CLASSIFICATION MANAGEMENT

JOURNAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XXVII 1991

ISSN-0009-8434

Published by the National Classification Management Society. Mailing address: Executive Secretary, NCMS, 6116 Roseland Drive, Rockville, Maryland 20852. Editor of this volume: Eugene Suto, NCMS Editorial Oversight: Carol F. Donner. The information contained in this Journal and presented by various individuals does not necessarily represent the views of the organizations they represent -- unless they head their organization, or the National Classification Management Society.

CONTENTS

PROCEEDINGS OF THE 27TH ANNUAL TRAINING SEMINAR JUNE 24-26, 1991

PART 1. Speakers and Panelists

PART I

SPEAKERS AND PANELISTS

THE POLITICS OF DEFENSE

24 June 1991

Admiral Bobby R. Inman

The title I agreed to speak to is "The Politics of Defense." When I thought of that and my 30 plus years of being covered by the Hatch Act, even though I'm no longer covered, I gave it a subtitle--"Managing Security in a Dramatically Changing Environment."

I graduated from the University of Texas in 1950. My view of national security was shaped by a very clear understanding of who were our friends and who were adversaries. NATO had just been created. It was a world that was framed by clear alliances that indeed shaped the framework of how we thought about national security and how we managed it. It would be difficult to over- exaggerate how dramatic the changes have been just in these last two years.

But particularly important to me is the mission you carry forward now. Let's look first at the evolving threats to security that come out of this changing world with the demise of the Warsaw Pact. For most of my adult life we operated on the presumption not only of a huge and diligent KGB, but all the resources that were brought by the intelligence services of the Warsaw Pact. And many of them were very, very capable. Look at some of the more spectacular successes--the East Germans. Occasionally the Poles added to what the KGB could do, and outside the Warsaw Pact, Cuba.

One of the major questions for me is, "Now where go those East European services?" Are they going to be a challenge to us? My answer is probably, yes, not directly reporting to the KGB as a service. I've got a strong hunch that there are a lot of individuals who spent their life there who are hedging their bets. They'll be beating a fast path to Bonn, Brussels, London, and Washington, but they'll also keep their contacts with the East.

The Soviet Union is undergoing a very dramatic change. We don't know the outcome but we all got a chance to observe this this past week, when the head of the KGB, Mr. Kryuchkov, undertook to once again label the US as the cause of all the economic problems related to espionage and entrapment. He was prepared to do that at the potential expense of part of the power of his patron. The KGB is not yet deciding it is time to pull in its horns and be less aggressive in its activities.

There have been dramatic changes in the People's Republic of China. And, indeed to my astonishment, changes in North Korea. There is an application to join the UN. They have indicated a willingness to accept observers to do nuclear inspection at a recent visit sponsored by the Asia Society of a number of U.S. corporation CEO's and journalists. As you look at all the openness in the Soviet Union and some in China, that goes up and down, and now in North Korea,I'm suggesting there's another side of that coin.

Along with openness will also come access, because we have many more of our own citizens traveling to those countries and there will be reciprocal visits as well. Therefore, there will be new players looking for ways to derive information that they believe is important to their own government.

At least as dramatic is the shift in the nature of the international market place. In 1960, less than three percent of our gross national product was derived from international trade. By the end of this year it will be somewhere around 14-15% of a vastly larger gross national product. There is no going back to a domestic market place if we are going to have any prospect of sustaining our standard of living.

Then, as one thinks about managing security, increasingly our national security evolves around our economic performance in the international market place. Our principle competitors are our primary political and military allies. Indeed, they are going to see their economic interest making it essential that they make a concentrated effort to understand what's going on in the US government and what's going in US industry. Indeed, the lines will be blurred between government espionage efforts and industrial espionage efforts.

In the past we tended to think about industrial espionage as a problem between competing US corporations or occasionally, with a little publicity of things like the Hitachi case, focused on a single one of our economic competitors.

My suggestion to you, as you think about managing in this exciting future world, is to sort out industrial espionage from government directed espionage. Ask if the industry in that competing country is totally free market-driven or is it government owned.

For many years, as I practiced the intelligence profession, and worked at both protecting US classified information and trying to derive information other countries wanted to keep secret, we thought in terms of defending against concentrated efforts via the governments. Increasingly, we now think about concentrated efforts by industry, at least in some countries. Let me suggest to you there is yet another problem out there on the horizon. That's the enormous wealth that has been accrued by the narcotics barons. And indeed, as one thinks about security devices, protection for classified communications, we may be on the edge or even past the edge of an era where vast amounts of money from the narcotics area will be poured into efforts either to defeat electronic protection or in fact to use it as a new method of finding out what government efforts are underway to try to detect and prosecute narcotics activities.

I spent two years, late 1988 to early 1991, serving on a panel put together by the chairman and vice chairman of the Senate Select Committe on Intelligence, better known as the Jacobs Panel, looking at counter-intelligence. I crammed that into the schedule partly, I think, out of a guilty conscience for having spent so little time focusing on counterintelligence in all my active years of government service.

It crystallized for me again what one thinks about change. Our counterintelligence processes were developed and focused for many years on counterintelligence challenges provided either by individuals who were ideologically sympathetic to other governments or who were being blackmailed. The reality at the end of the 1980's is that there are virtually no ideologically committed spies. Further, it is pretty hard to blackmail people for life style in the late 1980's. But the new phenomena is the US volunteer. We have a counterintelligence process that was developed to deal with these other processes, not the volunteer. There will be significant efforts going forward to enact legislation which will give those in the business some additional tools to lead with the challenge of the US volunteer. But my suggestion to you, again, as you think about these challenges ahead of you is how do you deal with a volunteer that is volunteering to help a friendly foreign country or even businesses in another country for personal gain as opposed to simply volunteering to help the foreign government for that gain. Indeed as we have greater difficulty sorting out who are friends and who are foes, the one constant is that the information we have set out to protect has a vast array of people who would like to access it, sometimes for national security purposes but more often for commercial gain.

As I focus on the incredible change in the national security arrangements abroad and on the reality of the changes in who are spies, we also have to look at the incredible changes in the management of information. Again, as I go back to my early days of entering this process, we looked at investment in communications and in computers, as a necessary expense to sort of keep up, but not really recognizing, in the government's eye as quickly as we should have, the critical importance for productivity gains. The reality is that we aren't going to have more people or more money either in government or in industry to undertake these challenges. We're going to have to look for productivity in the management of the protection of our information systems. And here is the explosion in the use of telecommunications and microprocessors which give us wonderful ways to move vast quantities of data in tiny fractions of the time we used to consider. It also says that information is being moved and stowed in ways we never contemplated back when we thought simply about how do you protect the document or the knowledge that an individual carries in his or her head.

Indeed we are in a period where we are facing major changes to the very concepts of national security. The new world order is the phrase we hear repeatedly. It is a little hard to define at this point exactly what this new world order will be. But what drives the search for a new world order is a sense that the old world order that I spoke of at the beginning, of a NATO and a Warsaw Pact, and bilateral US alliances that completed a circle for containment, are at best undergoing change and in some cases, perhaps headed for dissolution. NATO was already under significant pressure as an institution before the collapse of the Communist regimes in Eastern Europe.

The reality is that of a growing economic community with a different set of members where primary concerns were addressed daily by finance ministers and foreign ministers who then gathered every six months as the defense ministers and foreign ministers to talk about policy under the NATO umbrella. What became increasingly apparent over the last several years was that North America was frequently excluded from much of that daily dialogue, driven by economic concerns. So I believe, NATO as an institution, would have been under very significant pressure after 1992 when the EC moves to its next stage of development, even if we hadn't had the demise of the Warsaw Pact. There is now a scramble underway to determine what will be the shape of security alliances in Europe going forward. Will it be something that is based on the model of the Helsinki Accords that covers security from the Kuriles to the Aleutians and leaves out Japan? Will it be a slightly expanded NATO or will NATO stay as it is but simply change its boundaries and change its approach or will NATO indeed wither away with European security be increasingly in the hands of the Western European union or some evolvement under EC?

In thinking about management going forward, which is fundamentally why we share information with our allies, there are some critically important issues. Will there be new alliances? I talked about the trend in Europe with the common market. What if we are successful in recreating North America as the world's largest market with the US/Mexico Agreement and have US, Mexico, and Canada? Where does that, over time, take us? Strategically, we want to protect information related to our economic success or progress or weaknesses from those in other countries who might use them to our disadvantage.

And then there was the Gulf War. NATO didn't provide the basis for that. The UN actually functioned to some degree as we had planned it back in the 40's, but only for getting approval. The actual operations weren't conducted under the UN Military Committee. They were conducted under a loose coalition of forces. I have been deeply engaged now for some months on the President's Foreign Intelligence Advisory Board in looking at how intelligence performed throughout that conflict. One of the things that pops up is that we had long standing arrangements for sharing classified information. We have our NATO allies, and bilateral arrangements with a number of countries. But we've never thought about providing support for coalition forces. It was done superbly, as best I can tell. It was done sort of "on the fly" and I would suggest that if many of the classification management specialists could see what was actually done in a hurry, they would shudder. It worked, but it's going to raise an awful lot of questions and it will certainly have created appetites to know much more about what we have in the way of capabilities that we do not routinely share even with some of our long time allies.

Let me focus briefly in thinking about the politics of defense and the changing environment for managing security to the US willingness to invest in national security. I see a number of familiar faces in this room who know that I have fought pretty fiercely to maintain my political independence in the almost nine years since I retired from government service. That came under more intense pressure in 1988 than ever before. And my way to evade it was to get deeply involved in transition issues during the campaign and the candidates from both sides eventually accepted that that was probably a better contribution than I could make otherwise in any case. I worked defense issues for strategic and national studies. I was the resident liberal at the Center for Strategic and International Studies, and at the Center for National Policy I was their resident conservative. What it did was to give me access to a lot of money to poll U.S. attitudes about investment and defense. The results shouldn't surprise you, but they did surprise me a little at the time.

What I found was that if the topic had appeared on prime time evening news for 90 seconds three or more times, undecided's in a poll were 8% or less. If the topic had only rarely been covered or not covered at all, the number of undecided's in a poll went up to the 28, 30, 32%

bracket. So we talked about burden sharing with allies, 32% were undecided. And about evenly divided on what we should do. Should we reduce investment in defense-- only 8% are undecided, 62% say we should reduce. We pursued that to understand if it was tied to visions of this changing world, and found no correlation. It was tied to a basic view of not getting value for dollars spent--waste, fraud, and abuse. That's what the public had seen repeatedly and it shaped their attitude about investment.

I have been going down to Williamsburg biannually, for a long time, to help the Library of Congress indoctrinate newly elected members of the House and the Senate. I found, in January of 1989, a very receptive audience in focusing on the outside world and how it was changing. They were curious about it. But then when I was followed by two major speakers from the Department of Defense, the only questions that the newly elected had for them was, "Where do we cut?" And they were very direct. The only thing they were interested in was where should we make the reductions. Indeed, by the summer of 1989 support for the defense budget appeared to be in a free fall. And it wasn't at all clear how that was going to come out. That continued until the summer of 1990 and then suddenly Saddam Hussein, (Hollywood couldn't have cast a better villain,) elected to move into Kuwait. The US responded and public attitudes began to shift dramatically. We don't yet know how long that impact will be sustained. But what we do know is that the image of competence of the management of the military has changed dramatically. It is not clear yet that attitudes about defense procurement have changed that dramatically, but over time there has to be some positive benefit from how well the hardware worked and how well it performed in very hostile environments.

But while the Gulf War was going on, the Executive Branch and the Congress entered into a new budget agreement. The budget deficit had not been harnessed by Gramm/Rudman/Hollings. Loopholes continued to be found, and the extraordinary inflationary pressures which were harming our entire economy had continued to grow. So a new agreement was devised, at very substantial loss of political capital on the part of the president, and in that agreement funding levels for the next five years for defense or foreign aid security arrangements and for the domestic program were set. There is an enormous reluctance, I find, both in the Congress and in the Executive Branch to do anything to upset that agreement.

What that says is that we have locked in a 25% reduction in investment in the national security account over these next five years. And not withstanding the success in the Gulf, that is not likely to change. The good news is that 25% does appear to be a floor at this point in time and sharper reductions in these next years are not likely. But stay tuned. If the world continues to evolve, there will be heavy pressures again when this agreement ends to aim for another 25% reduction.

As one thinks about the consequences of those changes in levels of investment, we also have to look at what's happening out in the commercial world in developing new technology, what's happening internationally in pushing the new frontiers of new technology, and candidly look at the practices of a procurement process begun in the 60's, growing throughout the 70's and 80's which has taken us through a defense procurement cycle that used to be 4 to 5 years and is now more often 12 to 13 years in moving new technology to product. The reality is that it is increasingly rare when technology evolves into product for defense until well after comparable technologies are already in commercial use. There are some very important exceptions--materials, the whole area of stealth. But when I was growing up in the process, the cutting edge of use of new technology was usually found in support of national security--in computers, in telecommunications, and in a variety of sensors and systems. Increasingly, in many areas the cutting edge is commercial. So when you think through the reality of that change and the consequences of a declining defense budget and the investment that can be made, I believe the lesson that is out there for us is that we've got to move as a country towards a single technology base. We simply won't be able to afford, and we won't protect the national security needs if we stay on this track we've been on of a totally separate defense technology base from a commercial technology base.

This has many ramifications. Detailed military specifications drive the approach toward a military technology base that was mandatory when quality didn't exist in US products. In this changing world I think that's something we simply won't be able to afford and increasingly we're going to have to be in a process where we can accelerate invest-

ment in many technologies which will likely be dual use, but insuring early access and use for national security needs. And you will have already jumped ahead of me to begin thinking about the ramifications of that for protection of classified information. If you're going to have a common technology base, what is it you protect? You try to protect the basic technology or is it the applications of technology and if so, for how long and in what circumstance? Indeed, as one looks forward to the complexity of managing a more complex environment with less money, I would suggest to you one of the biggest challenges is going to be to focus much more clearly than I was ever able to do back in the days when I used to build a lot of compartmented systems to protect new technology. I have no apologies for the early protection for stealth. I think it gave us a great lead over other countries in its use. But what we never did well was to construct an equally good approach to how did we take technology out of the compartments? Indeed how did we take away the classification barriers when there was no longer a driving need?

