for the administration of the Government-wide information security (security classification) system. He previously served almost ten years in the Office of the General Counsel of the General Services Administration, in which his positions included Chief Counsel for the National Archives and Records Service, Chief Counsel for Information and Privacy, and Chief Counsel for Civil Rights.

Mr. Garfinkel is a member of the District of Columbia Bar. He has received a number of awards during his Federal service, including eleven different citations from

Presidents Reagan, Carter and Ford. These include the Presidential Rank Award Meritorious Federal Executive. He has also received commendations from the National Security Council, the Department of Defense, the Department of Justice, the Office of Personnel Management, GSA, and several non-government professional and service organizations.

ERNEST HAAG

Ernest Haag is a researcher and manager of western operations for Human Resources Research Organization International, Inc. (HII) based in Monterey, California. His special interests are in personnel security issues, particularly in the area of security awareness, continuing assessment and management systems. He is also a management and organization development consultant. Mr. Haag served as a Naval Aviator (Anti-Submarine Warfare) for thirty years, holding various command billets and helping develop and deliver competency based leadership and management training for senior Navy officers. He holds a BS from the University of Southern California.

JOHN R. HANCOCK

John R. Hancock, of System Planning Corporation (SPC), is currently engaged as Project Manager and Physical Security Coordinator with the Department of State Embassy Task Group in Arlington, Virginia. Other assignments for SPC have been as Special Advisor to the Strategic Defense Initiative organization and industrial security consultant on various tasks. He has over twenty-three years of security experience as former Chief of the Program Management Division, Defense Investigative Service; former faculty m ember at the Defense Security Institute. He has a BA degree from North Central College and has done graduate work at George Washington University. An ASIS member since 1968, Mr. Hancock has served as Vice Chairman of the Architect/Engineer Subcommittee under the Standing Committee on Physical Security. In addition, he has served his Fredericksburg/Quantico Chapter in many capacities.

CHERYL S. HESS

Cheryl S. Hess is currently a Senior Security Specialist with the U.S. Department of State, Bureau of Diplomatic Security, Industrial Security Division. She joined the Department in 1987 and has worked exclusively on developing the Department's world-wide industrial security program with particular emphasis on the Department's use of contractors in its overseas construction program. Included in her duties are overall policy development and implementation as well as managing the contractor personnel security clearance program. This position requires close liaison with the Defense Investigative Service to coordinate user agency requirements, other federal agency coordination as well as close coordinations with other Diplomatic Security functions.

A graduate of the University of Central Florida with a B.A. in Criminal Justice, Ms. Hess spent five years at NASA's Kennedy Space Center as a Security Specialist before relocating to Washington, D.C. where she spent two years as a Security Supervisor in private industry working DoD programs prior to joining the State Department. She is a member and past office of the Washington, D.C. Chapter, NCMS and a former Chairperson of the Florida Peninsula Chapter, NCMS.

PAUL R. LAPLANTE

Paul R. Laplante was appointed Chief of the Policy Branch, Office of Classification and Technology Policy, Defense Programs, U.S. Department of Energy (DOE), in December 1987. In this capacity, Mr. Laplante is responsible for cross-cutting policy, guidance and procedural issues concerning the DOE classification program. This program includes National Security Information under DOE's cognizance and Restricted Data and Formerly Restricted Data classified under the Atomic Energy Act. In addition, Mr. Laplante is responsible for similar matters concerning various kinds of unclassified but sensitive information, such as Unclassified Controlled Nuclear Information (UNCI) and Official Use Only Information. He is also responsible for the development of detailed technical guidance for the UNCI program. Prior to accepting his current position, Mr. Laplante served in a variety of staff positions in this and other offices with Defense Programs which involved long range policy and planning as well as classification and control matters.

From 1978 to 1980, Mr. Laplante served as the Deputy Chief of the Information Security and Classification Management Branch at the Defense Nuclear Agency. While there, he was also involved in the classification of information protected under both Executive order and the Atomic Energy Act. Mr. Laplante conducted the classification education program for the agency

and the technical education program for the classification staff.

Prior to this, Mr. Laplante worked as a civilian for a year for Naval Intelligence and was assigned while on active duty in the U.S. Army to the Electronics Command Laboratory, Fort Monmouth, New Jersey for four years. His technical specialties included non-volatile memory devices and fiber optics communications systems.

Mr. Laplante has a B.S. degree in physics from Worcester Polytechnic Institute and a M.S. in physics from Case Institute of Technology.

M. J. LEVIN

Mike Levin joined the Army Security Agency in 1947 (after service in WWII as an Artillery Officer with the 7th Armored Division in the European campaign) and has continuous service with the Armed Forces Security Agency (which was the immediate predecessor of NSA) and then with the National Security Agency itself since its beginning.

He has served as a professional in NSA's special field of intelligence for 43 years. Early on, he took time out from his normal duties to do a little teaching for the Agency. He taught one of the first formal classes in Radio Traffic Analysis and also taught the first Agency sponsored class in Intelligence Report Writing. He was chief of several key operational areas at headquarters and overseas. In 1975 he moved to the Director's Staff. For seven years he was Chief of Information Security and in 1983 became Chief of Information Policy. Information Policy encompasses Information Security, Public Affairs and Freedom of Information/Privacy Act functions. He now serves as Special Assistant to the Director of Policy and is also Senior NSA Classification Officer.

Mike has been actively involved in the struggle against Unauthorized Disclosures for many years. In 1985 and 1986 he was chairman of the DCI Security Committee Unauthorized Disclosure Investigations Subcommittee and under the current DCI Unauthorized Disclosure Committee he chaired the Working Group which developed a new draft National Security Directive which is now under review at the National Security Council.

Mike is a native Nebraskan and is a graduate of the University of Vermont.

JAMES R. LINNEN

Colonel James R. Linnen has served as the Director of Counterintelligence and Security Countermeasures, Office of the Deputy Chief of Staff for Intelligence, Headquarters, Department of the Army since August 1987. Immediately prior to that assignment, Colonel Linnen served for four years in Germany, first as Commander of the 103d MI Battalion, 3d Infantry Division, then as Chief of the DIA Liaison Office in Bonn.

Colonel Linnen's military career has included a variety of assignments in the intelligence field, including faculty positions at the Army Intelligence School, Fort Holabird, Maryland. He served in Vietnam as Recce Team Chief, Tac Air Control Center, U.S. Military Assistance Command, Vietnam and later as the S-3, 1st Military Intelligence Battalion (Air Recon Support). From August 1979 until July 1982, he was OPSEC Division Chief and Commander, Security Support Battalion (Prov), 902d Military Intelligence Group, Fort Meade, Maryland. From July 1982 to June 1983, he was Operations Officer, U.S. Army Central Security Clearance Facility.

Colonel Linnen graduated from St. Norbert College with B.A. degree, and received a M.L.A. degree from John Hopkins University. His professional education has included the F.B.I. National Academy, the U.S. Army Command and General Staff College, and the Army War College.

Colonel Linnen is a native of Waupun, Wisconsin. He and his wife, Gaby, have two children, Patrick and Katherine.

OLES LOMACKY

Since 1976, Mr. Lomacky has been associated with the Office of the Secretary of Defense, most recently as Special Assistant for MCTL and Long-Range Planning in the Office of the Under Secretary for Research/Engineer Research and Advanced Technology. Within the Department of Defense he has held positions as Acting Assistant Deputy Under Secretary for International Technology and Trade; Director, Technology Trade; Assistant Director, Technological Commitments and Trade; and as a Staff Specialist for Technology Transfer. Prior to this, between 1963 and 1976, he was a Senior Research Scientist in the Structures Department of the David W. Taylor Naval Ship R&D Center.

Mr. Lomacky has a Ph.D. in Engineering, Applied Mechanics and Mathematics, Washington University, 1969; M.S. in Engineering, City College of New York, 1956. He is a graduate of the Federal Executive Institute, and a Registered Professional Engineer in New York and the District of Columbia.

KENNETH E. LOPEZ

Kenneth E. Lopez is the Director, Office of Procedural Security, Bureau of Diplomatic Security, U.S. Department of State. In this position, he manages the Department's Information Security, Industrial Security, and Domestic Physical Security Programs. He is responsible for policy development and oversight of implementation of Information and Industrial Security Programs affecting all domestic State Department activities, 256 U.S. overseas Embassies and Missions, and over 500 classified contracts. The Domestic Physical Security Program encompasses 100 separate Department facilities nation-wide.

Mr. Lopez received a B.A. degree from the University of California, Los Angeles in 1966, then served from 1966 until 1971 as an Armored Cavalry platoon leader and Military Intelligence officer in the U.S. Army. From June 1973 to September 1978, he was a Supervisory Security Program Manager in the Office of Investigations and Security, Federal Aviation Administration, responsible for the protection of National Air Space System and Air Traffic Control facilities.

From September 1978 to Septembe 1981, Mr. Lopez was Director, Division of Security and Protection, Office of the Secretary, U.S. Department of Health and Human Services. He managed a multi-faceted security program for the Federal Government's largest civilian agency, consisting of over 140,000 employees and 3,500 facilities nation-wide. From September 1981 until March 1986, he was Chief of the Security Office, John F. Kennedy Space Center, National Aeronautics and Space Administration, and managed security, intelligence and law enforcement activities at the Space Center.

Mr. Lopez resides in Alexandria, Virginia, with his wife, Patricia and three children, August Zachard and Mariana.