My experience in dealing with government users and industry users of classified information is skepticism about the value of what we do when we set out to manage the protection of classified information. And as I probe that, I find time and again that skepticism grows from anecdotal evidence of information which they don't believe reasonably needs to be protected. It is very difficult to put in place a process that produces a free flow, much harder to do that than it is to make an initial decision of how to protect and to put things in a protective envelope. I think in the exciting challenges ahead of you, one of the ones that will be very difficult but ultimately enormously productive will be designing new systems which ensure conscious sunset provisions but that will dramatically alter the way information can flow and reduce barriers as there is no longer a compelling need to protect. There will always be some need to protect information.

Statement: Admiral Inman has agreed to some questions and answers, so do we have any questions from the floor for the Admiral, please?

Question: One of your last points seemed to me what I heard, I thought, was perhaps that we need to move in an area of protecting less information, but protect it better. Is that one solution perhaps for absorbing that 25% decline in the defense budget as it might pertain to our security mechanisms?

Answer: I think you got a good deal of it exactly right. But the more complex part of it is going to be that it's a continuous process. If you could be certain that you could simply go back and sort through what's now classified and say OK, this goes out, we'll protect this, and do it as a one time evolution, I think all of us could set out to do that pretty easily. What I'm suggesting to you is that this is going to need to be a rolling event that goes on constantly. And how does one sets out to do that? Maybe I'm an excessive optimist about automation, and what this marriage of telecommunications and information systems is going to permit, but I think we've got to get out there and harness it early to let us literally, on an ongoing, day to day basis, be able to sort out and constantly change the targets of what we're going to protect. The hardest part will be the learned judgments of when to make the shift. But nobody else is going to be more competent to do it than this group, of that I'm certain.

Question: Do you see this as an opportunity to work toward breaking down some of the barriers in combining security functions? What's classified and what should be the resources of the intelligence community?

Answer: I'd have to tell you I'm skeptical only because I'm a little worried it's going to end up being bureaucratic again. I've lived through a period of the late 70's where a new leadership came in determined to dramatically change the whole classification system. And I don't want to be too discouraging of the efforts but I think the most attractive thing about the program were the pink and blue slides that were used to advertise it, and not its substance. Because what we never were able to get across, when you really think about counterintelligence threats, compartmentation does work. And so my worry is another bureaucratic approach that let's sort of merge and it doesn't deal with the reality that there will be enormously important things to protect. That compartmentation, rather than the specific level of the code words, may turn out to be the most important factor for providing security, but only for a period of time. This is a very complex pyramid. There are areas where you want to protect something even if only for a year or two, simply to give you a lead, but you may not need to do it after that. And current

processes simply don't do that very well. So I don't want to disparage what may turn out to be a wonderful new approach, I'm just very skeptical going back to my experience in the late 70's. It will be more of a bureaucratic management approach than really thinking through what needs to be protected, for how long, at what level, for whom, by, and the degree to which we can merge compartmentation with levels of classification as a more effective way to do the job that needs to be done. We're going to try it. I can't over emphasize the importance of deciding when to take it out. You will have observed a new national hero taking some real pot shots at the performance of intelligence during the Gulf War, based on some anecdotal evidence which was wrong. He was misinformed on events, but the image that was left in his mind and now conveyed to the public at large, was that it was essentially a problem of compartmentation as opposed to the reality of investment in communication capacity to move information rapidly into the hands of people who could use it. It wasn't a compartmentation classification problem at all. It was an investment problem, failure to invest.

Question: Seems like a lot of companies across the country are being scrutinized and as a result, will there be a reduction in their security budgets?

Answer: The natural tendency is to reduce them, it's an overhead expense. Frankly, here's where a degree of your good dialogue with your government counterparts is the critical ingredient. If the government specifies this is the level they want you to have and this is what they expect you to do, I don't know any CEO's who are going to overturn budgets. That's a totally bureaucratic response from somebody who's spent a lot of his life protecting budgets. That's the reality answer as opposed to the good philosophical approach. Indeed I have found, throughout these nine years in the private sector, that most corporate leadership views investment in security at best as a nuisance but at worst as an unnecessary expense. And indeed you find that they are not responding to government in the great reluctance to invest in protection against industrial espionage, unless there is clear evidence. All it takes is another Hitachi scandal and there will be a lot of CEO's who will suddenly be willing to put more corporate resources into protecting proprietary data. But it won't last long unless there are a series of scandals in the process. However, that is just a reality. For those in the national security arena here is where the dialogue back and forth and specificity by the government of what you have to have in order to remain viable in their view will, I think, be the critical ingredient in protecting that corporate security environment and investment.

My answers to solve this problem have been shaped by a variety of experiences in these last nine years--such as four years of heading a research consortia owned by 21 competing firms, work under the auspices of the Counsel on Competitiveness and a two year effort drawing in some of the best brains from industry--looking at nine industrial sectors to say how are we competing for the outside world. A publication was issued last March. It assessed where are we leading, where are we competitive, where are we losing, where are we losing badly, and why. And a parallel ongoing effort, not yet finished, by the Commission on Science, Technology, and Government looking specifically at how the government is organized to manage the government's part of that process. It was a lot easier to define what the critical technologies are than it was either to get U.S. industry to prepare to use the rapidly changing technologies or than it was to get government to organize to make quick decisions on how to create the environment to support the process. On the first part of it, the corporate side, there are still far too many corporations who simply believe that unless they create the technology or that they were given it by the government and directed to use it, they can't derive a competitive advantage of it. Here's where studying the Japanese model for just a little while is very instructive. They frequently get access about the same time and go to the market place both in Japan and elsewhere. They collaborate in accessing the technology and then compete fiercely with their own product and go to the market place. On the US government side, here I'm afraid my frustration sort of bubbles over. We set out in 1947 with the National Security Act to organize how we thought about coping with national security in a very organized way. It had its critics, but I would argue that for the intervening now 44 years, national security policy has been shaped, altered, executed, on balance with substantial effectiveness. We have no comparable way of approaching domestic policy. There is no structure like the National Security Council, the National Security Council staff, and the National Security Advisor to coherently look at the range of issues which get at our economic liability and success. Whether it's health or education--a whole range of problems in

getting at this issue--there will be a Carnegie Commission Report in another month or two, I'm not nearly as proud of this one as I am of the Council on Competitiveness report "Gaining New Ground". Because we simply have not been able, even internally, to get solid agreement for change. What I found was that most views are still those shaped by people while they served in government. If they were on the Council of Economic Advisors, they have a view. If they were with the National Science Foundation, they have a totally different view. You raised the prospect of charging the National Security Council with a wider view to deal with these issues and they instantly think of somebody they did not like who was the National Security Advisor 5 years, or 10 years, or 20 years ago. You can't close on the reality of the need to change government organization and structure to deal with the reality that how we compete at the international market place ultimately is the overriding solid basis for national security. It isn't an either or. We're not going to be successful in the national security arena unless we are far more successful in competing in the international market place, and there are a whole range of domestic challenges that have to be solved in that process. Managing this technology is just one of those elements. It may be possible to extract the management of investment in research and development out of that larger problem and make some progress. I've been reluctant to do that because of a sense that we need to force addressing all of the issues and not just that. But my frustration level is somewhere up to about here and I may fall off and be willing to accept part of the loaf to get on with how government manages their role in this process-making priorities, trading off, how much do you invest in large sciences against small sciences, what are the incentives you use in the tax code to get industry to do what they ought to be doing at the pace at which they use technology. How to use the tax code to not just deal with the cost of capital but the readily available supply of capital to apply technology. One of my proposals which wins me no friends in the financial community, is a simple tax code change that says from pension funds for any asset held less than three years, 85% tax on capital gain. For any asset held longer than three years, 10%. Changing overnight, get rid of all the program trading by pension funds and force them to focus on what's going to be the gain three years out. I'll hear about this as soon as I get back to the next board meeting because that says instead of earning the pension needs this year, we're probably going to have to pay out a profit into the pension funds. But if you're looking for stability for investment, which is critical for changing the attitudes for the approach that our international competitors have, on focusing on the speed with which you turn technology into a product, absolute quality, and planning from the beginning to introduce change, how do you manage the cost of change. It has to be the focus on the process and not how do you get a production line and let it run as long as you can with minimum change and don't worry about quality and incidentally lose most of the market share to the foreign products that compete. Thank you very much for your kindness. ■

NEW WORLD DISINFORMATION

24 June 1991

Prof. Lawrence Martin Bittman

It is a great pleasure to be with you. This morning, when I attended the session with the guest speaker, I was very envious because he was not only educational, he was also very entertaining. That is one of my problems. Of course, I can not communicate the way you do because English is not my native language. When I started teaching at Boston University 20 years ago, now I'm one of the old timers, I always was envious when I listened to my colleagues who could be witty, and entertaining, and educational. So I tried to always start with some joke and it was always a disaster because most of my jokes were European or East European and the students were looking at me and thinking, "What is he talking about, this guy?" So I abandoned this practice. Nevertheless, I want to start with a story which is symptomatic of the situation in Eastern Europe. About six weeks ago, I found an interesting article in one of the Czech newspapers. I subscribe to a number of Czech newspapers and all of them came with a very interesting story about a Czech terrorist who was just arrested in Prague. His name is Musik. The story is quite interesting but there was particularly one sentence or one paragraph that really stimulated my interest because it's about me. Mr Musik was a Czech agent who was sent to West Germany shortly after the Soviet invasion of Czechoslovakia in 1968 as a political refugee to get a job with Radio Free Europe. That's what he did. After a couple of months he became a broadcaster for the Czechoslovakia desk of Radio Free Europe and worked for that institution for a number of years until 1975 when West German counter intelligence became a little suspicious and he had to desert. He surfaced in Prague and that was the beginning of a huge propaganda and disinformation campaign against Radio Free Europe that lasted for about two years. Czech intelligence made him a hero who spent seven years or so in West Germany, who supposedly collected a lot of top secret information. They made a number of statements against Radio Free Europe to undermine the reputation of the station, to threaten people not to get in touch with Radio Free Europe.

Well now, Mr Musik was arrested not for working for Radio Free Europe, he was arrested because it was found that he sent Prague a number of proposals to conduct terrorist operations against Radio Free Europe. And, as some of you probably know, that's what happened in 1981. Radio Free Europe was bombed. Several people were seriously injured and the building of the Czechoslovak desk was very damaged. That's why he was arrested.

When they investigated the papers and the proposals that he sent to Prague, they discovered, at least this is what the article says, several proposals he also sent to Prague on how to assassinate me in the United States. He also volunteered to do the job. It's not pleasant reading for someone like me, but frankly, it's not so simple. It is relatively simple to kidnap somebody from Austria. That's why I was in a hurry to get out of Austria in 1968 because Austria was and probably still is, very deeply penetrated by Soviet intelligence. But to kidnap somebody in the United States is not so simple.

One of my former colleagues, who defected about a year after me, wrote in his memoirs that Prague developed a plan on how to kidnap me from the United States, and bring me back to Prague and then to film the interrogations in color and show the film to every officer in the service as a warning. Well, I'm still here. And not only that, last year I got an invitation from Prague to become a director of a cooperative project between Boston University and a University in Prague to investigate Czechoslovakian disinformation campaigns in the last 20 years! So in about four weeks I'm going to Prague. It's still a little risky but I am sure that I'll be back after two weeks.

Now why was the Czechoslovakian intelligence so angry with me? I spent 14 years in the intelligence service in basically all major sectors--in the evaluation and analysis department, in the operational sectors working mainly against German speaking countries, Germany and Austria. Then for two years I was the deputy commander of the department for active measures and disinformation. I had intimate knowledge of these campaigns and this was the first time that somebody from Communist intelligence would come to the West with the intimate knowledge of disinformation and active measures. There were, of course, a lot of defectors who came with some knowledge of this area, but for the first time somebody who was directly involved in the conduct of these operations. Obviously, that was a very serious blow for Soviet active measures.

In 1971 I was sentenced to death in absentia and just now the military court is handling the so-called rehabilitation of Lawrence Martin Bittman. It is a democratic process that will take probably another year or so. But at least the new government is handling this. Why am I talking about this? It is symptomatic of the situation now in Eastern Europe. What is happening there, what we can expect? This is the end of the old era of the monstrous Soviet bloc intelligence, espionage organization, that has been involved in penetrating the West and developing countries for nearly four decades.

Official cooperation between Czechoslovakian intelligence and the KGB ended last February when the Czechoslovakian government completely broke off relations with Soviet State Security and prohibited the Czechoslovakian existing state security structure to have any official contact with Soviet intelligence. There is now, of course, discussion on what to do, how to handle this new development. Just in the last couple of weeks there was a discussion in the parliament to create a new intelligence service, relatively small, that would deal mainly with collecting information abroad and presenting this information to the political, military, and economic decision makers. But this new organization is not allowed to conduct disinformation active measures in traditional anti-western, anti-American methods. Now the collapse of the state security structure also created some problems, problems that will last probably several decades. First of all, it was discovered there were 140,000 secret agents or informers among Czech citizens, at all levels inside the government, inside businesses, everywhere. 140,000 official informers. Now after the election a number of people were suddenly accused of being actual informers during the previous regime and it was discovered that several ministers were former agents, including a number of the new parliament. Obviously this is a problem. So they were asked to resign or they would be publicly exposed. Several of them did resign. Some of them are fighting these accusations in court. Because, remember it can also be disinformation. Somebody can accuse a member of the government of being a former Communist agent without any evidence. This is part of the new game. And this is something that will not be resolved in the next couple of months or years. This will stay with Czechoslovakia for at least a decade, probably more, because it creates very good conditions for various disinformation campaigns against individuals who occupied important jobs during the old regime.

Now, in addition to this, of course, there were several thousand Czechoslovakian agents recruited around the world--in America, in Britain, in France, in West Germany, Austria, in developing countries. Now what to do with these people, how to handle this case. And you see when I'm talking about Czechoslovakia, it is not only Czechoslovakia, it's also a matter of Polish agents, Hungarian agents, Bulgarian agents, East German agents. Well, I think this problem hasn't been resolved yet. But the fact is that the Soviets are intimately acquainted with every individual who was recruited by the Czechoslovakian intelligence or the Polish intelligence or the Hungarian intelligence. That means that even if in these new regimes, new intelligence services in Eastern European will refuse any cooperation with the Soviets, Soviets know about these people and they can approach them again and say, "Listen, guy, we know this about you. You were very nice to the Czechs 10 years ago and you cooperated with them for a number of years. Now you will do the same thing for us. And if you don't you will pay the price." So this, of course, creates a situation whereby they can use these people.