JOHN MARTIN

John Martin has been a national correspondent with ABC News since 1983. He reports for ABC's "World News Tonight with Peter Jennings." During the past year, Mr. Martin covered the nomination of John Tower to be Secretary of Defense, the federal pay raise defeat and the Pentagon bribery scandal. he reported on the rise of drug-related murders in Washington, D.C., and the career of Wall Street trader Michael Milken for ABC News "Nightline". During the 1988 election campaign, he compiled a profile of vice presidential nominee Dan Quayle.

In recent years, Mr. Martin reported on the Iran-Contra scandal, starting with the trial in Nicaragua of former CIA employee Eugene Hasenfus. He also covered ethical questions involving former White House aides Michael Deaver, Lyn Nofziger and Edwin Meese III. From 1983 to 1985, Mr. Martin served as the principal correspondent for "This Week With David Brinkley." Traveling to the Middle East, Central America and China for the Sunday interview program. In 1985, he was nominated for an Emmy Award for 18 reports on the search for Nazi fugitive Joseph Mengele. mr. Martin obtained exclosive interviews with Dieter Mengele, t he figuitive's nephew, and with then-President Alfredo Stroessner of Paraguay. In 1983, Mr. Martin reported evidence of visits to the United States by another Nazi fugitive, Klaus Barbie.

Mr. Martin has compiled a series of reports on the deaths of major world figures: William Casey, Leonid Brezhnev, Anwar Sadat, Henry Fonda, Grace Kelly and Tennessee Williams. The Brezhnev obituary was nomiated for an Emmy in 1982. His reports on suspected war crimes by Kurt Waldheim were nominated for an Emmy in 1987.

Listed by "Who's Who in America," Mr. Martin won the 1988 Excellence in Journalism Award from the National Association for Home Care for his report, "Orphans of Technology," which dealt with children saved at birth but impoverished by high-technology medicine. In 1987, Mr. Martin received the San Diego State Univeristy Distinguished Alumnus Award from the College of Professional Studies and Fine Arts. In 1983, TV GUide named him one of the top five investigative reporters on network evening news broadcasts. In 1982, he won the National Society of Professional Engineers Award for reporting on lasers, and in 1980, he wonthe National Headliner Award for a report on microsurgery. Mr. Martin has reported for the ABC News programs, "20/20" and "Nightline." He

was nominated for a Sigma Delta Chi Award in 1978 as correspondent for the ABC News "Closeup" documentary, "Politics of Torture."

Mr. Martin joined ABC News in 1975, in New York. He began his career in journalism as a copy editor and reporter at The San Diego Union, The Augusta Chronicle (Georgia), and The New York times international edition (Paris). He was a reporter, producer, and anchor at KCRA-TV News in Sacramento for nine years.

Mr. Martin lives in Washington, D.C. with his wife, Katherine Fitzhugh. He has two daughters, Sophie and Claire, by a previous marriage.

THOMAS P. MAURIELLO

Mr. Mauriello is a former Security Awareness Educator for the National Security Agency, Office of Security. During his tenure, he briefed over 12,000 peple while presenting security briefings ranging from Security Indoctrinations to TDY briefings. Prior to this, he was employed as a Police Officer for the State of Maryland where he developed the Department's first Police Community relations program, personally conducting hundreds of speaking presentations on crime prevention and personnel security.

He is a lecturer at the University of Maryland's Institute of Criminal Justice and Criminology where he has been teaching for the past 12 years, and he is presently the Chief of the National Security Agency's Security Operations Center. Mr. Mauriello has most recently written a book entitled: "Police Investigations Handbook," published in June 1990 by Matthew Bender Publishing Company.

STANLEY SIENKIEWICZ

Mr. Sienkiewicz is the Associate Deputy Under Secretary of Commerce for Export Administration, and holds the commerce Department Faculty Chair at the Industrial College of the Armed Forces. He served as the Special Assistant to the Under Secretary of State for Security Assistance, Science and Technology from 1981 to 1989. In that capacity, he served as the principal oversight official for U.S. army transfers and security assistance programs.

Prior to joining the State Department, Mr. Sienkiewicz served as the Senior Professional Staff Member responsible for National Security Affairs and legislation for the Republican staff of the Senate Committee on Foreign Relations. Earlier in his career, he served as the Armed Services Committee staff member for Senator Richard S. Schweiker of Pennsylvania. In the late 1960's, he also worked in various capacities for several other members of Congress.

During the 1970's, Mr. Sienkiewicz served as an operations-research analyst in the Office of Secretary of Defense. In that position, he worked on interagency studies of U.S. nuclear forces, U.S. arms control policy and negotiations as well as the annual defense program review and preparation of the Defense Posture Statement. Earlier in his career, he worked as an analyst and writer at Radio Liberty in Munich and in the New Jersey State Department of Higher Education. He speaks russian and german.

His education includes attendance at the U.S. Military Academy at West Point, a Bachelor's Degree from Princeton University and Masters Degrees and a Soviet Studies Certificate from the John Hopkins School of Advanced International Studies and the University of Pittsburgh. He has also done graduate work at the Massachusetts Institute of Technology and has been a Research and Teaching Fellow at Harvard University's Program for Science and International Affairs. He has taught courses in arms control and national security at several universities since 1976, and published numerous articles on national security issues over the past two decades.

Mr. Sienkiewicz was born in Germany in 1945. He is a naturalized U.S. citizen, has held a Top Secret security clearance since 1972. He is married and the father of three children.

L. BRITT SNIDER

Mr. Snider has served as the General Counsel, Senate Select Committee on Intelligence since February 1989. He serves as principal legal advisor to the Committee, drafting legal opinions and providing legal advice to the Chairman on a variety of issues. He drafts legislation and Committee reports, prepares material for hearings and floor proceedings, coordinates Committee participation in legislative efforts of other Committees, and prepares statements and other materials for the Chairman and Vice Chairman of the Committee. From January 1987 to February 1989, he was the Committee's Minority Counsel. Also, in 1987, he served as staff liaison for Senator William S.

Cohen to the Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition (the Iran-Contra Committee).

Mr. Snider served as an officer in the U.S. Army Signal Corps from November 1969 to October 1971. From January 1972 to February 1975, he was Counsel, Senate Judiciary Subcommittee on Constitutional Rights, then served as Counsel, Senate Intelligence Committee until May 1976. From May 1976 to June 1977, Mr. Snider engaged in general civil practice as a partner in the legal firm of Ketner & Snider. Then from June through October 1977, he was Chief Counsel, House Government Operations Subcommittee on Government Information. He directed staff activities in areas including the Freedom of Information Act, Privacy Act, and security classification.

From October 1977 to January 1987, Mr. Snider was a member of the Office of the Deputy Under Secretary of Defense (Policy), including service as the Assistant Deputy Under Secretary of Defense (Counterintelligence and Security). His responsibilities included counterintelligence, security classification, personnel security, industrial security, physical security, operations security, international arrangement of the disclosure of classified information, technology transfer, and other Department policy in these areas and monitored implementation on behalf of the Secretary of Defense. In 1985, he also served as Staff Director of the DoD Commission to Review Security Practices and Procedures (the Stilwell Commission).

Mr. Snider holds a B.A. degree in Political Science from Davidson College, North Carolina, and a J.D. degree from the University of Virginia School of Law. He attended Harvard University Executive Program in National and International Security in 1980. He is a member of the Virginia State Bar and the District of Columbia Bar Association.

DEBORAH V. TAYLOR

Ms. Taylor has been an Information Security Specialist with the Department of Commerce for over four years. Debi's primary duties involved information security classification management, industrial security and security education and awareness. She is presently detailed to the National Oceanic and Atmospheric Administration (NOAA) where she has been assigned the responsibility of developing a comprehensive directive for the implementation and administration of a NOAA-wide security program. Debi is an active member of the Security Awareness and Education Subcommittee and chairs the "Security Briefings Course" Working Group. She has coordinated and participated in the presentation of three "Security Briefing Courses" hosted at the Department of Commerce.

Before coming to the Department of Commerce, Debi was an officer in the U.S. Army Military Police Corps serving as a MP platoon leader at Fort Ord, California; Special Weapons Site Security Officer and Brigade Physical Security Officer at Miesau and Pirmasens, West Germany; and Brigade Assistant S-4 (Logistics) and Brigade S-1 (Adjutant) at Fort Dix, New Jersey. Her awards include the Army Commendation Medal (1 OLC) and the Meritorious Service Medal.

Debi is a native of Philadelphia, Pennsylvania and has a B.A. in Criminal Justice and Sociology from LaSalle University, Philadelphia and has taken graduate courses in security management and administration at George Washington University. She has been a member of NCMS since 1986 and is a former Washington, D.C. Chapter Treasurer, 1988-1990. She was the Publicity Chair for the Chapter's 1988 mini-seminar and is the Publicity and Printing Chair for the 1990 Seminar here in Washington.

Debi is married to Captain David Taylor, USAF and has a daughter, Johanne and twin sons, Jason and Jarrod. Debi and her family will join David this September at Midenhall RAF, United Kingdom where she will begin working as a consultant developing security education presentations and materials. Debi looks forward to becoming a member of the NCMS European Chapter and participating in its activities.

WARREN M. VOLLERT

Mr. Vollert, since 1984, has been the FSO and Director of Security for E-Systems, Inc., Melpar Division located in Falls Church, Virginia. Warren is a former Air Force officer who spent 20 plus years assigned as a special agent with Air Force Office of Special Investigations (AFOSI). His involvement in the industrial security arena began in 1981 when he was assigned to the Air Force Research and Development, Special Projects Office. His responsibilities included the oversight of industrial security programs of defense contractors involved in the development and manufacture of the B-2 Stealth Bomber and the F117 Stealth Fighter.

Warren is also the Vice President of VOS Associates, Inc., a computer software firm specializing in security management systems for U.S. defense contractors.

SANDRA (SANDY) J. WALLER

Sandy began her government service in 1958 as a fingerprint technician with the FBI. She spent 15 years with the Naval Air Systems Command and was a Contracting Officer for Security Matters for 10 years. She served for 5 years as a Staff Specialist for Information Security in the Office of the Secretary in the Department of Transportation. She moved from Transportation to the Defense Investigative Service as an Industrial Security Specialist and served for 5 years as the principle staff officer for classification management. Sandy joined the staff of the Office of the Deputy Under Secretary of Defense for Policy in April 1986 where she is currently an Industrial Security Specialist in the Industrial Security Directorate.

Sandy has served in many positions in NCMS since she joined in 1971. She was Secretary of the Washington Chapter in 1977-78; Vice Chairman in 1978-79; and Treasurer in 1979-80. She was also on the National Board of Directors for 4 years where she served as Secretary for 2 years and as Chairman of the Publications Review Committee and the Government Awareness Committee. She was on the National Seminar Committee for the seminar held in Richmond in 1980, on the committee for the mini-seminars held by the Washington Chapter in 1981 and 1988, and participated in the Inspection Skit with other "NCMS Players" at the mini-seminars held in White Oak, Maryland and Huntsville, Alabama in 1981. She has been a speaker and panelist at many NCMS and ASIS seminars and at the Defense Security Institute in Richmond, Virginia.

She is a native Virginian and currently lives in Springfield, Virginia.

ANDREA G. WRAALSTAD

Ms. Wraalstad is currently the Chief of the Industrial Security Division, Bureau of Diplomatic Security, Department of State, where she is responsible for the development and implementation of policies and procedures for the Department's worldwide industrial security program. Prior to joining the Department of State, she was the Classification Management Specialist at both the Capital Region and Headquarters, Defense Investigative Service, and has been employed by the U.S. Navy in several security positions. She attends college part-time and is pursuing a degree in Business Administration. She has been a member of NCMS since 1975, an active participant in several national seminars, and is part Chairman of the Washington, D.C. Chapter, where she was responsible for two very successful Chapter seminars.

PART II
NCMS
VIEWPOINTS

NOTICE

We wish to thank those authors who have contributed to this new portion of the Classification Management Journal - NCMS VIEWPOINTS. We encourage additional authors to submit articles. We plan to issue NCMS VIEWPOINTS as a second Journal if there is sufficient interest and contributions.

PROPOSALS FOR IMPROVING SYSTEMATIC DECLASSIFICATION REVIEW

Albert L. Thomas
Kirtland A.F.B.

The U.S. Government ought to address several critical problems with the systematic declassification review program. I will begin with some background information on these problems based upon a review of Executive Order (EO) 12356 ("Background of EO 12356," Information Security Oversight Office Annual Report to the President, ,FY 1982, p.17). Then I will discuss some problems with the current program, and offer several ways to solve them.

The Systematic Declassification Review Program

In 1972, President Richard Nixon signed EO 11652 which introduced for the first time a program to review retired record files systematically for declassification. The order provided that the Archivist of the United States would conduct a systematic review of classified holdings in the National Archives when those records became 30 years old. The new requirements came about as a result of public pressure generated by political events in the late 1960s and early 1970s, and growing Congressional awareness that classified records were increasing dramatically.

In 1978, President Jimmy Carter issued EO 12065 which directed all Federal agencies to conduct systematic review programs, and shortened the term from 30 to 20 years. This order vastly expanded the workload by millions of cubic feet of records, and required that more resources be dedicated to the task.

The current systematic review program dictated by EO 12356 signed by President Ronald Reagan on 2 April 1982 more closely resembles the initial effort envisioned in EO 11652. That is, it requires only the Archivist of the United States to conduct a systematic review program for the declassification of records accessioned into the National Archives, and of Presidential papers or records under the Archivist's control. As implemented by the Information Security Oversight Office, the current directive schedules systematic review at the 30-year mark, except that it delays the review of sensitive intelligence and cryptologic files until they reach 50 years of age.

While the EO does not require other agencies to conduct systematic review for declassification of records in their custody, it encourages them to do so if resources are available. Potentially, EO 12356 could worsen a problem that existed in 1972 and was solved in part by EO 11652, but has come back again in recent years: the buildup of permanently classified records stored in records centers, agency holding facilities, and the National Archives.

Executive Orders 10501 (signed by President John Kennedy in 1961), 11652, and 12065 all included some provision for the automatic declassification of national security information based solely on a fixed age. EO 12065 carried the concept of automatic declassification the farthest:

"At the time of the original classification, each classification authority shall set a date or event for automatic declassification no more than six years later. Only officials with Top Secret Classification authority and agency heads . . . could classify information for more than six years from the date of original classification." (ibid., p.23)

In theory, original classification authorities (OCAs) had two alternatives:

First, they could disregard any concern about the duration of the information's sensitivity, and mark documents for automatic declassification in six years or less.

Second, they could bring the information before the head of the agency or a Top Secret OCA, and seek to have that official classify it for a period of time not to exceed twenty years.

Foreign government information could be protected for terms not to exceed thirty years. In practice, many OCAs chose the first alternative less than ten percent of the time. They selected the second alternative, requiring special procedures, that were mandated for sparing use, approximately 65 percent of the time.

To handle the remaining 25-30 percent of original classification decisions, some classifiers relied upon a technique that was not even contemplated in EO 12065:

"Review in six years"

EO 12356 established the principle that information be classified for "as long as required by national security considerations" (or OADR for "Originating Agency's Determination Required"). When

able to do so, OCAs are asked to establish specific dates or events for declassification at the time it is first determined to be classified. Otherwise, declassification requires agency review, a process which may be initiated at any time by officials inside the agency, or requested by persons outside of it.

Problems with the Systematic Review Program

The present systematic declassification review program is not working very well. First and foremost, there is no automatic declassification or downgrading process (EO 12356 provides for declassification of information without review after 30 years (50 years for intelligence and cryptology files), except where an original classification authority issues instructions and guidance that it must remain classified beyond that period). The original classification authority (sometimes incorrectly called the originating agency) must determine up front how long the information should be classified. Most of us acknowledge that it is difficult, if not impossible, to determine how long the information will remain sensitive when initially classified. Rapid advances in technology and lack of access to an appropriate data base make it difficult to keep up with all information and data that are currently sensitive to our national security. Because it is difficult to determine declassification dates early in the acquisition process, much information receives an indefinite (OADR) declassification marking. This results in overuse of OADR for the "Declassify on" date, which causes the accumulation of files that are seldom reviewed later for declassification.

In addition, there is no systematic means to downgrade information on a schedule with the passage of time, especially Top Secret information. This results in even greater unnecessary costs for storage containers and requisite accountability and control measures.

Federal agencies generally place no emphasis on, and give no urgency to, the declassification of information. While the intent of systematic review is to declassify information for research purposes, only a small amount of the declassified information is released to the public. Merely encouraging agencies to review their records when resources and time permit does not give them much of an incentive.

The EO requires that only permanently valuable records be systematically reviewed. Therefore, classified records that are not considered permanently valuable are not intended to be reviewed for declassification. They probably will never be reviewed because they should be destroyed when no longer needed. Examples include classified information originated by U.S. Government agencies for use in daily operations. Some of these nonpermanent records are maintained in storage for many years, however, which requires secure storage and other safeguarding measures. Significantly, they are not intended to be made available to the public, and could be downgraded or declassified and placed in less expensive storage areas without danger of compromise or unauthorized release.

Agencies may try to avoid responsibility, especially for old information they did not create. If it is sensitive, it may be career-threatening. We often cannot easily identify the responsible office or agency, so the buck gets passed to some other custodian who does not have the expertise to review it. Many documents require multiple agency review, but none of the agencies wants to go first. Those OCAs outside the requesting agency lack a sense of urgency, do not want to be bothered, and often need constant prodding to complete action.

When asked to declassify information, officials may face a task that is both new to them and largely unrelated to their previous experience. Corporate memory disappears with time and organizations are deactivated or realigned, thus forcing some official who has only current functional responsibility to make the declassification decision. Reasons for the initial classification may not be understood clearly, or at all.

Officials may be too busy to conduct intensive, time-consuming reviews. Declassification reviews receive low or no priority, and often are treated as an additional duty. Reviews are inefficient and costly, since they require line-by-line, page-by-page reading. Many offices lack the staff or funds to conduct an efficient program, and there is no data base to help the reviewer.

Generally, records cannot be declassified in bulk without page-by-page review. Bulk declassification was adequate for World War II records, and for some records related to the Vietnam Conflict. Multiple layers of review are now necessary because records custodians do not possess the experience, background, or knowledge needed to make declassification decisions relative to intelligence, national defense, and foreign relations.

Considerations to Improve the Program

The classification system should mandate a specified maximum period of time for protection of most categories of information, even though this exposes some of it to premature disclosure. At the time of the original classification decision, the OCA should establish a specific date or event for declassification. If the continuing national security sensitivity of the information cannot be related to lead time or system lifetime, the information should be classified no longer than 20 years from its date of origin. Military operations, weapons system advances, and emergency planning keyed to a lead-time phenomenon lose sensitivity and importance in relation to our national security with the passage of time. Intelligence, cryptologic information, and foreign relations information would be protected by exception to the 20-year rule.

Information marked for automatic declassification in 20 years should not remain classified under any circumstances without a personal determination that continued classification is necessary made by the originating agency head, deputy agency head, or the designated senior agency official.

In addition, the declassification review process should be prioritized to accommodate public demand for the information. First, decide if you need to keep the information. If you do, then review it for declassification.