Now, let me make a few observations about the KGB today. As you know, the KGB has been untouched until now. Since 1985 Gorbachev introduced a number of reforms, or tried to introduce a number of reforms, but there are certain institutions that he didn't touch. KGB is one of them. KGB is intact the way it was five years ago. It is still operating today. It is wiser, it is much better

prepared for the job, but glasnost, democratization didn't reach the KGB. Basically, the KGB operates under the same state security concept and state security philosophy that it operated under 40 years ago. That was developed during the Stalin years. I don't want to say that the KGB is an organization where everybody thinks along the same line. If you had the opportunity to look at how these people think, what they would like to achieve, you would see that there are two major groups. A group of the old timers who occupy the highest echelons, highest positions in the KGB who, of course, don't like any change, and democratization. The director of the KGB is the typical example. Because they are afraid that eventually, if democracy would enter the Soviet Union and the KGB, they would be punished for what they did 10, 20, to 30 years ago. And then there is a group of young, well educated officers. Some of them spent years abroad in the United States, in Britain, in France, who learned a lot about the West, who would like to see certain changes. So, under the surface there is this competition between the old concept and between this new generation of young KGB operators who are actually much better prepared for the job than their predecessors, the old generation.

Now what about KGB opportunities now? What are they doing in the field of collecting information and in the field of disinformation which is actually my major concern? How does the KGB in the year of glasnost and peristroika operate? Along with openness comes greater access. About two months ago, one of my colleagues, a professor at Boston University, came with a gentleman to my office and said I'm going to introduce you to this man who is from the Soviet Union and briefly described what he's doing. My colleague, the professor, is working on a book about the Soviet Union. And he left this Russian with me in my office, so I had an interesting discussion for about an hour with this gentleman. After that discussion I realized very clearly that this was a KGB officer. A number of very clear signals that, for somebody who spent 14 years in the business clearly showed who this guy is. He works for the Institute for the Study of the United States and Canada which is a typical Soviet institution where between 30 and 40 persons or staff members are KGB operators and use it as a cover. He spent years in the United States. He was fluent in American English. He spent years in the United States stationed with the American Embassy supposedly as an expert in the field of agriculture. Well, a number of signals very clearly showed that he's a KGB man. After this, the following day, I talked to my colleague and said, listen I just want to give you some friendly advice. This is what I think about the man. You should be careful. At first he was surprised and then he said, "maybe he's a KGB man, so what?" He works in the field of agriculture. If we can help Soviet agriculture, that would be only to their benefit and to our benefit. And then, of course, I told him what more he could expect if he continues this relationship. In the future, it means basically what the Soviets want from this colleague of mine. I don't think they would like to recruit him, but to use him to open the door to a great many experts in various fields in the United States so that they will be able to meet a great many academic experts, and great many governmental officials, and this new era of openness offers a lot of opportunities for them.

In the field of active measures and disinformation the Soviets have two huge structures that they use. One is the structure for the official propaganda that is mainly promoting the positive image of the Soviet Union, and tries to influence public opinion in the West in a positive manner. That is to promote the Soviet Union, Soviet policies, and use official channels including very modern techniques like lobbying. The Soviet Union today is the third or fourth largest foreign lobbyist customer in the United States. They hire American companies to do it so that they are using our mechanisms now. And then they have this secret structure for propaganda and disinformation and influence operations. There are operations that are supposed to influence the decision making process in the West or public opinion in the West through secret channels, through recruited individuals, and through various secret campaigns. Some of them are ridiculous, and some of them have very little impact. Some of them are quite sophisticated. To give you an example from the years of my involvement, for a while I was a case officer on a member of the West German parliament and a member of the Defense Committee of the West German parliament. Of course, he was used as a source of information about West German defense policies and also about American troops stationed in West Germany. But not only that. Because of his position he was able to influence the decision making process in West Germany during certain situations. So he received instructions on how to react when certain issues were discussed in the committee or in the forum of the parliament. He served also as an agent of influ-

ence. There were quite a few people who were recruited among journalists in West Germany, in France, in Austria and other countries who published, on a regular or occasional basis, articles according to the instructions they received from Prague. This was done on a very systematic basis.

Disinformation or dissemination of deliberately distorted information and deceiving the adversary is, and of course, has been a standard tool of foreign policy used by the Soviets. For decades the Soviets and their satellites were polluting information and communication networks with heavy doses of disinformation. Now there is no doubt that there are reforms in the Soviet Union, with the new political climate. There is greater candor, stimulated considerable changes in the Soviet Union, including changes in Soviet science. Since 1985 Soviet science has experienced greater openness and less ideological conscriptions.

In the year of peristroika and glasnost the major priority of the KGB is to help the Soviet economy with massive infusions of western technology and economic and commercial information needed for advantageous business with western companies. And this is now what dominates the Soviet effort. You see 10 years ago, 15 years ago, and 20 years ago, the Soviets were obsessed with political information and, of course, military information to know what the Americans were thinking, how the American government official, and the British and West German were thinking, and what they were preparing in the political field. Now they are mainly interested in economic affairs, in scientific discoveries, and in technology information. This is priority number one. And they think this is a need in the present situation.

Creativity is the major secret behind the success of most American business companies. International pirates of all political colors have been stealing American inventions and ideas, ignoring copyright protection and patent rights. The US international trade established in 1988 that stealing American ideas, inventions, and technology cost as much as $61 billion annually in lost revenues, profits and royalties. The KGB, the GRU, the Ministry of Defense, and several other Soviet agencies have been involved in activities for over 40 years of stealing important western technology. And these operations required also tactical disinformation. It is not only a matter of getting access to new technology or scientific information, but also to cover it. To cover this act with disinformation because if they get access to certain technology, they have to deceive the country of the origin where this technology is heading and where it is ending. What is the end station for this operation?

The Soviet Chamber of Commerce and Industry, for example, is one of the cover organizations serving both legitimate commercial interests as well as the KGB. It was headed until recently by a KGB Lieutenant General who was also on the USSR Trade and Economy Council. About one-third of the 140 officials of the Soviet Chamber of Commerce are either KGB or GRU officers who specialize in scientific, technological, and commercial intelligence. The Chamber has also been involved in systematic commercial disinformation by manipulating end user documentation of products which western nations allow to be exported to Communist countries.

Another institution which is very heavily involved in both stealing information and also to a degree in disinformation activities is the Moscow Bank which is the center of numerous organization transactions helping the Soviets in financial dealings with the West, most of which are legal and legitimate. It is also used as a vehicle for intelligence operations, trying to penetrate the western financial world. A small bank in a western country can be a tremendously important source of information to a tremendously important institution. When I talked to some of my American friends, they said, "so what if they purchase a small bank, they will not change the American system. What can they do with this?" Obviously, they are not going to change the system, but a bank is a tremendously important institution in a capitalist system. First of all, it has intimate knowledge of a great number of individuals, their financial profiles, policies, and various organizations financial policies, and international contacts of a great many organizations. And, of course, this can then be very easily used not only as a source of information but also for manipulative purposes.

Well, we were lucky 15 years ago, when we discovered Soviet efforts to purchase two banks in the United States secretly. It was publicly exposed and the Soviets didn't succeed. But who knows, maybe they succeeded in other countries.

Well, let me finally make a few comments about the ultimate disinformation machine that we

are facing now. And that is the new era of disinformation which is highly organized, and potentially very dangerous. The era connected with computers.

Computers may eventually emerge as the ultimate weapons for criminals, terrorists, and also for foreign adversaries of the United States. Computers are used by governments, universities, science labs, as well as businesses and banks to speed up transactions, to collect, to absorb, and to analyze a great deal of information on individual clients. Computers are used openly or secretly to monitor communications and every modern military system relies on extensive use of computers. The Soviets together with at least a dozen other countries are very much involved in the secret business of stealing foreign computer security programs. Both the Soviet Union and American institutions are also studying the use of computers for international disinformation purposes, and for disrupting other nations computers by infecting them with viruses or self-destructive programs. The potential for offensive use of computer viruses is really great. You probably know about a great many instances in the last ten years when the Communist countries were exposed when they tried to get access to certain computer programs. There were a few people arrested. In Germany in 1989 or 1990, the Germans arrested a group who penetrated the American computer system and were able to steal through telephones from Germany some important information from American computer banks. They were arrested and some of them were sentenced.

Now what about computer disinformation? This is the really ultimate method. If somebody is able to steal information from computers, it is also possible to use computers to disorient the program, to manipulate the existing program or programs with the help of viruses. And this can have a really devastating impact on the decision making process of military, science, and other areas. When a virus penetrated an unclassified military computer network in the United States in November 1988, defense department officials played down the importance of this incident by saying it was impossible for such a virus to penetrate classified computer networks that managed nuclear weapons systems. They didn't say that a virus introduced into the system by an individual with access to the computer hardware can survive undetected for a long period of time because it does not have to be activated. At the right moment, for example, a military attack, the agent would insert the message triggering the virus. It would either erase all information or paralyze the system or send messages so that the military commands would create total world organized chaos.

Well this is, of course, not only a matter of potential danger from our major countries abroad, it is also a danger that major criminal organizations can eventually use as their weapon, for their own purposes, or international foreign terrorist organizations would use it for political purposes.

I would like to conclude my observations with the conclusion that obviously the competition will go on. Obviously the secret war between the United States and the Soviet Union will go on. Intelligence operations will continue. They will become much more sophisticated. The new era of relative openness and growing friendship between the two countries doesn't mean that the Soviets are changing their state security policies. They are very heavily involved in intelligence and they will continue doing so.

Question: Professor Bittman, could you give us one or two examples within about the last five years of major disinformation programs that were mounted against the United States by the Soviets or their surrogates and what the repercussions were?

Answer: In the last 10 years I think that there were a number of operations that had considerable impact on public opinion particularly in developing countries. I would like to mention one thing in connection with disinformation campaigns. According to my opinion, the influence of Soviet propagandistic disinformation campaigns on the American public is relatively small. I think that their official propaganda is much more effective than secret propaganda that they try to use to influence American public opinion. However, they have been quite successful in influencing public opinion in developing countries such as in Latin America, Africa, and Asia. One of the campaigns that was very successful, anti-American campaigns, was the campaign using AIDS. Saying that AIDS was developed in America and then distributed throughout the world by American soldiers, infecting people in the developing world. It is going on even today. It started about seven years ago and once successful disinformation is inserted into the international communication network, usually it goes on and on for a long time. If it is in tune with the prevailing feelings and biases in these countries

and obviously in developing countries, for example in Africa, it is much easier for people and the governments to think that AIDS is an imperialist virus that came from the United States rather than to accept the theory that it started somewhere in Central Africa. And that means that most disinformation, the successful disinformation campaigns, are feeding upon existing prejudices and biases, and that is the case of AIDS.

A similar case, the baby parts campaign, for example, saying that Americans are adopting children in Latin American countries and importing them to the United States to be used there as a supply for human parts for transplants. Obviously, this is an outrageous accusation, but in many Latin American countries it was accepted as truth and repeated again and again in the press. Then, of course, after certain periods of time the Soviet media entered the game. And they said we found it in the Brazilian paper, or in the French paper, and they don't say it started in Moscow. So these, for example, were very successful.

Then there are campaigns which don't attract much attention in the press, but they have also considerable influence on public opinion. All of you remember very well the Cuban boat lift in 1980 when 125,000 Cubans came to this country. Most of them were legitimate political refugees who hated the system. But it was also a useful, very sophisticated Castro disinformation game against the United States. He sent to the United States together with these 125,000, quite a few thousand of the hardest criminals and mental patients. He emptied the mental institutions and he emptied his prisons and sent these criminals to the United States together with legitimate political refugees. His objective was to undermine the Cuban exile community position and reputation in the United States. Cubans were always very proud people, that were trying to rely on themselves. They were strongly anti-Communist, and Castro wanted to change this reputation. If you study this operation, and how it developed, you will discover that it was after several months of great enthusiasm, and welcoming these refugees when suddenly one American city after another started complaining about rapidly growing criminality in the United States. Many of these refugees were young men in their 20's and 30's. No Communist country at that time was getting rid of this manpower. They became involved in criminal activities. One city after another was more and more hesitant to accept more Cuban refugees. Some of the most vicious and brutal crimes were committed by some of the refugees who came on the boat lift. So Castro, in this case, to a degree succeeded in creating certain reservations against the Cubans and undermined the position of Cuban exile communities and organizations in the United States. So I would say it was partially successful, this disinformation operation.

Question: Bob mentioned in the introductory comment that you had a rather difficult transition to a free society. Can you describe how you made the adjustment?

Answer: First of all, I would like to come back to the introductory notes about me. My debriefing ended in Washington, DC when the CIA apparently said "Thank you, it was nice meeting you and good luck," I'm not complaining about that. Actually, I'm very glad it was done this way because I had to find my own place in the American society. Several years ago I wrote a study about defectors from Communist countries in the United States. Many of them had serious problems of adjustment in America, because they grew up in a totalitarian society where the government decided everything. The government gave them an apartment, a job, and everything. Every major decision was made by the party and the government. Now when they came to the United States they thought that this would be the case here. That the government, the CIA, would come and say, "So here you have a job, and would you like this or would you like that," which is, of course, total nonsense. Particularly, in certain fields, like academia, you can imagine what would happen if the CIA would come to the Boston University in 1969 and say, "Here we have a guy, give him a job as a professor." That's absolutely ridiculous. This is the problem with many people like myself who grew up in a totalitarian society and had to get adjusted to the new rules, the new philosophy. You know the most dramatic part of my life was not the moment of escape and being followed by agents and all that stuff. That is probably good for spy stories, but that's nothing in comparison with the drama of adjustment. When you are here and when you face this new society you feel like an idiot. You have to learn everything from scratch, how to make decisions, how to find a job, how to establish a bank account, how to handle your own money, and how to do anything. This takes time. In my case it was about five years. Those were very difficult years. But after that, the last 15 years or so were the best years of my life. It's a marvelous country.

I had to go through the transition period of about five years to learn how this country operates and how to find my own place in this society.