Include information not considered permanently valuable in the systematic review process. This involves information originated essentially in daily operations. While the question of its retention should be the focus of attention as well, it should be systematically reviewed for declassification to avoid the high costs of unnecessary, long-term secure storage.

Where possible, records should be reviewed before they are forwarded for accessioning into the National Archives. This will allow the Archivist of the United States to accomplish follow-on review easier and faster. Further, agencies must provide the Archivist with declassification guidance and decisions on specific questions to facilitate reviews.

There needs to be more focus on declassification and downgrading during inspections, program reviews, and oversight visits. When inspectors sample documents, they should look for indicators that the program is working. They must be inquisitive. Could declassification have been keyed to a date or event? Challenge the use OADR for original decisions if there is a reason to disagree with its use. Are documents destroyed when no longer needed, or is their retention beyond five years approved by regulation? If a declassification date or event has been changed to OADR, were all known holders notified? Does the file copy of the document list all sources for derivative classification when multiple sources designation is used on the "Classified by" line? When documents are declassified, are they removed from classified storage containers?

Bulk declassification should be used when subject matter permits. Not all documents require item-by-item review. Focus on key issues and what is sensitive in the document; from that, ask the pertinent questions.

Agencies should be required, directed from the top down, to conduct systematic reviews for declassification of records in their custody. Something stronger than encouraging review when resources are available is needed. Each agency would have the latitude to declassify information for which it exercises exclusive OCA.

Another consideration is the application of automated data systems to aid in systematic declassification. We must develop a program similar to a spell-checker or an on-line dictionary containing classified words and phrases, as well as all known rules governing classification. This effort is suitable for applying optical character reader technology to allow the input of printed documents for automated processing. Information on intelligence sources and methods requiring more thorough review and coordination would be maintained separately.

Artificial intelligence (AI) techniques also offer many possibilities. A fast look-up capability allows association of one sentence, word, or phrase with any other sentence, word, or phrase within the document to determine classification by association. AI techniques could include the ability to tag each portion determined to be classified or declassified with the rule(s) that make it classified or unclassified. Computers can also be used to make immediate changes to document classifications as classified portions are regraded or removed.

Conclusion

This paper has provided a brief history of executive orders as they pertain to the systematic declassification review process, a discussion of problems with the current process, and several suggestions for ways to improve the process. Those of us involved with classification go to great lengths to ensure that information vital to the national security is adequately protected. We are obliged to exert a comparable amount of energy to ensure that information is declassified at appropriate times.

FORCING SPIES TO LEAVE MESSAGES

Wes Lemmon
Kirtland A.F.B.

The Challenge

Most of us use those little adhesive-backed notes fairly extensively for leaving brief messages. Within the Air Force, they seem to be everywhere, even in work centers where classified material is routinely handled. People leave messages for each other, for their supervisors, and for their subordinates. But spies seldom leave messages in any form. We cannot find out about their intentions or their actions. Not even from sticky-back notes. But those notes can help a spy.

The absence of telltale espionage indicators or messages poses one of our greatest challenges in safeguarding classified material. This is why safeguarding classified information is often more difficult than safeguarding physical property. If someone steals your truck, you immediately have firm evidence of your loss. But spies can steal huge amounts of information over a period of years, and those of us responsible for the information may never get a message that anything is missing.

Special Case of the Insider

Consider the Walker ring and the Cooke and Boyce espionage cases. All participants were insiders who were authorized access to the information. They became effective espionage agents, but seldom did any of them leave messages about their activities for supervisors or coworkers. The absence of such messages is the key to success of an insider espionage agent.

Detecting Espionage

To prevent espionage, we need to use every means available to detect that something is wrong. Having spies leave those little sticky-back notes would be perfect, but getting spies to cooperate is obviously out of the question. So let us consider some realistic ways to force the executors of espionage to leave us messages about their activities.

Copy Machines

We must ask more hard questions before allowing classified material to be reproduced. What documents are they, and what is their classification level? Why must they be copied? Who authorized the copies to be made? We may need to impose stricter requirements before allowing reproduction, such as demanding written authorizations, logs, and similar controls. After all, there is ample evidence that espionage agents use copiers to steal classified information.

Multiple Copies

The insider knows to look for multiple copies of the same document. A spy often can steal one of the multiple copies without raising suspicion, and the information is still available for those who need it. Such actions leave no message that something is wrong. Therefore, we need to eliminate the extra copies of classified documents in our storage containers. When the only copy of a classified document in storage is discovered to be missing, we get a strong message that information may have been compromised. Let us encourage frequent clean-out days and the prompt destruction of unneeded copies of classified material.

Destruction

When we decide to destroy classified documents, no one expects them to be used or seen again in the work center. The insider knows this, and may be able to remove selected documents without leaving a message that they are missing. We must ensure that two people become involved in verifying destruction.

Top Secret Documents Outside Accountability Controls

The insider also knows which documents are accounted for properly and which are not. Given the choice of which to steal, the insider spy will take those

not properly controlled. It is likely that the responsible custodian will be too embarrassed to report it missing, and would report it only reluctantly. Our commands should provide for full and continuous accountability for all such documents that require additional controls.

Conclusion

These are a few of the ways to ensure that someone stealing classified information leaves you a message. Security officials will understand my message: Simply look for ways to receive those telltale indicators that classified material is not being properly handled.

A Final Thought

By the way, I recommend that you not attach sticky-back notes directly to classified documents. The classified information may be transferred to the adhesive and wind up in unclassified waste containers.

SECURITY AWARENESS AND EDUCATION:

A Diversified Approach

Diane Thomas & James L. Watson
AT&T Bell Laboratories

We are now witness to an era of unprecedented change. Numerous events are occurring worldwide that just five years age were probably unthinkable, even to the most brand-thinking american. Consider, for instance, recent apparent changes in USSR policy addressing recognition of the practice of religion, the admission of war crimes and unjustified aggression, the granting of independence to Soviet republics, and the reduction of arms. Consider the large share of the american automobile market that foreign companies now enjoy. Or, consider the demise of the Berlin Wall and the security implications arising from that situation. These unthinkable changes have not altered the prime focus of the security profession, that is, the protection of assets. But they do signal the need to replace what has been, in many of our industrial security organizations, a rather one-dimensional way of focusing on and handling security concerns with a diversified approach to security awareness and education.

One aspect of the diversified approach is becoming evident in many organizations whose security awareness programs traditionally encompassed only the protection of classified information. Spurred by the unthinkable changes mentioned above, these organizations found it necessary to include the protection of proprietary information in their security programs as well.

We connect classified information with the security of the nation and proprietary information with the security of a company. But we should not overlook the fact that proprietary information, like classified information, is targeted by foreign intelligence activities. Their corporate intelligence collection is geared toward attaining a competitive edge for economic or technological reasons.("Are Your Secrets Safe?" The Lippman Report (September 15, 1989)

Some traditional security specialists argue that a diverse security awareness program minimizes the importance of classified information. On the contrary, a program that focuses on both classified and proprietary information yields double dividends. Although protection requirements for proprietary information usually vary significantly from those for classified information, the concepts involved in protecting both kinds of information are very similar. Thus, once employees develop a mind set for protecting either kind, adhering to the requirements for protecting the other kind becomes almost second nature. A security awareness program that is double-focused or diverse in scope, then, may actually reinforce the importance of protecting classified information rather than detracting from it.

A diversified approach to security awareness and education requires a change of emphasis in three key elements of program implementation. Assessment, marketing, and communication. The methods used in these elements are not new, but they involve a change in emphasis. In fact, they reflect the customer focus that now pervades industry.

Assessment

A traditional method used for training and education in security awareness programs is to bombard employees with boilerplate information, both routinely and as needed. Admittedly, this method accomplishes the objective of imparting the required information to the target audience in a timely manner. It does so, however, by way of excess-excess in employee time and company expenditures.

How can this excess be eliminated? One

way is to assess the extent to which the training provided is beneficial to or suitable for employees through a series of measurements. One such measurement is a survey given to the employees in question that simply asks for responses to questions involving their perception of the quality and value of the briefing. Another measure is a quick pre-test to establish how much knowledge they already possess, with a post-test to see how much of the course material was actually absorbed. Follow-up to the process is important. There is a benefit to questioning this same group within an established time to determine retention or usefulness of the information. The measurements can be combined to provide a snapshot that helps determine the value of the instruction or training--perceived and actual. This information can provide the necessary justification for continuing the training, modifying its content, or eliminating it. If the results indicate that the training should be eliminated, there should be no hesitation in taking this action. This is especially true if the effort does not provide a positive effect on the bottom line. Tom Goud states in his article, "ISD Technology for Everyone," that instruction must equip people to do their jobs. More instruction than that is wasteful; less can cause big problems."(Tom W. Goad, "ISD Technology for Everyone," Designing and Delivering Cost-Effective Training and Measuring the Result, (Minneapolis, MN: Lakewood Publications, 1988), p.9)

Marketing

When we think of marketing, we think of strategies and techniques associated with the buying or selling of goods. We often think of security awareness as antithetical to this concept. Marketing implies that a buyer has a choice as to whether he or she will buy what the seller has to sell, whereas security awareness is an area in which the buyer, or employee is obligated, usually by signed agreement, to buy or to abide by the security regulations of the controlling organization -- the U.S. Government or the company. However, marketing also implies that the seller is responsible for making the goods appealing to the buyer, and that is an aspect of marketing that we as security professionals would do well to master.

Early in 1989, Joseph Grau, Chief of the Information Security Division at the DoD Security Institute, in his article "Selling Security,"(Joseph A. Grau, "Selling Security," Security Awareness Bulletin No. 2-89 (May 1989), p. 1-13) proposed various marketing principles to sell our business. We would like to add market segmentation, which is a phrase used for describing a situation in which the customer is not viewed simply as the customer, but rather as part of market with diverse needs.