I think that definitely this is the beginning of a new era of also different methods of approaching potential sources. When I look back I see that during my time, the 1950's were still the time when there were some people who worked for the Communist intelligence services for ideological reasons. There were community sympathizers in the west, left oriented individuals, and radicals on the left, but this was rapidly diminishing. And then came the era of blackmail when I would say about 80% of the people recruited in the 1960's and 1970's were blackmailed by force to accept this. Now, of course, we are entering another era of commercial cooperation and friendly contacts. This is a society where money speaks and money is very important. And whether we like it or not there are quite a few individuals who are willing to sell. They don't care about ideological preferences and philosophies if they are approached by a Soviet citizen or agent who says "Listen, I'll give you $200,000 for this. That is the deal, you'll never hear from me again." Obviously there are individuals who will do it. This is one road.

The second road is the friendly connection. The KGB is a huge organization of roughly some 20-22,000 people involved in foreign intelligence. Of course the KGB includes also counter intelligence, and altogether it is about a half million people. About 22,000 of them are involved in foreign intelligence. Here in the United States, three years ago, there were about, I think 1,500 Soviet bloc representatives stationed in the territory of the United States. Roughly 30% or 35% of them were KGB operatives, that is, professional intelligence operatives. Now they will be much more careful in handling their sources in the United States. I think there will be a certain switch from the traditional blackmailing, forceful recruitment, to friendly connections, to develop friendly personal relationships with American journalists, American businessmen, and American scientists. Americans are very generous people. If a Soviet scientist comes and says "We are really in serious trouble, this is what is happening now, we really need your help." Americans wouldn't think about it as violating any American laws but just helping the Soviets to improve the situation and standard of living in the Soviet Union. I think this will be the major role for them. They will go to finding new sources and information that they consider important today.

Question: You mentioned recruitment. In this new period we're entering into, do you feel that there will be equal emphasis on use of front companies and diversions, and do you have any personal knowledge of communications collection against industry?

Answer: I think, I would have to speculate. I believe that they will establish a number of new front organizations, business organizations, and semi-official organizations very heavily staffed with KGB and also ideological cooperators from among Soviet citizens who will operate in the west. But I cannot be more specific. I don't want to guess too much. One thing I need to emphasize very much is that we are facing a new quality on the side of the Soviet intelligence operatives. You see those are not the guys of 30 years ago dressed in ridiculous clothes, speaking with heavily accented English. 90% of them today receive a very good education at the Institute for International Relations in Moscow. All of them speak at least one, some of them two or three languages. You listen to Soviet representatives and journalists speaking on American television. You know how well prepared they are and how much they know about the American environment. That means that there is an equality on their side. We have to realize that these are not the Soviets of the 1950's. We are facing a new generation of Soviet intelligence officers well prepared for this objective and for this new era.

When I look back over the last five or ten years, I see a very clear relationship between Gorbachev and the KGB. Gorbachev was very closely connected with the officer who headed the KGB for 18 years and then was for a short period of time leader of the Communist party. Since 1985 when Gorbachev came to power he has made a number of changes in the party and also in the government. But he has made absolutely no changes in the KGB. The KGB is the same organization, subscribing to the same basic philosophy of KGB today as it was five years ago. Basically, I think that Gorbachev is afraid that if he tries to change the system, to deprive the KGB of the power it has, that it eventually would lead to his end which is possible. You know, we are speculating, but I think that he is afraid to dramatically change the position and influence of the KGB. Personally, I think there is a very good chance, if he makes this attempt, that it may be the beginning of his end. ■

Left to right: Deborah D. Varljens, Gerald Schroeder, Steven Garfinkel, Ernest Mayerfeld, James Rowley

FREEDOM AND SECURITY Can They Live Together?

24 June 1991

Panel Discussion

Moderator :

Steven Garfinkel, Director
Information Security Oversight Office

Panelists:

Ernest Mayerfeld,
Attorney at Law
James Rowley,
Correspondent, Associated Press
Gerald Schroeder,
Department of Justice
Deborah Varljens,
Chief Counsel, Subcommittee on Civil Service

Steve Garfinkel

I need to make a plug for my office, the Information Security Oversight Office, and our participation tomorrow in the boardwalk. I guess a number of you have played over the past five years, this is the fifth anniversary of our game of Security Pursuits. I believe it's the fifth anniversary. It was developed for an NCMS national in Huntsville and I think that's four or five years ago. And in celebration of that, we were thinking about the fact that we hear a great deal now about cooperation between industry and government. We hear all this stuff about the National Industrial Security Program that's bringing us all together. And then we hear about a kinder, gentler DIS and all that stuff. What we would like to do is to bring the hostility back into the relationship. And so in honor of our fifth anniversary of Security Pursuits, we're going to be playing it tomorrow on the boardwalk and we have a special version of the game that all of you have to participate in. We are dedicating this Information Security Oversight Office (ISOO) cup, named as you are probably aware for Lord ISOO, and it says "Information Security Oversight Office Security Pursuits Competition - Government vs Industry." And so tomorrow both sessions, we're going to have a total points game beginning in the morning, ending in the afternoon, and the winning team will be appropriately inscribed on this trophy. We hope to get invited back somewhere so we can amortize the cost of this trophy with a couple of other competitions.

Now for the business at hand. For the most part you have biographical information on this very fine group of speakers who are going to participate as panel members this afternoon. The one person you don't have a bio on yet, and I understand that will be provided, is the person seated at my far right, that's Deborah Varljens. Deborah is not in your biographical information because she was kind enough to substitute for a panel member who because of illness in his family had to pull out at the very last minute. We were extraordinarily lucky, and owing to her good graces, that Deborah agreed to substitute for that fourth panel member. Deborah is the chief counsel of the subcommittee on Civil Service, chaired by the honorable Jerry Socorski. Jerry has been kind enough to have me questioned before him several times. Deborah is the chief counsel for the sub-committee on Civil Service of the House Committee on Post Office and Civil Service. I won't go too much into the rest of her biography except to say that she has had

essentially a two career life where she was a practicing registered nurse and a chief pediatric nurse, helping humanity in all kinds of ways and she left that to become a lawyer and to work for congress.

Now to my immediate right here is Jerry Schroeder. Jerry is the senior counsel for the Office of Intelligence Policy and Review at the Department of Justice. You have his bio essentially in the package of material. What you don't know about Jerry is that Jerry, we believe, is the only person ever to defeat Dan Quayle in an election. This is a true story. Jerry defeated Dan Quayle in an election for the student board of governors at the Indiana University Law School. Is that correct? Obviously, it was handily.

I wanted to say obviously it was an election where looks had nothing to play with the outcome.

On my immediate left is Ernie Mayerfeld. I've known Ernie for 17 years. I first knew him when he was an Assistant General Counsel and he was later Deputy General Counsel of the Central Intelligence Agency. As a little bit of an antidote about Ernie, that you may not know about. Ernie was telling me that when he was head of litigation for CIA he had a case in which his defendant was one George Bush. He was representing George Bush as the government attorney. George Bush, at the time, was Director of Central Intelligence. Ernie told me that one day he was returning to the CIA headquarters from court and as he was approaching the building he saw then CIA Director Bush jogging in his jogging clothes. The CIA director saw Ernie and knew Ernie had been in court, and he ran over to him and asked him how things were going in court that day. Ernie was dressed in a three piece suit and had two big briefcases full of legal material with him and Ernie started to explain how things were going in court when the CIA director became a little impatient and asked Ernie to jog along with him and tell him how things had gone. So carrying two big briefcases and in his three piece suit, Ernie got to jog along with the future president.

Our last panel member on my far left is Jim Rowley. He is legal correspondent, not for ABC but for Associated Press. The interesting thing about Jim that should strike a responsive chord in a number of people here is that Jim, before he decided to become a journalist he worked in the declassification division of the National Archives, declassifying old records. He didn't stay there very long. The records are still there. Still classified.

What we're going to do this afternoon is present some questions to the panel members and get them to respond. I will address the question to a named panel member and then invite the other panel members, and the members of the audience to give their views or ask follow on questions. We want to cover a number of thorny topics in a relatively brief period of time, so it may be that I'm going to have to cut off the discussion and go on to a new topic if it goes on too long.

My first question is for Gerry Schroeder and it goes like this. During a periodic reinvestigation of your eligibility for access to classified information, a source unrevealed to you, alleges that you have regularly attended parties at which cocaine was available for the guests. The Justice Department adjudicator determined that the terms of your clearance must be withdrawn, which in turn makes your continued employment within the Justice Department doubtful. On your Justice Department rules you are entitled to know the allegations upon which the withdrawal of your clearance is based, but not who made the allegations. You are also entitled to make a written reply, and to receive a final written decision from another official. Under these exact circumstances were you an employee of a government contractor, you would be entitled to make both written and oral replies, to be represented by an attorney, and to demand a full blown evidentiary hearing at which you could confront the persons making allegations about you. On the other hand, were you an employee of some government agency, which shall go unnamed, the only information or response to which you would be entitled is the bare fact that you were losing your clearance and probably your job. What possible justification can there be for this double and triple standard? Isn't every employee, no matter where he or she works, entitled to fair and equal treatment? In your personal view, what is the appropriate procedural standard recognizing that one day it could apply to you? And finally, is your personal standard achievable under the current political stalemate?

Jerry Schroeder

None, yes, due process, no.

And I second that.

First I want to say that I was not at the party and if I was at the party I didn't know they were

serving cocaine and if I did know I didn't partake, and if I did partake, then I go back to the first answer, I wasn't there, I was in Cleveland.

The question asked raises a number of issues and it also has been asked, as I'm sure you've noticed, on a very personal level. So I want to say right up front and in all candor, I'd want all the due process I could get my hands on. To include, if you'll pardon the oxymoron, a good lawyer. I think the simple truth is that anyone in that position would feel the same. But that's not surprising. Every bank robber, every mugger, and every burglar that you want to ask will assure you that they want their case to go to the Supreme Court. I understand that and I would too, but the issues that are raised by this question have to be answered more in a policy arena by consideration of other issues other than what the bank robber, and I don't mean to equate people who lose their security clearances to bank robbers, but what the person who is affected would desire, if they had it in their power to create any sort of due process that they wished. Obviously, any sort of due process that doesn't return one's clearance is going to be viewed as having been insufficient.

The government has a number of interests to balance here. And as soon as any sort of suspension of a clearance or notice of revocation is issued, the first thing that happens is that due process is invoked. And that immediately gives, in my judgment, the moral high ground to the person who is the subject of the adjudication and places the government on the defensive. The mere mention of due process seems to compel some sort of automatic acceptance. My own view is that due process is not an end in itself. Its constitutional purpose is to protect a substantive interest to which an individual has a legitimate claim of entitlement. And that last phrase to me is critical. Because as the Supreme Court has said, none of us have any claim of entitlement to access to classified information. It is an inherently discretionary function and decision, unique to the executive branch. Following that Supreme Court case, two circuit courts have held, taking it to its next logical step, and pardon the legalese, but that there is no property or liberty interest on the part of an individual in a security clearance. Now what that means to a lawyer is this. In the absence of a property right or interest or a liberty interest, there are no legal requirements for due process.

I'm becoming very popular, I can see that now.

Now that is not to suggest that there isn't an obligation here out of simple fairness to be fair. I don't think it's in the employees best interest, obviously, and certainly not in the government's best interest as an employer to remove clearances from individuals based on erroneous facts. Seems to me that fundamental fairness requires that there be some notice, some opportunity to respond. I would suggest in writing only, so that if there has been a mistake of fact, if there are mitigating factors, if there are extenuating circumstances, that all of those facts can be brought to bear in the adjudication and be taken into account and given the weight that they are due.

So specifically, Steve, to answer your question regarding the double and triple standards, I don't think there is any justification for different standards. There should be no reason why some agencies of a government have procedures that they follow through revoking security clearances and other agencies having none. In my view there is no legal or practical reason why defense contractor employees should be entitled to full-blown evidentiary hearings while government employees, in some cases, are entitled to nothing and in others are entitled to mere written responses. I would give written responses to everyone and get rid of that cottage industry in the contractor arena.

I think I've answered the second question which is, isn't every employee entitled to fair and equal treatment? Yes. But I emphasize again fair and equal treatment does not always translate, for example, into full-blown evidentiary hearings.

What is the appropriate procedural standard? Put very simply, I'm repeating myself slightly, but I think notice, and opportunity to respond in writing, opportunity to appeal to a different official, other than the one who made the initial determination, and finally, the right to have a statement of reasons at the end of the process. I think that is more than fair and it certainly satisfies any constitutional requirements for due process.

Is this personal standard achievable under the current political stalemate? I think not. Congressman Sikorski had some hearings some years ago. This particular standard was contained in a draft executive order that would have allowed, but not required clearance revocations to be handled

this way in the defense contractor arena and the mere allowance of that possibility, leaving aside any question of mandating it, created enough controversy and discussion and attention in the media that that executive order, at least as of this morning, and this was a number of years ago, has gone nowhere. So the short answer to that question is no.

Thank you Jerry. Deborah would you like to retort.

Deborah Varljens

I've been anxiously awaiting.

I think the unique aspect of the debate between those that would err on the side of the government and those that would err on the side of the individual is that due process rights for the individual, the same rights which the administration objects to, are America's only real national security guarantee. It is the position of the Civil Service sub-committee that the withholding of information that could result in the loss of a security clearance does not improve our security system. In fact, a system devoid of due process will inevitably lead to uninformed, inaccurate, and unwise security clearance decisions grounded on undisclosed gossip, distortion, and mistake and potentially motivated by malice, greed, prejudice, or worse. Eliminating an aggrieved person's right to know the accusations and respond to them does not solve our unauthorized disclosure problems. But it does violate due process. Those that argue that due process procedures which would provide a meaningful response are unnecessary, a meaningful response to us means the opportunity to cross examine those who make accusations against you, and the opportunity for an impartial judge to examine the credibility of the witness against you. These people ignore the stigma that follows the civil servant to a career within a chosen field in which a clearance is vital. Denial of a security clearance frequently means denial of employment and the addition of a black mark against future employment. If anybody has ever been guilty by suspicion I think that is an excellent example of what can happen. Granted it's a long time ago, and hopefully it wouldn't be that bad, but it could be pretty devastating and we have cases day in and day out that show us that at the Civil Service sub-committee. You mentioned Egan and I'd just like to say here that the Supreme Court said in Department of Navy vs Egan that the judicial branch will grant deference to the executive branch in these matters unless Congress specifically provides otherwise. Currently there are two pieces of legislation in draft in Congress which will provide due process to the person who is denied a security clearance.

Steve Garfinkel

Ernie, you used to work for an agency that didn't provide a whole lot in the way of due process. How would you respond?

Ernie Mayerfeld

I don't know, I'm not certain that that allegation is correct. We did provide a great deal of process but it wasn't all that public. There is one problem which an agency like CIA confronts if we proceed along the lines suggested by Deborah here. There could be information which is relevant to the denial of the clearance which unto itself is extremely sensitive which a revelation of that information could come from intelligence sources, and methods, or could in itself reveal secrets that the government needs to protect. What I'm specifically referring to obviously is counter-intelligence information. And simply to make that available along the lines suggested here, I submit may not in all instances be wise.

Steve Garfinkel

Do any of our panel members have any further comments on this particular question?

Does anyone from the audience want to add something before we go on?

Question. The legislation you were talking about that Congress is considering. Are they going to make this legislation apply to them? And do congressional committees at the current time give due process to those individuals they deny access by their committee to classified information?

Deborah Varljens

I'm not sure I understood the second part.

Question/Comment. It is a fact that in at least four instances, the Department of Defense has granted access to classified information when someone on a congressional staff needs access to that information on a need to know basis, and the intelligence community has, in fact, denied them access to classified information. I was wondering if those individuals were given any due process.

Deborah Varljens

I really can't answer that. Not being on that committee, I have no idea, to tell you the truth. In terms of the first one you've got a definite Catch 22 that happens in almost every law that Congress has passed. That is their reluctance to make it apply to themselves. I can't speak to that except to say that our reluctance to not apply it to ourselves does not mean that we should not make the situation correct for over 3 million people that it applies to in the executive branch and contractor employees. Again, I wish I could have a better response to why Congress doesn't pass laws for themselves. Also, I'm not personally saying that I believe it's correct. But, I still don't think that should lead to inaction for the executive branch.

Steve Garfinkel

We're going to go on to the second question. I direct this question to Jim Rowley of the Associated Press. A Pulitzer Prize winning journalist once said to an audience of government and industry security managers brought together by ISOO, and I quote, "It's my job to get the information and it's your job to protect it. If I publish classified information it's because I've succeeded at my job and you've failed at yours." While this standard might provide security managers with an incentive to do a better job, does the end justify the means for successful investigative reporting? If this is not the appropriate standard for a reporter to use in deciding whether to publish classified information, what is? Finally, in a nation where anyone may purport to be a journalist why should journalists be above the law with respect to the unauthorized disclosure of classified information?

Jim Rowley

I think the statement by my Pulitzer Prize winning colleague reflects the swagger that he must feel after having disclosed some sensitive information, but I think it's a blunt but true reflection of the kind of standard the journalistic organizations operate under. We're not in the business of protecting government secrets. We're not in the business of helping the police catch criminals. We're not in the business of helping government agencies right wrongs. Our job is to ferret out information that is newsworthy and to publish it so that our readers or our viewers can make informed choices about how society should solve its problems, how elected or unelected officials are behaving, how governments and institutions are doing their jobs. So that when we report any story we report it without regard for the political or bureaucratic consequences. Working reporters regard themselves as not pushing any particular political point of view. So I think that that statement reflects an accurate, though I must admit, crude formulation of what our job is. We are definitely in a cat and mouse game, an adversarial situation with government officials, police, politicians, and I'm sure many politicians would regard us as above the law, but journalists, to a man, feel that we are an essential part of the system by which this country works. And we do work within the law. We don't burglarize government files, we don't break into offices, we might cast a glance at somebody's desk if there's a memo sitting there, but we wouldn't open the drawer to rifle somebody's papers. We're not in the business of breaking laws. We're in the business of trying to expose things that are wrong, that should be known to the public. In the case of classified information I think there is a caveat to what this reporter once said to this group. We don't just expose and publish information for the sake of doing it. It has to have newsworthy value. And if there's something that could have a danger to somebody's life or a danger to security, we would be in a position of having to balance between the public's need to know the information and the harm that it would cause. We don't just willy-nilly expose secrets for that sake. It has to have newsworthy value. It has to be something that definitely has an impact upon the political process or the public's knowledge of a particular thing. For instance, the Glomar Explorer episode of the mid '70's is one in which a very particular sensitive CIA operation was conducted to salvage submarines that the Soviets had launched and which had sunk at the bottom of the Pacific. Now this was a very sensitive story, there was a great effort on the part of the government to keep this out of the press. But a decision was made at a certain point among news organizations that had the story, that it was vital for the American people to know about it. And sometimes we will balance the need to inform vs the security on the basis of the need to reveal or the ability to reveal the degree of detail. Sometimes the average reader does not need to know the types of details that, if we were to leave out, would really cause a security problem. And, therefore, because of the nature of our ability to synthesize and edit out certain facts which are really not germane to informing the public, we would be in a position where we could get out of the dilemma of publishing something which would cause harm. But it is a determination that we would make ourselves, not totally in a vacuum. If I were to receive a secret that I realized was

probably very sensitive, I wouldn't just rush to the AP wire with it. I'd certainly call the agency that generated it and ask for some sort of comment. That's just done routinely with any story whether it's classified information or not. In that process, certainly there would be some consultation about the wisdom of my publishing this. The agency that was charged with protecting the secret would certainly have a hearing among the people in my organization as to the wisdom of our proceeding with the story. And that's certainly been true time and again in the annals of national security reporting.

The Washington Post sat on a story about the national security agencies listening post in the Western Pacific, which was known as Ivy Bells, a secret project which convicted spy Ronald Pelton had told the KGB about. Long before his trial the Washington Post was onto the story. The effort of the administration was to keep it quiet. In response to requests from the administration, the Post did not publish the story until other news organizations did and then they published a highly sanitized version of it. I think the press' mission is to inform people. We see our role as doing so in a way that will not endanger people's lives or vital programs of this country. For instance, I think that war correspondents have proven time and again in situations when they are sent out with troops that if there's a situation where they are reporting a particular fact or sequence of events that would endanger troops, they would refrain from doing it. What's been particular insulting to the news media, in its recent treatment by the administration, has been a presumption that we don't act responsibly and that's why we were kept in pools and kept segregated from the action in Desert Storm. I think in Vietnam it was proven that the press could be trusted with information that might endanger the lives of troops.

Steve Garfinkel

Why do you think there is a presumption not only within the government, but I think, if the polls are correct, probably among the general citizenry that the media cannot be given that degree of responsibility to make those kinds of judgments. In other words, you are suggesting the very important role that you play, indeed under the Constitution of the United States, but the people don't believe that the media are playing that role appropriately. I think many government officials feel the same way. Certainly there must be some reason for this difference of perception.

Jim Rowley

I think government officials feel it because they get a lot of bad publicity when they do things poorly. When some public official, particularly one in a high place falls, he feels the lash of bad publicity. Therefore, I think there's a hostility that's built in between politicians and the press. I don't detect that the public has an overwhelming hostility toward the way news organizations go about their business. In fact, my dealings with individual members of the public who have worked for government agencies or elsewhere in terms of gathering news is, that people are very anxious to make sure that we get the straight story and they do cooperate with us.

Steve Garfinkel

Do you feel, building on that comment that you made, do you feel that the pooling process should be abandoned by the department?

Jim Rowley

Absolutely. Absolutely.

Steve Garfinkel

Do any of our other panel members have a comment on that?

Gerry Schroeder

I have a couple of observations although I must say in fairness to Jim, I feel a little awkward in making them, because we had a chance to have lunch together earlier and at least as reporters go, he seems to be a very reasonable person. But, two things I think warrant at least further thought, if not discussion. The first is that based on my own experience in handling classified information, there are times when the sensitivity of the information itself is not apparent on its face. In those situations sometimes, frankly, there is no sensitivity to the information which is why it's not apparent. In other cases there is extreme sensitivity and it's not apparent for a variety of reasons. I find it a little troubling, particularly for those reporters who unlike Jim may not check with an agency, but who take a piece of classified information that on its face may not be sensitive and publish it, when as Jim has acknowledged and we all know, lives, literally lives can be at stake with certain kinds of information. Secondly, I have some difficulty although I certainly understand it, don't necessarily agree with it, with the assumption of giving the decision making process to themselves in deciding whether or not something should be published and if I were that source who's life hung in the balance,

I would not want a reporter balancing my need to live with the public's right to know. And secondly this comes from a group of people who don't care too much about the government's sources but who would go to jail before they'd let someone else, like a judge, a real judge, balance interest for their sources.

Jim Rowley

To respond to that last point, I think that reporters would go to jail to protect a government source if that person was put on the line to identify the source of a story that implicated a government source. I think that reason that the decision whether or not to publish a piece of information should only be made by the news organization is that it's just inherent in the first amendment that our basic constitutional protection is that we have a free press in this country. Which is not to say that we need to consult with your office or a government agency, why a particular fact should not be published. You would get a fair hearing in a situation like that. But the press cannot be in the business of deferring a decision about what's newsworthy. There may be all kinds of motives of why governments would want to keep something out of the press because it might cause adverse political reactions or consequences that they are trying to avoid which have nothing to do with the sensitivity of the information that's at issue.

Steve Garfinkel

Jim, I'd like to follow up on your statement about what is newsworthy and responsibility. I have to go back to what this very same journalist said to us about 10 years ago. He was asked a question from the floor and probably some of the people who are out here today were out there 10 years ago when this journalist was asked, "If I hear you correctly sir, what you're telling us is it's your job to decide whether to print a story based first on its sensationalism, second on whether you have the scoop, and third and only third, and that's way back, on the basis of whether it's true." And the journalist stared at the question, put his chin in his hand, and he stared and thought a while. He finally looked up and said "scoop is definitely number one."

Question

This may be very naive, but something I have not understood is when a person, a US citizen, gains access to classified information they sign a statement that they are subject to espionage laws and that it would be criminal activity if they were to divulge that. In a reporters getting information from a person that is classified, you know, gets classified information, is that aiding and abetting a criminal activity and because of the journalistic umbrella is not only able to be prosecuted, but can aid a criminal activity. Could you respond how you feel about that ethically and legally.

Jim Rowley

I think that in most situations where reporters have gained access to classified information it's either through accident or through a calculated leak from somebody within the government and may be politically motivated. And may be with the sanction of people very high up in that particular agency or the administration. My understanding, and I'll have to defer to Jerry on this, is that the Department of Justice does not interpret, at least the theft of government property laws as applying to journalists as it would apply to government officials who convert to expose information. I don't think that when reporters go about their business they are aiding and abetting the commission of crimes. Even in that context they are trying to get at the truth and that's why I think that the Justice Department has historically been loathe to prosecute journalists who are performing their job, in recognition of the constitutional role that they play.

Steve Garfinkel

Jerry, did you want to comment.

Jerry Schroeder

Why not, I've already alienated the Congress, the media, and the defense industry. Are there any other groups represented here that I don't know about?

I really can't speak to the question of theft of government property. But I think that the Samuel Loring Morison case in the fourth circuit definitely, if it proved anything, showed that the espionage statutes are not restricted to classic espionage such as a mole providing information in an unauthorized manner to a hostile foreign power. Morison was a naval employee, as I recall, who provided information to Janes Weekly. And there was some dispute over his motivation, but the Washington Post and list of media organizations that fills an entire page filed amicus or friends of the court briefs when that case was appealed. So it is, or at least has been in the past, and I must say I don't

work in the criminal division, so I leave it up to you if you want to believe what I say, but I speak only for myself. It's my opinion that the espionage statutes clearly, after Morison, apply to leakers which would then raise the question of aiding and abetting that was just raised here in the front. There is also a question, and I think it's an open question and I want to say in fairness, that there are very significant policy and legal and first amendment issues surrounding this question and I wouldn't ever attempt to answer it. But the obvious question is, is this applicable to the news media. That is a very, very sensitive question and as I say, there are a lot of equities inherent to that that the Justice Department has never, and Jim you stated it correctly, at least in my knowledge has never prosecuted a member of the media. Certainly under the espionage statutes and I'm not aware of any under 641 which is the theft of government property either. But, interesting question. Leaking is a crime. Rarely prosecuted, because we can never find out who did it and that topic could fill a seminar all on its own.

Steve Garfinkel

We had one other question.

Question

Jim, your mission stated here today is to publish. I'd like to pose two questions, sir. How do you make balanced, fair, judgments, and what qualifications do you bring to that task?

James Rowley

Journalism is a craft that one learns over time. I think that knowing what news is and reporting on it accurately and writing it in a lucid, lively manner that will interest people are basically the three major elements of it. It's not a esoteric kind of science. You don't need to really study journalism. It takes more knowledge of history, politics, economics, sociology, or even specific subject matters on which you are reporting. I think that I know news when I see it and if a story doesn't write itself it's probably not a story. That's sort of the old adage in the newsroom. If you're having trouble in writing the story think twice about whether you really need to tell it because people are probably not going to be that interested in it.

Question

Jim, you commented earlier that the media somehow proved its trustworthiness during the Vietnam War. Did you have any specific cases in mind as to how the media did that?

James Rowley

I don't have any specific examples of that. But in my general reading of the performance and from the debate that has recently broken out on this issue, it wasn't, from first hand accounts of reporters who were there, the issue wasn't so much of the performance of the media on the field, the actual war correspondents that reported battle field events, as much as the hostile editorial tone that editorial pages took toward the war. I think in this country the press has taken a beating for its coverage of the war because it was so negative. I think that one of the things that resulted from the perception that the press helped lose the war is that we're now being punished for that. We're being kept out. We were kept out of Grenada, we were kept out of Desert Storm. I don't think that the news media lost the war. I think that there were a lot of factors which contributed to our unsuccessful efforts in Vietnam. The coverage of it was merely a reflection of what was going on. Not something that caused the defeat.

Question

Is someone going to put forth a proposition that the absence of the media in Desert Storm resulted in our winning it?

James Rowley

I'm quick to respond the ease with which we won the war just shows how ridiculous it was that reporters were kept out. It just didn't seem necessary.

Comment

This is not so much a question as a comment. I'm from the United Kingdom and obviously we are very unfortunate in the United Kingdom and you here in the United States are fortunate in that you have a press that is dedicated to such heart warming things as the public's right to know and the press' duty to reveal. You see in UK our press and media generally is driven by awful crass motives like selling more newspapers, and building a reputation as a journalist. So I wish you well. I only wish we had people like you in the business in my country.