Examples of market segmentation are in evidence when employees are addressed as software developers, production staff, program managers, technical support/secretarial staff, security guards, contract management, custodial staff, or senior management instead of as all cleared personnel or all personnel. The point, of course, is that different groups of employees require and respond to different kinds and levels of information. The information that senior management needs to protect information, for example, is drastically different from the information needs of software developers or security guards. Senior management normally needs to keep informed on a general level about the various safeguards and procedures the organization has in place for protecting information. Security guards, on the other hand, normally need to know how to ensure that the information is protected from a physical standpoint.

With some planning, it is not difficult to identify audiences with common needs. In marketing parlance, the vendor who focuses on the customer is rewarded with follow-up sales.

Communication

Clear communication is essential in any security awareness program. And the major responsibility for ensuring that information is communicated clearly rests squarely on the shoulders of the security professional. Perhaps the first rule for the security professional as it relates to clear communication is, as Louellen Essex puts it, to understand the customer's frame of reference before making a statement.(Louellen Essex, "Checklist Helps Clear Channels for Participant Communications," Creative Training Techniques Vol. 3, No. 1 (January 1990), p.2) Important questions to ask in gaining this understanding are questions such as:

1. To what audience or market segment is the information being directed: Developers? Management? Custodial Staff? Secretarial Staff?

2. Has this market segment had prior exposure to the information? If so, to what extent? If not, is there likely to be any apprehension associated with the initial exposure?

3. What level of formality in presentation is the market segment accustomed to? Highly formal? Somewhat

formal? Informal?

4. Is the responsiveness of the market segment likely to be affected by the time of year, month, or day selected for presenting the information?

As these questions are addressed, the security professional will find it necessary to comply with the FCC requirements--that is, he or she will find it highly advantageous to be flexible, current, and creative in executing the security awareness program.

Flexible

Being flexible requires the ability to adapt to change. If it is found that some programs do not add value or are considered to be of no use, we as security professionals must ask whether we should continue to run the programs the same old way, or even to discontinue them.

We must understand that, with the diversified work force of today, which will be even more diversified in the future, flexibility is not a nice-to-have option. It is a must. No two groups of individuals will react the same way to the same information. Therefore, we must have enough flexibility in our security awareness programs to adjust to the differences that may be inherent in a diverse audience.

Current

There is much to be learned from the past. However, we must learn to select from the past only what is necessary and, leave the rest there. There are definitely lessons to be learned from the Boyce, Bell, Cavanaugh, Pollard, Pelton, Chin, and Walker cases--lessons that should never be forgotten. At the same time, we cannot afford to ignore the lessons springing from the current changes in Eastern Europe and the increased theft of high technology. Indeed, pointing out the lessons inherent in current events helps to emphasize that we are combatting a clear and present danger.

Creative

Studies have proven that creative training can enhance the learning process. We as security professionals must continue to learn about the techniques professional trainers employ, such as:

- Practical hands-on exercises
- Role playing
- Group discussion and information finding
- Participant presentations after learning experience.

Information protection is a serious business, but it does not have to be boring. The security professional who uses creative techniques will keep the customer interested and also increase the customer's respect for the security awareness program.

Summary

In an era of unprecedented change, information protection is increasingly important. We as security professionals will be successful in meeting the challenges of the future to the extent that we comprehend the wisdom of diversifying our security awareness programs in scope and in method.

OTHER SUGGESTED READINGS

Broardwell, Martin M., and P. Carol Broardwell. "Reaching for Rapport." Designing and Delivering Cost-Effective Training and Measuring Results (Minneapolis, MN: Lakewood Publications, 1988), p. 319.

Fagans, A.E. "Security for the 1990's Remains a Tough Challenge." NSI Advisory Vol. 5, No. 6 (January 1990), p. 11.

Walker, Robbin. "Check Attitude to Communicate Positive Expectations to Class." Creative Training Techniques Vol. 2, No. 12 (December 1989), p. 2.

SECURITY STARTS AT THE TOP

Neal W. Tuggle
Sverdup Technology, Inc.

Security Must be Included in Planning and Operations

Any defense-related organization that is big enough to hire a security professional, but does not include that specialist in the decision-making process, is probably receiving less than full value, and may be costing itself money. Effective security measures can and do save scarce resources. Security is less than fully effective, however, if the security specialist is not involved in all aspects of the organization, from

strategic planning through customer delivery. This will happen only if the senior security professional receives the direct support of the organization's top executive official.

Security in the Reactive Mode

In too many organizations, security has become a function to be tolerated at best, and avoided or worked around at worst. Security is perceived as, and sometimes is, the enforcement office that looks for ways to say why something cannot be done. Two contributing factors have led to that harmful organizational attitude. The first may happily be nearing extinction: the old-time security manager who understood uniforms and rules, but who could not see gray areas, squelched innovative solutions,and avoided taking risks. The second remains with us today: management that brings security disciplines into play only after all decisions have been made or a loss has occurred. When management adds on security measures at that point, they become expensive. This is what I call the reactive security mode.

Security in the Proactive Mode

Proactive security, on the other hand, engages the security specialist in all phases of program management. It is much cheaper to build the required security into a program than to add it on afterwards. This holds true whether we are protecting information or products. You may think this premise is self-evident, and there is no need to expound on it. Unfortunately, in companies even today, security is either considered after all other program elements are implemented, or early planning is accomplished by management based on what was used in the past.

Continuing Improvement

I do not mean to imply that previous experience should be ignored. I submit, however, that with our expending technology, there is probably a better, cheaper, more efficient method for protecting anything than was available previously, even if only last year. Any organization that does not have and use its available security expertise is simply not being as efficient and cost effective as it could be.

Caution: Nonstandard Security Terminology

Simple examples of proactive security are unfortunately not easy to provide. Before giving several, I must add a word of caution. Although security is evolving into a recognized profession, we are sometimes splintered that common terms do not have common meanings. When I use the term closed area, it means one thing to a defense contractor, something else for a bank security manager, and has still another meaning for the military security specialist. Therefore, I will use basic security terms and define them, without apologizing for doing so.

A Success Story

I will given an example from my personal knowledge of reactive security that turned into proactive security. A manufacturer was told by a government customer to provide protection for a part being built. The contractor program manager took that direction to management, an architect was hired, plans were drawn up, and bids were invited. After reviewing the bids, management asked the security manager to comment on the lowest one of $850,000 for adequacy. The security manager looked not only at the plans but also the basis for them, and determined that it was not necessary to secure the entire plant. Only the finished product and one small part during assembly needed protection. He was also aware that another product line was already using a secure room for products awaiting shipment to a different customer. His recommendation: Purchase three metal cabinets to store the part on the assembly line, with a total cost of $2,800 to achieve compliance with customer requirements. In this case, the total outlay for the contract was significantly reduced. Had the security manager been involved from the start, however, additional administrative and management costs could have been avoided as well.

Diverse Security Skills Needed

A professional security manager should be able to bring to bear the knowledge necessary to provide adequate protection for the company or government organization at the least cost. This holds true whether the security issues relate to classification management expertise for guiding the handling and layout of a new program, to architectural expertise to advise on the physical layout of a new building, or to personnel security issues related to handling and processing of employees during a reduction in force.

Conclusion

Cost effective security can be provided to an organization only if the security manager is fully involved in the decision-making process. If the security

professional is supported by the senior executive of the organization at that location, the security manager can be more productive. Removing the security manager from the senior executive increases the cost of providing adequate security and reduces security effectiveness. You should look for, and document, areas where the organization could have saved money if the security manager had been in the decision-making loop. If you cannot find any such instances, have you been to any security seminars or taken any courses recently? They will help keep you looking sharp.

UPGRADING SECURITY CLASSIFICATION AND EXTENDING DOWNGRADING AND DECLASSIFICATION DATES: IMPACT ON INDUSTRY

John S. Bowers
Westinghouse Electric Corporation

At times it becomes necessary to protect certain information at a higher level or for longer periods than originally anticipated. This may occur when classified systems are provided to foreign countries and the classification is upgraded or extended to accommodate requirements of a foreign government.

User agencies often do not fully consider the ramifications of such actions at the time when such decisions are made, however. The impact on industry can be significant. For example, upgrading information from Confidential to Secret involves locating all copies of the unaccountable Confidential documents and hardware and placing them under security accountability. Such a change may have less of an impact upon U.S. Government agencies.

Probably the most common reason for extending the security classification is that systems are kept in the active inventory much longer than originally anticipated. This is especially true where Reserve units and foreign countries are involved. The current austere budget environment will undoubtedly increase these occurrences rather than decrease them.

The number of documents to be upgraded or extended will depend upon such things as the technology involved, system parameters, sensitivity, and size of the program or system. In any case, considerable time, effort, and expense are involved in determining which Confidential documents and hardware are affected.

In addition to locating and re-marking documents locally, a contractor must determine if copies were transmitted to subcontractors. Where this is known, subcontractors must be contacted and directed to re-mark, destroy, or return the items.

For small research or study programs, this obviously does not present a large problem. But when many Confidential drawings, specifications, and reports have been generated internally, it can be virtually impossible to locate and re-mark all items. When this occurs near the completion of a contract, or after the contract is already completed, the contractor will not have the funds available to upgrade the items.

A similar situation occurs when the downgrade or declassification date is extended near or after the completion of a contract. Since most production contracts require that contractors provide aperture cards for all drawings and specifications, it becomes painfully evident that a contractor cannot simply pull the original drawings and extend the downgrading markings to the new date.