James Rowley

I can't let that go without some attempt at response. But I wish I could cash in commercially on stories the way you portray. The job of a journalist does not necessarily entail or does not result in large magnificent financial rewards. It may be that newspapers thrive commercially because they have a staff of talented reporters, but I think the commercial success of new organizations is largely irrelevant to the news value of its contents.

Steve Garfinkel

I would like to just add one little antidotal thing to that comment because I think it's worthwhile for all of us to think about as well. I've been interviewed on a couple of occasions by reporters from the UK who were on fellowships of some sort or another to a news organization in the United States. In both cases, following their interviews we got into personal items. They both expressed their regret over the fact that they were returning to another country, another democratic country, where doing their job was so much more difficult and providing the news was so much less available because here they had actually gotten used to the fact that they could get to any level of government or any level of industry or elsewhere and there the rules were so different. And they ended by saying that they only wished that the rules were the same where they were going back. Interesting comment.

Ernie, Congressman John Conyers, Chairman of the House Government Operations Committee, recently stated that pre-publication review provisions are a blatant infringement on the first amendment rights of current and former government employees and contractors. These pre-publication review provisions usually appear in non-disclosure agreements that pertain to intelligence information. They create a life-time obligation on the signer to clear books, articles, speeches, and the like through agency reviewers called censors by Mr. Conyers and other critics of this practice. Over one million Americans including possibly every member of this panel have signed agreements that contain these provisions. Are pre-publication review provisions really necessary for the intelligence community to protect its legitimate interests? Do they not create an extraordinary opportunity for an agency to censor its critics, to eliminate embarrassing disclosures, and to stifle the debate that is necessary to an informed citizenry? From your personal point of view, how have these provisions affected your freedom of speech as a practicing attorney no longer associated with the government?

Ernie Mayerfeld

Well, with all due respect to Chairman Conyers he's just wrong. The Supreme Court which is supposed to rule on issues of constitutional significance, the Bill of Rights, and the first amendment, disposed of the first amendment question in relation to pre-publication review in a footnote in the Snep case. Most of you will remember what the Snep case was about. Snep was a former CIA employee who duly having signed a non-disclosure agreement with a pre-publication clause, decided that he wanted to write a book and was not going to submit it to pre-publication review. He proceeded to do that. He surreptitiously dealt with his publishers and so forth. He kept assuring the Director, who knew he was writing this book, that he would submit it and the next thing that was known, it appeared on the stands and briefly he had some success as a best seller. We then proceeded to go to court to enforce Snep's agreement including the pre-publication review provision. We sought two remedies. One, we wanted to take the money that Snep made in that book because we felt that he had violated a judiciary obligation by signing that pre-publication review provision, rather than by signing a non-disclosure agreement. And the second thing, we sought an injunction to prevent his doing it again. Snep, well represented by the ACLU, argued very vigorously that his first amendment rights were being violated. Now as I said, the Supreme Court dismissed it very quickly citing lots of other cases and well established law which says in effect that the government may impose reasonable restrictions on its employees to prevent their speaking which otherwise this person, as a citizen had, and the government may do this only if there is a substantial government interest that needs to be protected. So in other words, two tests must be met. One, is there a substantial government interest to be protected. Well, what is a substantial government interest in this case which is to protect the disclosure of classified information? Now I don't think that anybody will quarrel with a notion that the government has a vital interest in this. The second test that needs to be met is that those measures must be reasonable. Well indeed the courts ruled that such measures are reasonable because although Chairman Conyers says it gives the right of the government to censor, what is it that the government may censor? What is it that

the government may deny permission to publish? It is only classified information, not anything else.

I think you all know that the rules about classification are very stringent. The executive order sets forth in great detail what may be classified. But more to the point, the executive order quite specifically says that you may not classify in order to conceal violations of law, inefficiency, administrative error, or to protect embarrassment to individuals or an agency. Now it is that kind of thing where I will not quarrel with Jim that the press has a right, indeed a duty to publish, to expose wrongdoing of such nature, violations of law, inefficiency, administrative error, or embarrassment to an agency or an individual. But you can't classify for such reasons. Classified information is classified information. And as you all know, it is the agency that classifies, or the individual that classifies is not the final arbiter. The court reviews classification decisions and there have been hundreds of such instances in which classification decisions were reviewed by the court. And in every case the agency was obliged to jump through hoops in order to demonstrate to the satisfaction of a judge that the material is classified. So therefore, are we restricting first amendment rights when the only thing that the government can do in this pre-publication review process is to deny permission to publish classified material? Any citizen, any former employee subject to pre-publication review provisions and non-disclosure agreement may still criticize, he may still disagree, he may still whatever, as long as he does not disclose classified material.

Now the other question, Steve, that you asked. Why pre-publication review? Is there another more pleasant way to protect classified information in the heads of employees or former employees? I wouldn't know what it is. It has been frequently argued that disclosure of classified information is against the law so, therefore, why not apply sanctions after the information has been disclosed. What good does that do you? What satisfaction do we have by sending someone to jail when the damaging information is out there. So yes, the answer is that it is a necessary and reasonable device. Final question. Has it inhibited me in any way since I left the government having signed several of such agreements? The answer is no, not in the least. I'm speaking now.

Steve Garfinkel

Did you have your response reviewed by your former agency?

Ernest Mayerfeld

Very good question because the issue of oral extemporaneous statements, how can you have those reviewed? On the other hand, Steve, as you know, I knew what question you were going to ask me. You sent it to me. Therefore, I did think about it and therefore, I did make a few notes to myself as to what I was going to say. And the answer to your question, Yes, I did submit those to the CIA and the CIA came back and said, "Go with God."

Steve Garfinkel

And, of course, if the CIA had come back and classified some of them, you couldn't tell us anyway.

Gerald Schroeder

Ernie, I've signed an agreement very similar to yours and I didn't have it reviewed. Does this mean you get to keep the money for appearing on this panel and I have to turn mine over?

Ernest Mayerfeld

You're right Jerry. That's it. See you in court.

Steve Garfinkel

Do any of our other panel members have a comment? Deborah.

Deborah Varljens

I'd only like to say that I think that part of your argument is based on the law says so, so therefore no embarrassing or otherwise information we want concealed will get classified. I think that is a somewhat dangerous position and one which Congress doesn't take. But most of my arguments on that are in my answer to my question from you, so I'm going to wait.

Steve Garfinkel

To Deborah Varljens. A disgruntled employee blows the whistle on his agency by providing copies of classified documents to his congressman. Because the employee did not receive permission to make the disclosure, the executive branch would treat this disclosure as unauthorized and may seek sanctions against the employee. On the other hand, several prominent members of Congress have declared that each and every member of Congress, by virtue of his or her constitutional

position is inherently trustworthy and has a "need to know in order to perform his or her legislative or oversight functions." In their view, therefore, such a disclosure is always authorized. Which of these positions is correct from both a legal and policy perspective? How is it possible to manage an information security program if 535 individuals, each with a different political and policy agenda and each sheltered by the constitution's speech and debate clause have unrestrainable access to all classified information? And finally, are there and should there be any sanctions available to discipline members of Congress who disclose classified information?

Deborah Varljens

Restrictions on whistle blowers right to petition Congress infringe on Congress' access to information regarding the operation and policies of the executive branch. Such infringements are contrary to the principles on which our government is based. Our government is dependent on the separation of powers between the executive, the legislative, and the judicial branches to provide the checks and balances essential to accountability in bureaucracy. The danger where Congress is denied access to information, is that the controversial information will be suppressed and disclosures critical to prevent deception and dishonesty in public debate and in lawmaking will never see the light of day. I'm going to give you a little bit of the legal basis that preserves the civil servant's right to talk to Congress. And they are numerous. I have to quote from a Government report because I think it's probably a pretty drastic opinion, but, according to the 1982 Government Operations Committee Report, the Constitution does not assign power over foreign policy and national security to the President, but rather creates a system of shared responsibility between Congress and the President for those matters. The report points to the many powers of the Congress that deal with national security in Article One. For example, providing for a common defense. And the Congress' sole authority to appropriate, even in the national security area.

There is a very interesting history in the report which indicates that the framers of the Constitution were very aware that giving the power of the purse to Congress created a check on the executive branch, particularly in the national security area. And they intended that it was so. Article One also grants any individual the right to petition Congress. It does not say "unless you are a disgruntled civil servant." And, of course, the first amendment's free speech rights. Statutory protections of the free flow of information to Congress were enacted as early as 1912. The law states, the rights of persons employed in the civil service to petition or any member thereof shall not be interfered with. At the time of passage one supporter declared, "how can a conscientious member of Congress vote intelligently and for the best interests of the American people if the most reliable sources of information are closed to him." A little more recently, 35 years ago, the then Senator Nixon framed the issue quite well in a floor debate when introducing legislation to make it a violation of law to discipline a government employee for testifying before Congress. There is too much at stake to permit foreign policy and military strategy to be established on the basis of half truths and suppression of testimony. Unless the employees of the government right to petition Congress are protected, Congressional hearings will amount to no more than a parade of "yes" men for administration's policies as they exist.

The most recent enactment, the Whistle Blower Protection Act, protects public disclosure of information which an employee believes is evidence of violation or waste, fraud, and abuse. Protected disclosures are to be reported to the agency's inspector general, the Office of Special Counsel, or the Merit System Protection Board. But, 5 USC Section 1202 clarifies that nothing in the Whistle Blower Protection Act is to be construed to authorize the taking of any personal action against employees who disclose information to Congress. Lastly, the Code of Ethics specifically requires the exposure of corruption at 5 USC 301. The law protects the employees right to petition Congress and examples abound of the benefits to the public good derived from these laws. The public would not know of cracks in the reactor base at Waterford Nuclear Plant disclosed by Ben Hayes. The public would never know of the serious breaches of security at nuclear weapon sites throughout the nation. The public would never know that there were pressures within the inspectors office at Comanche Peak Power Plant to whitewash findings of harassment by officials for inspectors reports of safety violations. The public would not know of the cover up of the radioactive waste fill at Wright-Patterson Air Force Base in Ohio. Nor would the public know of the 50 safety violations at Handford Nuclear Weapons Production Facility which seriously threatened workers

lives. Casey Rhoades disclosures eventually lead to the plant's shut down.

Administration's testimony at Congressional hearings on the issue of non-disclosure agreements do not reveal the supposed harm done by the disclosure of civil servants and contractor employees. I presume that's because the information itself is classified. The trend since the 1982 Executive Order 12356 toward increasing classification of information makes Congress even more open to the concerns of the informed civil servant. Prior to the Executive Order 12356, previous executive orders had established a trend toward limiting, or at least specifically defining the classification materials and surrounding procedures. The 1982 executive order reversed that trend by, among other things, increasing the amount of information that was subject to classification, weakening the minimum standard for determining whether information qualified for classification by dropping the requirement that damage to national security be identifiable and by dropping the balancing test that required classifiers to consider the public interest in disclosure vs the need to protect the information. In short, executive order 12356 took dramatic steps to decrease the flow of information to Congress. In addition, by-products of the executive order such as SF 189 in pre-publication review agreements also make Congress uncomfortable. Increasing classification to the point of over-classification of information reduces public and Congressional confidence in the validity of the classification system by jeopardizing the respect necessary to protect information that truly warrants classification. Over-classification has prompted prominent members of Congress to exclaim, and I quote from Chairman Brooks, "Most of the classification, in my judgment, is not to keep our enemies from finding out the information. It is to keep the American people and the Congress from finding out what in God's world the various agencies are doing." The more classified information unavailable, the increased reliance of Congress on the informed observation of the conscientious civil servant. The administration contends that Congressional access is pre-conditioned on a need to know. The need to know requires the administration to determine if Congress has the need. It would be literally impossible to carry out oversight responsibilities of the executive branch if those agencies could determine what Congress can and cannot have access to. I will grant you that there may have been Congressional indiscretions with national security information. But I also venture to say that there have been many more instances of classification of information that meets the prohibitions of Section 1.6A that is classified because it conceals waste, fraud, or abuse, or embarrasses. Frankly, to Congress, it is probably not worth dealing with unless it conceals information critical to public debate or embarrasses the administration when Congress is doing precisely what is mandated. That is when the system of checks and balances is functioning at its best. If there are Congressional indiscretions, the indiscretions need to be fixed. But the right of the employee to petition Congress cannot be infringed upon without endangering that system of checks and balances essential to our government.

Steve Garfinkel

Any of the other panel members want to comment? Jerry or Ernie?

Ernest Mayerfeld

Well, Deborah, you talk about checks and balances, now. There are three branches of government and I did mention the heavy involvement of the judiciary in this process. For the Congress to say that the executive branch over-classifies, we could debate this back and forth between us endlessly. But in a specific instance, every citizen, including his or her congressman, has the right to go to court and have that classification decision reviewed. So where is the problem? If we believe in checks and balances in a constitutional system and the judiciary has the final say so on these matters, is that not a good thing? In 1975 the Congress amended the Freedom of Information Act (FOIA) because up until that point the Supreme Court in the famous Mink case said that if there's a secret stamp on a piece of paper that's the end of the inquiry and it remains classified. Congress didn't like that and although a lot of my former colleagues may eat me for saying this, when the FOIA was amended and thereby authorized the judiciary to, in effect, second guess classification decisions, I think it achieved a very salutary result. Consequently, the threat of judicial review will inhibit any bureaucrat from over-classifying or classifying in violation of the executive order by putting a secret stamp on something that reveals inefficiency, violation of law, or embarrassment.

Steve Garfinkel

Jerry, did you want to comment, or Deborah did you want to respond?

Gerald Schroeder

Well, I was essentially going to make several of the points that Ernie just made. There is a constitutional principle made as separation of powers, Deborah, but if Congress has them all and the executive branch has none, that's not separation. There are things such as executive privilege. The whole idea that the whistle blowers statute which, as you noted, does contain an exception for national security information classified under an executive order, and I assume, but don't know, that the Congress knew what it was doing, doesn't create a situation where there can be this parade of government workers down Pennsylvania Avenue delivering box car loads of classified information to the Hill. Clearly, the points you make are well taken. Congress does have a role to play, very definitely and it can't play that role, just like the public can't play its role without information. But I think we have to be reasonable here, on both sides. You can't classify everything and give it to no one, but to suggest that any piece of classified information can be provided to 535 members of Congress, willy nilly, in violation in my view of the law, I just don't buy it. I think the answer is somewhere in between, certainly, and I enjoy the give and take, but I'm sorry, your answer is too one sided.