Actually, changing the original drawing is just the proverbial tip of the iceberg because an engineering drawing Revision Notice (RN) must first be prepared and processed. Then the original drawing must be located, re-marked, and a new photo processed to create another aperture card containing the extended date and new markings.

There is a significant cost to write and process an RN, which includes approximately four hours of engineering and drafting time for each drawing or specification. Using a costing rate of $70.00 per hour times four hours, we have a cost of $280.00 for each such change. As required by contract, a new set of aperture cards (prepared in accordance with MIL M 9859, type 1, class 1) must be created at an approximate cost of $0.16 for each card prepared. Normally, four cards are required by contractors and an additional card must be provided to the customer. Many times these revised documents must also be provided to subcontractors.

On most production contracts, there is a requirement to maintain these drawings and specifications for the purpose of providing spares and repairs for the systems still in use by the U.S. armed forces. Also, many systems are provided to foreign

countries under Foreign Military Sales or on commercial contracts approved for release on export licenses.

Additionally, many contracts require that warranty clauses and training and operation manuals must be maintained. Therefore, the documents must be available for use even after the contract has been completed.

When a user revises a security classification guide (SCG), especially for production contracts, without thoroughly considering the effects that the changes mandate, serious problems and greater expenditures will most certainly result.

Industrial firms have also observed that the changes imposed by revised SCGs are frequently ignored by the various military units which maintain documents and equipment. Generally, the reason that military units do not make required changes is because they have no resources to take appropriate action.

When the U.S. Government user agency fails to make the necessary changes, the information could be compromised--or at least subject to a discrepancy notice--even though contractors dutifully took the appropriate action. To illustrate, contractors regularly receive defective units from the field which contains outdated or unrevised markings. Also, user agencies send improperly marked correspondence that does not accord with the current or revised SCG.

Industry is not interested in simply fighting the problem. Rather, U.S. Government original classification authorities must be made aware of the ramifications and costs of their upgrading and classification extension decisions. Those decisions should never be made in a vacuum without thorough review and understanding of the consequences. Interaction and coordination between user agencies and contractors will go a long way toward improving security measures in such cases.

INCORPORATING THE CONTROL OF UNCLASSIFIED-SENSITIVE INFORMATION INTO THE DEFENSE INDUSTRIAL SECURITY PROGRAM

James J. Bagley, R. B. Associates, Inc.
Charles H. Kocher, Martin Marietta Astronautics Group

Introduction

With the enactment of Public Law 98-94, the Secretary of Defense was given the authority to limit the dissemination of certain unclassified technical data.

Section 1217 of the Defense Authorization Act of September 24, 1983 was implemented by Department of Defense (DoD) Directive 5230.25 dated November 6, 1984. The directive "applies to all unclassified technical data with military or space application in the possession of, or under the control of, a DoD Component which may not be exported lawfully without an approval, authorization, or license under E.O. 12470 or the Arms Export Control Act. However, the application of this Directive is limited only to such technical data that disclose critical technology with military or space application." (DoD Directive 5230.25 of November 6, 1984, "Withholding of Unclassified Technical Data from Public Disclosure")

The Problem

Traditionally, organizations which deal with classified information have had the task of managing and controlling both classified and certain types of unclassified information. Controlling unclassified information was seldom considered to be a security problem, in spite of the fact that unclassified information has been subject to distribution controls through a number of laws which have been in effect for many years. Moreover, there is some unclassified information not authorized for public dissemination under the Freedom of Information Act and the U.S. Criminal Code. Thus, the problem facing industry, in particular, is how to rationalize the rules and integrate into a coherent control mechanism the requirements of the U.S. Government to protect unclassified-sensitive information, as well as the requirement to protect classified information. This paper proposes a plan which could be accomplished using the existing inspection assets of the U.S. Government (regardless of the real possibilities of reduction in those assets in the days ahead) by incorporating the overall oversight responsibility into the Defense Industrial Security Program (DISP).

Some Background

The principal DoD directive on controlling unclassified information is 5230.25 which, in the opinion of these writers, may not be well understood by the Defense community. As a result, it has been variously interpreted and used frequently to deny

access to information by people and organizations who may have a legitimate right to access. Ironically, the fact is that some requestors are denied access to unclassified information when access would be authorized if the information were classified.

The important first step in this examination is to detail the policies and limitations of the DoD directive:

- The directive "does not modify or supplant the regulations promulgated under E.O. 12470, the Arms Export Control Act governing the export of technical data, that is, 15 CFR 379 of the Export Administration Regulations (EAR) and 22 CFR 125 of the International Traffic in Arms Regulation, (ITAR)."

- The directive "does not pertain to, or affect, the release of technical data by DoD Components to foreign governments, international organizations, or their representatives or contractors, pursuant to official agreements or formal arrangements with the U.S. Government, or pursuant to U.S. Government-licensed transactions involving such entities or individuals. In the absence of such U.S. Government-sanctioned relationships, however, this Directive does apply."

- Technical Data with military or space application may be withheld from pubic disclosure if such data cannot be exported without a valid license. However, technical data may not be withheld if otherwise permitted pursuant to a general, unrestricted license or exemption if permitted under the export control laws/regulations.

- Unclassified data that are not governed by DoD 5230.25 unless otherwise restricted, shall be made available to the public as well as state and local governments.

- Technical data may be provided to individuals and enterprises that are determined to be currently qualified U.S. contractors when such data relates to a legitimate business for which the contractor is certified.

- Technical data may be provided to the Congress, or any Federal, State, or local governmental agency that requires such data for regulatory or governmental purpose. Any such dissemination shall include a statement that the technical data are controlled by the DoD.

- The directive may not be used to withhold from public disclosure unclassified information regarding DoD operations, policies, activities, or programs, including the costs and evaluations of performance and reliability of military space equipment. When such information does disclose technical data subject to the directive, the technical data shall be excised from that which will be publically disclosed.

- The directive may not be used as a basis for the release of limited rights or restrictive rights data as defined in the DoD Federal Acquisition Regulation Supplement, or that are authorized to be withheld from public disclosure under the Freedom of Act (5 USC 552(b)(3) and (4). However, the directive may be used as a basis for denial under the Freedom of Information Act (FOIA) of technical data determined to be subject to the provisions of the directive.

- The directive may not be used to provide protection for technical information that should be classified in accordance with current directives.

The Implementation Process

The directive defined "Qualified U.S. Contractor" and established the procedures for a contractor to become qualified, and spelled out the responsibilities of any recipient of such information. Furthermore, the directive established the conditions by which a Canadian contractor may become qualified. It may be helpful at this juncture to re-emphasize the following points:

- The directive does not modify or supplant the export control laws. Therefore, it could be concluded that a valid export control license to have access to comparable technical data, or at least, provide justification for such access.

- There is no steadfast prohibition on foreign dissemination, as the directive specifically authorizes dissemination to companies of countries with which there are formal exchange agreements.

- Not stated specifically, or included in the reference used for this paper, is the point that most Memoranda of Understanding (MOUs) include specific requirements for the protection of classified and unclassified controlled information such as patents, proprietary information, and bid or proposal data, as well as information protected under privacy statutes.(Federal Acquisition Regulation (FAR), Part 25, Defense Federal Acquisition Regulation (DFAR) Part 225) Also not stated is the fact that most foreign-owned firms which do business in the U.S. are

incorporated in the U.S. and subject to U.S. laws as well as laws of the countries of origin. Thus, a failure to comply could make foreign owned company liable under the laws of the U.S. and the parent country.

Distribution Limitation Statements

It is often forgotten that the requirements for distribution statements on technical documents have been in effect for years. The current Directive replaced a directive which was issued in 1970 and was the result of the additional responsibilities to control military and space information (DoD Directive 5200.20, "Distribution Statements on Technical Documents", of September 24, 1970, canceled and replaced by DoD Directive 5230.24 of November 20, 1984, "Distribution Statements on Technical Documents). It also should be noted that the Congress has required the Department of Energy to control certain unclassified nuclear information (10 CFR Part 1017, "Identification and Protection of Unclassified Controlled Nuclear Information").

What to Do: A Cost Effective Proposal

There are sufficient regulations in place to control the dissemination of unclassified information which the laws of this country have mandated should be controlled. All to often it is overlooked that:

- The ubiquitous DD Form 254 is a contract specification issued under the authority of the Federal Acquisition Regulation (FAR) and the DoD implementation thereof.

- "The FAR is the primary regulation for use by all Federal Executive agencies ... PL96-83." (FAR, Subpart 1.1, Purpose, Authority, Issuance)

- Most of the Federal Executive Branch Agencies (User Agencies) who award contracts to industry are included in the DoD Industrial Security Program (DoD Industrial Security Manual for Safeguarding Classified Information, para 1.c. March 1989 edition). (Obviously those agencies have statutory authority to control the dissemination of their unclassified information. Classified information is controlled by EO 12356).

- Contractors who export are bound by the export control laws, and depending on the scope of their business, have internal mechanisms to manage and control exports. However, in many companies, export and security are separate entities, and, in some, are not even part of the contracting function.

There are citations and references in the Industrial Security Manual (ISM) to inform contractors of the legal requirements to control the export of technical data. Oversight is solely the responsibility of the DoD Components (DoD Directive 5230.25 of November 6, 1984, "Withholding of Unclassified Technical Data from Public Disclosure", p.8). (See also page B of DoDD5230.24) The Directive was issued under the sponsorship of the Under Secretary of Defense for Research and Engineering (USDR&E) and is not, per se, a "security" directive.

Given the background and the need to control the dissemination of certain unclassified information and to use current existing directives, we make several recommendations.