Deborah Varljens

Can I just say that I don't know of every instance in which classified information has been brought to Congress. But there is a system. It's not willy nilly by any means. The classified information should be brought to the committees of jurisdiction. I am the counsel for the Civil Service Subcommittee. Our jurisdiction covers the personnel aspects of the civil servant. I choose not to deal with the classified information. Actually, I haven't had the opportunity to, but I would chose not to deal with it. I would chose to funnel it to the committee that is supposed to deal with it. And in that way the people that have classified or that have security clearances can deal with it. I grant you that 535 members should not be able to just get information willy nilly. I completely agree with that, but using the system as developed, Congress has to be able to get to the information that they need and the committee system should guarantee that. The only other comment I wanted to make was that sections differ on the courts deference here. According to Congress, in Egan the courts said that they will defer to the executive branch. Now I think that's pretty significant that they have, in writing, have said that they would defer to the executive branch in these matters. So to me that creates the increased need to make sure that Congress has the information that it needs.

Jim Rowley

I just want to respond to one thing that Ernie said earlier about the executive order prohibiting classification of materials solely to hide wrong doing, criminality, or inefficiency. I'm not much comforted by that provision of the executive order in that since there are so many things that are secret, who's to know whether or not there's a body of knowledge out there that's being protected for base motives that could even be brought to a court's attention for judicial review much less whether or not you survive the deference test if you got into court. You might not even know it exists. I think that a good example of this is in the Iran Contra context where the FBI was asked to hold off for awhile on a criminal investigation of the Southern Arab Transport crash on the basis of national security. It seems quite clear that this was done because the people involved in Iran Contra wanted to protect their operation from exposure to law enforcement, not because of any particular devotion to protecting national secrets.

Steve Garfinkel

I'd like to thank everyone for participating and listening so well. Thank you very much. ■

SECURITY FOR THE 1990'S

25 June 1991

John F. (Jack) Donnelly
Director, Defense Investigative Service

I have been in the security countermeasures business for 40 years, and the last few years along with the next 5 to 10 will prove to be the most interesting and perhaps the most challenging. Things that are going on now very few of us thought were even possible three years ago. We have the new East-West Alignment. We have the metamorphosis of the Eastern Bloc countries and a unified Germany with Berlin once again its capital. The Warsaw Pact has been disbanded. The Eastern European countries are moving toward western thinking industrially, politically, and economically. We've seen the Soviet economy collapse, and is that good or bad? I personally think that the disruption can be dangerous. Will the Soviets be able to move from a socialist economy to a market economy? It's too early to tell. They're having trouble. Will there be independent soviet republics linked together through a loose federation? We'll have to wait and see.

Times are really changing and they are having an effect already. The impact on defense is going to be significant. We will definitely be taking very serious cuts in our force structure. These cuts are going to reach every part of the Department of Defense, the Military Services, and all Defense Agencies. If the military services and defense agencies are going to take cuts, obviously the industrial structure that supports us will also be subjected to cuts. We expect to see prime contractors doing much more work in-house as opposed to contracting out. In real terms, the FY96 defense budget is projected to be 22 1/2% less than the defense budget for FY90. At the end of FY95, the Army will have 29% fewer divisions, the Navy will have 17% fewer ships and the Air Force 28% fewer tactical airwings. These cuts are going to hit a lot of people, every region of the country and a lot of companies.

There are a lot of challenges out there that we are going to have to meet with less resources. The following are some of the effects of these changes: Defense is definitely going to be dedicated to maintaining the technology industrial base that we have. Research and development in industry is mostly paid for by contract or it's reimbursable independent R&D. I expect that we will see the R&D budgets increase as the procurement budgets decrease. We are a reflection on the commitment that DoD is making, based on the superiority of our weapons systems as demonstrated throughout the recent Desert Storm conflict. We are going to see a shift in the emphasis of where we put our dollars, from the battlefield to international economic competition. The company that has the technological and scientific base and the marketing skills, is going to be the company that wins the war with its competitors.

The old enemies were easy and we knew who they were. The new competitors are not so visible and they're everywhere. There is going to be a lack of enthusiasm for strict regulations governing security when the people see us granting "most favored nation status" to the USSR and PRC. Motivating the personnel that work in our offices and companies is going to be more difficult, it may have some international repercussions; you can't very well tell our people, "watch out when you go to Paris, it's full of spies." The bottom line is, we really are going to have some significant challenges that are different in the 1990's.

There are a number of political decisions that are ongoing, that will intensify the changes and the need for us to change, in the future. We have the INF treaty which brought Russian inspectors into our plants and onto our bases, and a portal of permanent Russians in Magna, Utah. The conventional forces Europe Treaty is about 98% ready to be signed. When it is, we will start destroying tanks rather then buying them. We will also be

destroying artillery pieces and armored personnel carriers; and so will the other side. START has been signed and both countries definitely want it. It's going to come. Fortunately, there will be only one portal although there will be many more soviet inspectors and many more visits to industry.

The west will be propping up the eastern European and Soviet economies. The Group of Industrial Nations are meeting with the Russians in London trying to determine ways that we can help them, knowing full well that they don't have the hard money to pay. Russia has been offered an associated membership in the International Monetary Fund, the first one offered to any nation. Because we know that we want democracy to take over in Russia and Eastern Europe, we are going to have to help them.

Increased immigration from the USSR and Eastern Europe is coming, but not all the visitors that arrive will be spies. We are going to have to determine who is it that is after our technology and who is it that is after our classified capabilities. Are they really from the old countries that we have looked at as enemies or are they from our best friends? What is the overall effect of this for U.S. industry? I think that we are about to enter a decade of "globalization." It is becoming increasingly true that if a company can't succeed overseas then it is going to have a difficult time succeeding here in the U.S. Foreign Military sales will increase. You can imagine, after watching the Desert Storm conflict on television, how many countries want to buy our weapons as opposed to weapons from other nations, and for good reasons. This is good because it leads to interoperability of weapons systems, and when we have to fight a coalition war as in Desert Storm, we can interface with weapon systems of other countries. By sharing in the production of these weapons systems our allies can share in the costs of the weapons and it also gives us an opportunity to share in the technology being developed by the foreign countries. I used to think that we were the only country that had leading technology. Well, that's not true. All of this globalization and all of the other changes that I have mentioned are going to cause us to change, and some of the changes you will see pretty soon.

The criteria country list or the designated country list that we all are familiar with will have to be changed. The counterintelligence community has already come up with a way to change it. The new proposed list will be called the National Security Threat List. It will have two parts. The first will amount to what the criteria country list was in the past only it will be shorter. Some of the countries that were listed will no longer appear. There will be a second part that will be dynamic and fluid in nature based upon a country's activities considered inimical to U.S. interests. The big challenge to us in government is how to get this real time classified threat information to you in a timely and continuing basis. The national counterintelligence community and we are developing ways to do this. DIS is in the process of developing industrial security awareness councils in the regions. We have about a dozen set up now and we intend to put on a full court press and establish them all over the country. The FBI has established a national DECA coordinator with DECA representatives in every one of their districts. They all came to our headquarters when we had our last industrial security meeting and interfaced with our regional directors of industrial security. We intend to include the FSOs from the areas in the regions where we set up these councils so that we can be talking on a continuing basis, with representatives of industry. We can get the word out to you and we have to get it out to you. It is going to be a challenge.

The next major change is going to be the National Industrial Security Program (NISP). I participate in the NISP steering group and I am amazed at how far and how fast the process is moving.

The NISP will set uniform standards for security in industry. One level, the base level, will be standards for handling classified information up to and including Top Secret. Supplemental levels will be more intensive and used for handling special programs, SCI and energy programs. There will be a single scope background investigation where every agency uses the same form. Inspections and investigations will be reciprocal to the extent possible. The President will establish the NISP in an Executive Order. We believe that this will lead to significant cost-avoidance and bring greater effectiveness to the way we do business in the 90s.

I do not want to shock anybody, but the truth is that we can't protect everything. Besides, our free society won't stand for it. We do have laws and regulations controlling the export of certain technologies. We can do a much better job of protecting our technologies than we have in the past.

But, I don't think that we will ever be able to protect it all. We certainly have to put much more emphasis in deciding what really needs protection. We just have to have more and better classification managers so that when we give classification guidance to industry, it is logical and intelligently conceived, doable and achievable. I think that those of you who are classification managers in the government and in industry have the ability to meet these challenges, and we are going to work with you to make it work. That brings us to what you are really waiting for - the Cogswell Awards Ceremony.

This is our first time giving the James S. Cogswell Awards for Outstanding Industrial Security Achievement at NCMS, and I am pleased to see the reception that we are getting here. Colonel Cogswell was the first director of unified industrial security for the federal government back in 1965. He had a short tenure and died rather suddenly. But he was around to oversee the development of the concept of a partnership between government and industry, and the establishment of a program honoring excellence in industrial security achievement. How do we decide who gets a Cogswell Award? The first criteria is that senior management has to support the program. Without that, there will be no really good, viable program. All of the people in the company who will have access to classified information have to be educated and know how to protect classified information and support the program. The FSO and the managers of the company have to cooperate with the DIS special agents when they are conducting personnel security investigations at the company and we consider the overall professionalism of the FSO. How do we actually make these selections? The selection is made first of all by a nomination of the Industrial Security Representative. This has to be endorsed by his/her Field Office Chief. Then it goes to the region where it is endorsed by the Director of Investigations who knows how the agents are being treated when the agents go to the companies in connection with personnel security investigations. Then it is endorsed by the Director of Industrial Security for the region and the Regional Director. Then it comes to Washington, where we coordinate with the military departments and defense agencies doing business with the companies that have been nominated to see if the customer is really satisfied. We also coordinate with auditing agencies of government and the investigative agencies. It is an exhausting process. Those that have lasted to the end and who are going to be honored here today, really deserve the award and I want to congratulate all of you, and all of your personnel for having an outstanding industrial security program. It is quite an achievement.■

Editor's note: *See awards section for companies who received the Cogswell Award.*

INDUSTRY PERSPECTIVE

25 June 1991

Lawrence J. Howe

Our topic this afternoon is challenges. I've talked about identifying three challenges. Now if you're going to narrow all the challenges that we have down to three it might imply some kind of special inside knowledge or track, and I'll deny either because it is simply one man's musings about some of the things that are ahead.

The first challenge that I'm going to talk about is one that I'm going to spend a little more time on. It has to do with the dilemma that we're no longer in a binary world. Yesterday, Admiral Inman spoke very eloquently to the fact that we are very much in a changed situation. Right now, we are lacking the relative luxury of a world ordered by conflict. That is, things aren't black and white any longer. In the emerging state of world affairs, the appropriateness of clean clear distinctions for those of you who deal with computers all day long, or trying to reduce things to ones and zeros, just don't seem to apply anymore.

Those of you who may be like me and are fans of John le Carre' and some of his novels may recognize a paraphrase of a quote that comes from his most recent book, The Secret Pilgrim. As you know, George Smiley is his spokesperson and in the book Smiley comes down to the school for the service. There is a class of new intelligence officers there and Smiley is addressing them after dinner. In his comments he notes that "the absence of conflict over ideology may have made the world a more dangerous place." Now I think that one of the things that George Smiley was getting at was the way things were, nobody here wants to go back to them, but at least the way things were, we had an idea of where the lines were drawn. We could anticipate, with some degree of accuracy, at least so we thought, what direction we might anticipate hostile acts to come from.

Well, where are we now? The battleground has shifted away from military confrontation aspects and deterrent to a playing field of economics where world market shares are deciding who's on top. In all probability the playing cards that are going to be significant to have in your hand are going to be ones dealing with high technology.

Stepping back from the brink of thermonuclear confrontation and getting a perspective on the economic contest that we've actually been in for some time, many people feel that we've been overly preoccupied with the military and have not paid enough attention to our relative position in the world economically.

There is a more cynical version of this point of view that suggests that while we were all poised to face a military threat, some of our friends may have been taking advantage of the opportunity to stand by our side to pick our pockets. We're still very much in the sorting out process. The redefinition of the threat is having to take into consideration that many of the world's so-called free market economies actually have a very heavy level of government involvement. First of all, there are heavy levels of government involvement in coordinating industrial activity and providing focus. Next there is a high degree in many of these countries of government subsidization and capitalization providing seed money and deciding on what programs shall go forward and which ones shall not. We believe, and we have strong reason to believe, that in many of these countries there is very strong support from the government intelligence resources to support the industrial base. These are not just features of Communist or Soviet style governments, but exist in many places in the world.

As many countries attempt to make the rapid transaction through what Walter Rostow calls the five stages of economic growth, what's happened on the Pacific rim is interesting to observe and think about. Many of these countries have become the model for emerging nations to decide how they themselves are going to enter into the

race for relative economic position in the world. Most recently, PBS had an interesting series on the mini dragon. It talked about Korea, Taiwan, and Singapore. Each of these countries had an interesting commonality. In each one there is a very strong level of government involvement in what was otherwise termed as a capitalist free market economy. This was combined with a coupling of concentration of economic and industrial power in major domestic economic trading blocks. So between the resources available to a government and very large economic trading blocks in many of these countries, it provides a concentration of resources both economically and politically that are going to be something to which we are all going to have to contend with. Now what does this mean to us?

Very simply put, if research and development, front end cost and lead time can be significantly reduced by putting a smaller investment of resources in stealing the technology and development, then friend, I suggest to you that this becomes a relatively simple business decision. It is no longer a question of hostile international relations. This is even more so because the distinction between what is a hostile act between countries is even all the more blurred because in today's world, as most of you recognize, the ownership of business and economic resources is no longer confined to national borders. So the decision to spy on a particular company or international industrial organization is not really seen as a particular act against a given country.

Now, clearly in a world that is ordered by military deterrent there at least is lip service given to the moral imperative involved. Somehow, when you get into business confrontation and competition, no one even bothers to pay lip service to the discussion of what the moral imperative is.

Industrial espionage has always existed. Unfortunately, most U.S. businesses are neither prepared or adequately equipped to be protected against a well organized, orchestrated and financed intelligence effort, particularly if that effort is coordinated by the intelligence service of a given country. Surely in this country the idea of doing so called marketing research against the competitor has gone on a long time. I want to suggest to you that what goes on in this country in terms of so called market research is child's play compared to what you are up against when you're dealing with a disciplined, organized, and knowledgeable intelligence organization.