First, the Industrial Security Regulation (ISR) and the ISM should be revised to include responsibility for oversight of that unclassified information required to be controlled in accordance with statutory and regulatory requirements and which are the result of contractual requirements accepted by industry such as, but not limited to, export controls. (See also references 1,2,3,4,5)

Second, several actions should be taken to implement existing requirements:

a. The instructions for preparation of a DD Form 254 (ISM) be modified to include guidance and requirements for the control of classified and unclassified controlled information.

b. The DD Form 1423, "Contract Data Requirements List", be made an annex to the DD Form 254.

c. Military Standard 1806, "Marking Technical Data Prepared By or For The Department of Defense", also be made an annex to the DD Form 254.

Conclusions

Although there have been many requirements placed on both government and industry to protect against the unauthorized dissemination of unclassified sensitive information, there is not a coherent mechanism to surveil the process and to provide reasonable assurance that the sense of the laws be carried out. At the same time, there is not an effective

mechanism to assist contractors in carrying out their responsibilities resulting from a plethora of regulations for which compliance is mandatory and the penalties severe. It is insufficient to enforce export restrictions when the information to support an export may well have already been exported years before.

The DISP is the single point where all elements of a requirement come together. The point of merger is a contract which is a legally enforceable document. When a contractor accepts the terms and conditions of a contract, the firm is legally responsible for compliance. Unfortunately many times the security elements of a contract become the tail wagging the dog. Security is an afterthought: First, get the contract; then worry about the details. And, as is apparent, security and export concerns are an important detail.

All too often, the security manager is not thought of as part of the procurement or acquisition team in the government, or part of the bid and proposal team in industry. The key is that the driving force in any acquisition is the need to provide the goods and services required to fill an operational requirement.

Security personnel should not be thought of as the "No Sayers," but rather as a vital, albeit not overriding, element in the acquisition and procurement process. And, as NCMS has been preaching for many years, security is an eclectic process and a Cognizant Security Office (CSO) or Facility Security Officer (FSO) should be a competent generalist who knows a good deal about effective management.

Finally, the DISP is really the key to competent and judicious compliance; it makes sense.

LET'S TAKE A GOOD LOOK AT CLASSIFIED VISITS

Jeanne Bastoni
Dynamics Research Corporation

Visits by personnel from one DoD contractor to another can cause considerable annoyance when the visit requires access to classified information. The "Industrial Security manual (ISM), DoD 5220.22-M, states that "All classified visits require advance notification to, and approval of, the place being visited" using a written request. Sounds simple enough, right?

Wrong! There is not a direct contractor or subcontractor relationship, the Visit Authorization Request (VAR) must be signed by a contracting officer. "Simple" ends where the contracting officer certification begins.

If your company does not have a resident representative of the contracting authority readily available to sign VARs, you may be led a merry chase with considerable waste of time and effort trying to get an authorized signature. Your company's administrative or procuring contracting officer at a remote location may not be willing to sign VARs without the blessing of the technical program manager, so the request is referred to the program or project office. More delay! You will be lucky if, after running the gamut of authorizations, your VAR arrives at the facility to be visited anywhere close to the actual visit date.

The January 1991 edition of the ISM defines direct contractual relationships as Category 1, deleting all others. Most contractors have observed this as a rule, although, formerly, Category 1 visits included those associated contractors who were working on the same defense program under separate contracts. This made sense. These contractors should be permitted to visit and exchange classified information with one another. There are better ways to establish need-to-know in such cases than chasing after an authorized signature for VAR when time is of the essence.

On rare occasions, a facility may accept an advance copy of a VAR from a non-contract-related contractor, with a certified copy to follow. This saves time but not effort. It is still a hassle to get the authorized signature on the original VAR.

Remember that the ultimate responsibility for releasing classified information lies with the holder. The holder of classified information must make a judgment before releasing it, regardless of what the VAR says or how many signatures are on it. There should be reasonable prior knowledge of the need to release the information to the visitor. The VAR is not a license to obtain classified information. It is an aid in determining one's eligibility for access.

Speaking of eligibility, the Facility Security Officer (FSO) or the FSO designee signature on the VAR is accepted as verification of the listed employees' security clearances and other identifying information. Assuming that the requesting facility's clearance has been verified by the Defense Investigative Service/

Personnel Investigations Center (DIS/PIC), why is the FSO's signature not also acceptable as verification that the facility is, in fact, working under a specific DoD contract on a specified program? It would be easy to deduce that the visitor's facility and the host facility were associated contractors on the same program and have a need to exchange information. After all, it is equally important that the individual's clearance information be valid as well as the need-to-know; therefore, the FSO should be authorized to certify both.

Despite the narrow perception of the Category 1 visit, there is some creative thinking in practice. A blanket authorization letter was sent recently by a U.S. Air Force contracting officer to all contractors engaged in a certain program. A list of all facilities involved in the program was attached. The letter authorized the exchange of classified information and processing of visit requests as Category 1 among all facilities listed, provided the purpose of the visit pertained to the program. In addition, the letter stated, "You are hereby authorized to forward a copy of this letter to your sub-contractors, related program contractors, and government elements as their authorization for exchanges between the listed facilities". Kudos to the author of this innovative solution to an obstructive problem.

There is another possible solution to determining the qualification of a classified visit based on association of contractors on a common program. Why not attach a copy of the corresponding DD 254 (Contract Security Classification Specification) to the VAR? This document indicates the work being performed and usually the program it supports. It is also signed by a responsible representative of the user agency. This could satisfy the requirement for a signature on the certification of need-to-know.

When a potential host facility receives a VAR with a DD 254 attached, and it indicates a program on which their own company is performing, the visit should be honored. This assumes, of course, that the facility clearance has been verified and is current. If the security personnel have any doubts, perhaps referring the request to the point of contract indicated on the VAR would clarify the need-to-know. Most of the technical people know which contractors are involved in the program on which they are working. Since the technical people are probably the ones who will release the classified information, they are in a far better position to determine the visitor's need-to-know than the personnel in the security office or, in fact, an administrative contracting officer.

If any doubts remain, a telephone call to the project office where the DD 254 was signed should provide clarification. The phone number usually appears on the form.

It may also be possible to have the DD 254 annotated in the remarks section that this contract will require the exchange of information between contractors; therefore, classified visits should be approved. A list of all other co-contractors may be attached or not, depending on whether the list was available at the time of issuance of the DD 254.

All things considered, the whole process of visitor control should be objectively reviewed. In some areas, there is too much control, serving no practical purpose. For example, consider a facility where constant escort of visitors is required--especially one where the classified material comprises documents and computer media. If a visitor, whether cleared or not, eludes the escort, where would he/she go, and who would be so irresponsible as to release classified information to such a visitor? All the AISs (automated information systems) are in closed or protected areas, so these would be somewhat difficult to access. As for documents, remember, they must be under constant surveillance when not locked up. It might be better to have all those visitor escorts use their time to check on unattended classified material. It may also be better to spend more time instructing employees to be personally responsible for safeguarding classified material in their possession. Too much physical plant protection and control tend psychologically to relieve individuals of their personal responsibilities. Carelessness may be the result.

Let us be realistic about visitor control. How many cases of espionage are perpetrated by a foreign agent entering a defense contractor's facility or military base as a visitor and stealing documents? Usually, classified information is compromised by cleared individuals . . . those who have legitimate access.

There appears to be an encouraging trend to concentrate on the individual's integrity and ability to safeguard classified information. Adverse information reporting, increased periodic reviews of clearances, drug use in the workplace prohibitions, increased denials of clearances, and increased security education all focus on the individual. It is hoped that we may avoid Big Brother-ism and McCarthy-ism, but it is of utmost importance that a personnel security clearance

be respected as a privilege for only those who qualify. We should have reasonable assurance that the cleared individual is capable and willing to safeguard our country's defense secrets. We would then not become complacent with excessive reliance on physical plant controls and multiple signature requirements that really do not serve the purpose.

SECURITY EDUCATION IN THE DEFENSE INDUSTRIAL SECURITY PROGRAM: AN UNDERUSED TOOL

G. Ernest Govea
TRW Space and Defense Sector

Security briefings and presentations in the Defense Industrial Security Program (DISP) and for carved out contracts (Carved out contracts are classified contracts issued in connection with an approved Special Access Program in which the Defense Investigative Service has been relieved of inspection responsibility in whole in or part) have long been an underused tool for enhancing the security programs of defense contractors. These elements of security education are critical because they not only project an image of the security department and upper management's support for security, but they also present an opportunity to mold the attitudes and consequently the behavior of employees in ways suitable to and preferred by the security organization. Security managers have generally not given sufficient thought to the results produced by briefings and presentations in relation to their degree of quality and sophistication. There is room for dramatic improvement which, if achieved, will enhance the effectiveness and the image of security in the eyes of the employees. Better briefings will help capture the support of upper management for the security organization. The results will be employees who are not only better informed and more sensitized to indicators of espionage, but more willing to comply with our requirements and to report questionable practices and conduct.

I will cite the example of a young security specialist who delivered the initial briefing to a group of new employees. He was so nervous the employees thought he would bolt from the room at any moment. Throughout the briefing the employees' attention focused not on briefing content, but rather on his nervousness.

On another occasion, a young female security specialist giving a briefing to a group of new employees mentioned almost as an afterthought, that violations of certain sections of Title 18 were punishable by death or life imprisonment. The employees were struck by the contrast between a very serious message and the empty manner in which it was delivered. The security employee seemed to have little idea as to what she was saying.

On still another occasion concerning a carved out program, a young woman delivered a briefing on computer security to a group of program security officers. She spoke very rapidly and ended abruptly, using voice tones and body language that discouraged questions. Later, a security office representative confided that her knowledge of computer security did not extend much beyond the content of the briefing, and that before her briefings she always hoped no one would ask her questions.

These and many other embarrassing presentations are less the fault of the people who delivered them and more a reflection on management which allowed them to occur. Too frequently, we have assigned security education responsibilities to personnel who were not adequately trained, sufficiently knowledgeable, or genuinely dedicated. The results have been briefings and presentations that demean the security organization, detract from the mission of the awareness program, and promote the notion that upper management is not supportive of the security organization. Consequently, the recipients of ineffective briefings and presentations conclude, or at least speculate, that the security function is merely ritualistic, exists largely as a contractual requirement, and is so unimportant that responsibility for executing it falls on individuals whose qualifications are less than adequate.

Consider the character of the recipients of our briefings and presentations. They are a mixed lot, to be sure. But a substantial percentage are intelligent, highly educated and skilled professionals who are not about to be overwhelmed by security people whose knowledge is superficial and whose training abilities are mediocre. A poor security briefing can actually be more harmful than no briefing at all, especially for new employees who have preconceived notions of what security entails, only to have their expectations dashed.

We find later it is difficult to gain the sincere support of those employees who have witnessed

firsthand the product of our security organization, an office whose abilities to combat the sophisticated methods of hostile intelligence services they now question.

We all know employees who were unimpressed with and even contemptuous of security requirements. In many cases those attitudes were formed for reasons we may never know or understand. In some instances, those attitudes are reflective of disdain for what the employees perceive as ineptitude or, at best, mediocre performance. In some instances, security education has been responsible for the formulation of those attitudes. Those attitudes, coupled with the prevalent view that espionage is something that happens to someone else, serve to make our jobs more difficult. More alarming, they increase the level of security vulnerability.

In defense of management, it must be said that frequently resources are spread thin and tight schedules do not allow time for adequate training and preparation. The battle to locate and recruit quality security personnel is sometimes lost. But too often we have not given sufficient thought to the real damage done by inferior presentations and briefings, or to the potential benefits and rewards to be had as a result of superior briefings.

Superior briefings support the impression that upper management is concerned about the quality of the security program, and therefore the conscientiousness of the employees. They also demonstrate that the security department is staffed by competent, intelligent and knowledgeable specialists who are conveying the expectations of upper management as to employee conduct. Most importantly, they sensitize the employees to threats posed by foreign intelligence services, thus increasing the likelihood they will recognize behavior that may be indicative of espionage, and subsequently report their observations.

The unhappy truth is that, as far as publically known, all this is in spite of our elaborate systems, complex procedures, and millions of dollars expended. True, detecting spies is not our primary responsibility. Contractor security has never been responsible for the detection of a single spy. But mechanisms for the detection of espionage do exist in the DISP and particularly for carved out programs. They have never worked.

When friends and co-workers of William Bell noticed his improved standard of living and inquired as to where he was getting his money, his reply was that he had received a pay raise. Had they investigated further they would have realized that it would have taken an enormous increase in pay to justify his expenditures. Most of us are aware that merit increases which dramatically improve one's standard of living are extremely rare. Yet people accepted Bell's explanation, apparently giving no thought to wrongdoing. Part of the reason is that Americans, and very probably most nationalities have an abhorrence of reporting on each other. It is a taboo we are conditioned against from childhood. But much of the problem stemmed from a triple failure on the part of security education. First, Bell did not recognize that he was being recruited. Second, he did not report contact with a representative of a designated country. And third, the suspicions of Bell's co-workers were not sufficiently aroused.

Today's security departments are staffed by many intelligent, competent individuals whose experience, abilities and academic achievements are praiseworthy. However, those individuals usually have contact with only a limited number of employees outside the security department, and so the true character of the security organization goes unrecognized and unnoticed by the majority of the employee population. What gets noticed, however, are the security specialists whose responsibilities to deliver briefings bring them into contact with large numbers of employees, including those who will never handle classified material. If they do not adequately represent the security program an accurate and undesirable image is projected.

Personnel responsibilities for security education are among the most important in the organization. They represent the security director or manager who selects and allows them to remain in place. They also represent upper management, whose policies they promulgate, and, because of their high visibility, the entire security organization. Many security personnel labor behind the scenes, enjoying successes and enduring failures. But none are so well known as the security educators whose efforts are revealed in forum. Most employees will judge the entire security organization based on observations of training received.

The primary gauge by which contractor employees will measure and subsequently assign their own level of support, is the degree of support which they perceive to be bestowed by upper management.

Generally, no support from upper management equates to no support from the employees. In an environment in which employees perceive only superficial support from management, security conscientiousness actually becomes the aberration because its existence is an anomaly. In such environments there is decreased awareness. Procedures are not followed and violations not reported. Improper conduct and deviation from the rules, when observed by others, are likely to go ignored and unreported. An employee who observes another reproducing classified documents outside of the requirements, is likely to conclude that the perpetrator is circumventing the cumbersome system in order to be more efficient, giving no thought to the possibility of espionage or of reporting the incident. Some employees may go beyond merely circumventing the system. They may attempt to, and succeed in, removing classified material for the purpose of transferring it to a foreign national. Certainly, an employee will not be motivated to commit espionage based on the quality of briefings. But an employee with ill intent, who perceives his adversary as astute and competent, will be influenced and possibly dissuaded.

In selecting personnel for security education responsibilities, management should select individuals who are comfortable in front of large groups. They must be able to articulate policy and procedures. They must be professional in appearance and mannerisms. They should be knowledgeable of company's policies and procedures and of government requirements. They must have in-depth knowledge of espionage cases and be acquainted with recruitment methods. They must be familiar with indicators of espionage and recognize that they are fluid. They should be able to discuss intelligently current global political affairs and how they may impact on the security and interests of our country. They should have a good knowledge of the industry, its past, present and projected future. They must be able to grip and hold the attention of their audience. And they must execute their briefings and presentations in such a way that when released, the attendees feel they have witnessed a high quality employee in action, that the employee is reflective of the entire security organization, and that upper management expects compliance and cooperation from the employees.

In order for security employees to enhance their knowledge of espionage cases, the intelligence community, global affairs, the defense industry and Government and company requirements, a fair amount of their own time must be invested in reading some of the many excellent publications on those subjects. They must also follow events reported by the news media. Unfortunately, some educators will balk at such a notion, but should first consider this. We constantly flatter ourselves by claiming the title of professional. Many years ago, a professional was an individual engaged in a profession which required considerable academic preparation. Today, everyone claims to be a professional. Most of them are actually experts or specialists. There are many elements that compromise the true professional. The key element is education. Simply attaining certain levels of education however, is not sufficient. A non-degreed individual, while not educated by society's standards, but who is knowledgeable and well informed, is more valuable than the individual who attained a degree and then slipped into academic indolence. True professionals are individuals continuously involved in study, not only to stay current, but as a practical necessity in meeting the requirements of their profession.

Security educators must also recognize that briefings and presentations are an opportunity to influence the attitudes of attendees. If their attitudes can be influenced, their behavior can be modified. Our colleagues in the intelligence community have always understood and exploited this connection. Yet few of us in the defense contractor arena have sufficiently utilized it to our benefit. Too many of our briefings serve only to inform rather than influence. If we could modify the behavior of our employees, we would select cooperation and compliance. We would want them to willingly report violations, adverse information and viable suspicions. Our educators should study the techniques of some of history's great orators such as Abraham Lincoln, John Kennedy, Martin Luther King, Jr. and other great speakers whose words inspired people and spurred them into action. The point is that educators must perceive their responsibilities as exceeding the mere passing of information. Rather, it includes inspiring employees. It is not sufficient to tell COMSEC custodians that their combinations must be changed every six months. They must be able to appreciate, based on history, the sensitivity of their classified material, and based on examples of disastrous compromises, clearly understand why extraordinary security measures are required. The worst compromises are not those we detect, but the ones we do not know about.

Having a superior security education function will not guarantee harmony and a problem-free working environment. But no other function in the security

organization holds the ear of the employee population like educators. Therefore, no other function exerts the same degree of influence on them. Superior performance will benefit the entire security organization. Inferior performance will render inferior results.

Peace is being declared in the cold war. Disarmament talks are underway, but there has been no mention of easing up in collection efforts. Quite the contrary, not only are there indications that hostile intelligence services are as active as ever, but the relaxation of tensions with the Soviet Union is resulting in record numbers of people immigrating, visiting and otherwise entering the U.S. for official purposes. Many of them are entering with intelligence missions. Today's security educators must stay abreast of these events and keep in tune with how they affect our national security. An old military maxim says "never underestimate the enemy." The same applies in our business. But it is not only our old foes of whom we must wary. Indeed, even some of our allies who have readily accepted our generous aid have run espionage operations against us. There are still secrets to be kept and if America is to remain strong, a strong defense posture is and always will be necessary. Consequently, it is as important as ever that people with access to classified material be sufficiently educated about the threat of hostile intelligence agencies. They must be able to thwart recruitment and recognize those who are recruited and those who have volunteered.

Security managers must begin to redefine the goals and objectives of security education, placing dramatically increased emphasis on the development of innovative techniques for influencing and inspiring contractor employees. This must be based on high quality educational programs that exceed established paradigms, and in recognition that high quality products are the result of high quality people. Solid criteria for security educators must be established and clearly understood by new people recruited for educator positions. Many educators in place can undoubtedly contribute significantly to the formulation of those criteria and be willing to meet new standards. Those who can not, must be replaced with those who can. For too long we have ignored the real potential of Security Education. Corrections now by those in positions to do so, will benefit our profession and the national security. Inaction means continued mediocrity.