I think there's another factor we have to look at here and it's an institutional one. As the military confrontation has subsided, the intelligence organizations in most countries are looking for new ways to justify their existence. The idea of going to the national leadership and suggesting that there is a way to help the national industrial base improve their competitive position makes a very important and, I think, powerful marketing ploy for an intelligence service to use who doesn't want to see his resources cut. All of this goes by way of suggesting, I think, that it is quite clear that what we are facing in the years ahead is a very definite challenge and threat to our economic position posed by friends and foes alike who will be using their national intelligence resources against us.

Somebody said that to be in this business we are "paid paranoids" and I guess that statement probably illustrates the point. But I think, to do our planning on any other assumption would be absolutely foolhardy. In some respects our military defense oriented security programs, in my judgment, do not prepare us well for this challenge. For one, most companies with a mix of defense oriented and purely commercial business have found it necessary to have two divergent approaches to industrial security. The procedural or government ordered compliance security places an extremely heavy burden on industry. As a result, the companies traditionally have very little resources left, or enthusiasm for any other security program. In most companies the protection of proprietary information is modest at best.

Also, regrettably, there is a perception of government security being an impediment to production. This particular model does not encourage it being broadly accepted or adopted by industry.

It is my opinion, as we move forward to recognizing the need to protect trade secrets in the national interest, we need to understand very clearly the pitfalls of avoiding procedurally intensive approaches. First of all, the simple fact is that one way or another I don't think that American business is likely to stand for it. If there was an attempt to impose it, I suspect that we would have a revolt on our hands. Even if you were successful in getting some sort of legislation to somehow impose it, I think in reality any such program that was procedurally intensive would be largely ignored by industry and that you would have a subrosa subculture by which companies attempted to get

their work done in spite of what you were imposing.

More to the point, if we are going to be participants in this process, we have to be critical. What I'm going to suggest to you is that we have a security posture that supports efficient production rather than concentrating on instituting more barriers. As an aside, there is, in my view, a direct correspondence between an effective personnel security program and a vigorous security awareness program and a potential to avoid an over reliance on physical security barriers and an extremely intensive procedurally intensive information security program. What I am suggesting is the significant challenge for those of us involved in classification management is to decide whether or not we are going to be part of the solution or part of the problem. You say all right wise guy, what's this part of the problem stuff? Well, I'll be very frank with you and tell you what one of my fears is.

As military spending goes down I think there is a natural tendency for job security to set in. More than a few of us these days are worrying about justifying our existence. In my personal judgment, the worst thing we could do for the national welfare, and I suggest, our own credibility, is attempt to superimpose a close look-alike variant of the Defense Industrial Security Program on trade and proprietary secrets. Should we be players in the process of broad information security? Absolutely! I strongly urge that we add some fresh thinking and studiously avoid the procedurally intensive approaches that will do nothing but brand us as bureaucrats and exclude us from the process. We might as well confess that most of us are probably in a mold. As much as we rant and rave about it, we have become very accustomed to working in the safeguarding of classified information environment. We are probably more tightly locked in the paradigm based on the experience we had with the DISP than we actually realize. I am going to suggest to you an assessment to illustrate this point.

Someone suggested that there are some flaws in how we form safeguarding policy. There is a view that risk and threat analysis may all too often be based on the notion that if a particular avenue of breaching security is theoretically possible it therefore is. All I have to do is mention the word TEMPEST and the rest of you could give the rest of the speech.

This approach in and of itself disregards important corollary questions. What is the likelihood of this threat occurring? What is the value of the information being protected or the projected consequence of its loss? And on balance, do the proposed safeguarding measures make sense? We need to determine under these circumstances what constitutes an acceptable level of risk. I think that this is an approach that we are going to have to take to justify what we are doing. Regrettably, most of our threat analysis comes from some segments who have become highly specialized. They will elevate the theoretical and, because they are concentrating in this one narrow field, project it with a vehemence. Unfortunately, there doesn't seem to be a counterbalancing weight out there saying "Yes, we understand what you're saying, but now before we go ahead and institute this as policy let's go back and ask the questions again--relative probability of occurrence and are the measures justified by the consequences of loss?"

Does all the experience that we have collectively gained in protecting the national secrets have something to offer on the issue of protection of trade secrets and critical technology? Of course it does. I think we must be players. But I think the dumbest thing that we could promote would be to consider commercial proprietary information only some subset of classified information. Is that really likely? Well, we have had various forays into looking at the unclassified national security related information. That has ended up being a big bugaboo. I suggest to you that that's the foot in the door. If that goes too far, we will find ourselves hook, line, and sinker trying to legislate from government how proprietary information is going to be handled.

I feel that we have to reorient ourselves as we begin to come to grips with some of these issues. Will we ourselves and some of our organizations have to change? I suspect so. I think there is a risk in our not changing and trying to get out of some of our old paradigms. I think you might suggest that the question of the hour is whether it is necessary for either individuals or organizations to march steadily forward to a state of increased irrelevance so they can be disregarded and disposed of and replaced with somebody who has a fresh point of view.

Change is one of the most difficult conditions to constructively manage. That's why so many public institutions and institutions in the private

sector seem to just muddle along till they fall of their own weight. The challenge I'm placing before all of us, and I'm looking at myself in the mirror as I say this, is to be innovative participants in the structure, first and foremost. We still have important forms of classified information to protect, which will require the establishment of an effective and efficient way to protect important new technical developments. The challenge for us is to be participants and think out an approach to a national information security initiative. I suggest that this needs to come primarily from industry.

We're likely to find it necessary to operate in these two modes simultaneously. The protection of classified information, but adopting a different mode, a less procedurally intensive one, to handle critical unclassified technology. There is an important benefit in seeing to it that a broad spectrum of industry approach is taken. There are many, many corporations that are doing it in the purely private sector who have very effective information security systems. These are particularly the ones who are not involved in the Defense Industrial Security Program because they are not having to run a dichotomous operation. This might be the time when I might try to sneak in an ASIS plug: I'd like to promote a closer liaison between NCMS and ASIS in looking at the broad aspects of the protection of proprietary information. There are a number of very interesting things that are being done in industry that are totally outside of the government security theater field. It seems to me that the techniques, the structure of the discipline represented by classification management in this society, could do an interesting study in comparison with some of these people from other allied fields to find out what is working out there. What is acceptable to industry management? How do they find it efficient to do things and try to put that into a program which is then exportable and which this organization and ASIS could help try and promote on a nationwide basis. I suggest to you the proper initiative for this is not government, but industry helping itself just as this society does and ASIS intends to do. So I offer that as a challenge to our mutual organizations. I'm proud to say that I've been a member of NCMS as long as I've been a member of ASIS.

The remaining time I have to talk, I'd like to mention a few other issues. First of all: Special Access Programs. Yesterday, Admiral Inman reminded us of the importance of compartmentalization for effective security. Effective management has always been the cornerstone of good security. Unfortunately, we are not today, nor have we in the past, exercised a well practiced approach to need to know. This factor alone is probably one of the major reasons for the proliferation of Special Access Programs today. The issue of the hour is not to determine whether or not we ought to have Special Access Programs because clearly special access programs have a very important role in the procurement process. There are many significant programs; some of which benefitted Desert Storm. There was a direct benefit of special access programs. My concern is not whether they should exist. My concern is the need to restore a higher level of credibility to the special access process.

For the sake of discussion, I want to touch on two areas where special access programs may have gotten off track. First of all, when these programs got recognition by being incorporated into an executive order not that long ago, there was a need to establish a structure. The easy out was for special access programs to adopt a security system already in place which provided for top secret compartmentalized information. This quantum leap imposed physical security standards and personnel security procedures which, in some cases, appear to be out of proportion. There is no argument about the need for supplemental standards more demanding than what is afforded for the use of GENSER programs. The problem is taking something off the shelf which looks like it may have been the wrong size.

There is another area of possible negative offshoot of compartamentalization. An advantage of participation in a larger community is that you are afforded the opportunity for periodic sanity checks whether you think you need them or not. Much has been gained in recent years by improved partnership of the Defense Investigative Services (DIS) and industry in the implementation of DISP. Industry has a much improved perspective on the process and, I daresay, some perspective has been gained on the part of the government. The bottom line is the improved interaction between industry and government has resulted in a distinct improvement in overall effectiveness in safeguarding represented in the DISP.

In the special access community the same broader sanity check does not always seem to be in evidence. When those who have them, whoever *they* are, talk about special access programs, the

common characteristics that are often touched on are perceptions of arbitrariness, lack of consistency, and general overkill. The need to have flexibility to tailor security measures based on actual need is valid and they need to be part of special access programs. What I want to suggest to you is that the gray line into arbitrariness is a very easy one to cross.

The participation of the special access community in meeting with government and industry groups in recent years has taken some very positive steps forward. This is a trend that needs to be further encouraged. A gentleman who is on your panel tomorrow, Tom Adams, is a typical example of the outstanding job done by some people in industry to further this process.

Thinking back to the Vietnam years, you'll recall George Ball's famous analogy that getting on the tiger's back is not as hard as getting off. Now there is an opportunity for the special access community at hand which I sincerely hope that they use to dismount gracefully. I'm talking about the NISP, National Industrial Security Program.

First, I want to say that commonality is not synonymous with unification or consolidation. I'll say more about the NISP again in a moment. But the procedural autonomy of individual programs should in no way suffer from the adaption of more standardization and commonality. Working toward commonality is not synonymous with loss of authority. The restoration of credibility for special access programs, could be helped along by starting with a clean sheet of paper. It may take some courage to acknowledge that some requirements in the past have not been justified. But I want to suggest that graceful self-imposed readjustment is usually much more painless and usually recognized for courage. Imposed change tends to be less enjoyable. I sincerely hope that some of the signs we are seeing indicate an openness not only to recognize but actively seek larger community sanity checks by the special access program community.

Now, lastly and briefly, you'll be pleased to hear, is one of the most exciting things to come our way yet in a long time, the National Industrial Security Program (NISP). The level of cooperation between industry and government has been nothing short of phenomenal. Does that suggest that there are no problems? Not hardly. Briefly, what are some of the optimistic expectations and what are some of the aspects that might be unrealistic. Starting with the later: NISP will not happen over night; Many of the changes that have been implemented in the NISP are likely to be incremental. Not only will they be incremental, but some of them are likely to be sporadic. Some things will change quickly. It will take a while to work the snags out. Once we get the snags out then we'll make significant progress again.

Ladies and gentlemen I think the watchword for the NISP is optimistic patience. A great many bridges have been built, institutional walls are showing that they've got some gates in them. I want to encourage all of you to get to know as much about the NISP as you possibly can. And try to understand what's going on.

One of my fears is that one of the worst things that can happen is that as more people get involved with the NISP some of them might want to use it as a platform to vent some more frustrations. The NISP is proving itself to be very resilient and one of the reasons that both government and industry have made so much progress is they have adopted a very positive, forward looking, mutually respective approach to the process. In short ladies and gentlemen, those who want to be helpful with the NISP need to understand that when you're asking organizations and institutions to make changes it requires a high degree of diplomacy and tact. I want to respectfully suggest that this will not be an opportunity for employment for those who want to be zealous in this process.

What should we anticipate: The President has laid out a challenge for us. The President, based on the NISP report, expects us to achieve improvements in safeguarding capability and also achieve cost effectiveness. Are we going to see immediate cost savings? I suspect not. One of the reasons is probably incremental implementation of the NISP that I think we can anticipate. The second is, on the part of some government organizations, it is going to require some upfront seed money, some venture capital to combine and consolidate basic data bases. But once that occurs, in the out years, it is inevitable that both industry and government will see the cost savings. So we have to be careful about not over selling the cost savings at the front end.

Now, again, I want to repeat what I said about commonality. It is not synonymous with unification. Individual executive branch agencies have

unique missions. The recognition and the support of these unique missions by industry is absolutely essential. What NISP is trying to accomplish is the identification of commonalities and a mutually supportive structure. NISP is not trying to homogenize and merge all executive branch agencies into one. So far the progress has been very encouraging and I think we're all looking forward to the report of the panel tomorrow to see in what direction we are going.

One of the major advantages we have in coming to a meeting such as this is that we have an opportunity to get together informally. Very frankly, I think a great deal of the positive gets done, also there is a progressive, and creative nature in some of the informal sessions that occur in this type of meeting. All I can hope is that, if I have given you some ideas and that you can get into informal get-togethers and begin to kick them around, I will then have done my part. There is a little adage that comes out of the petroleum exploration field and that says if you haven't hit oil after 30 minutes, stop boring. So with that, thank you ladies and gentlemen. ■

EXPORT CONTROL AND TECHNICAL DATA

26 June 1991

Michael Liikala

I'll give you a quick overview of who we are at the Department of Commerce that regulates technology transfer, then try and go over briefly the ways we handle tech data and license it. That will primarily be included in your handout that we passed out. In close, some remarks about what we're doing in the 90's in terms of regulatory change because there is significant amount of change in store based on what's been happening around the world over the last few years.

Let me begin my remarks that since this is being videotaped this is dated information. The regulations, as I just mentioned, are under fairly significant change because of what's been happening in the Soviet bloc, what's been happening in the Middle East, etc. We expect the most significant changes since World War II in export controls to go into effect sometime around August or September. So I'm speaking today, June 26, and what I'm saying is effective today but it is not going to be very useful come August or September. Some of it will still be in effect, but it's going to require that anyone listening or watching this videotape check again with us in the fall to see where these regulations have changed.

Having said that, let me give you an idea of who we are. The Department of Commerce, in the International Trade Area, has two primary functions. One is to promote and assist US exporters in reaching foreign markets and selling their goods. Those are the good guys, the good side of the operation. We have offices in San Diego, in most major cities around the US, and have commercial attaches in most of the embassies overseas. We're there really to help your companies penetrate those markets, find distributors, participate in trade shows, etc.

The other side of the Department of Commerce that handles international trade is the Bureau of Export Administration. And that's the bad guys to some exporters because we regulate export. We're there to make sure that technology that is exported does not fall into the wrong hands. So we, in a number of instances, require licenses for those technologies or typically require those of you who make high technology items to check with us with regard to the country of destination, and the end use to make sure that it is legitimate to ship there either without a license or with a license, or whether it might be prohibited in any case.

The bureau is headquartered obviously in Washington. We've got about 700 people. We have enforcement operations here in southern California, northern California, and in eight cities around the US where we have people that work very closely with intelligence agencies trying to ferret out diversion schemes, intelligence operations of foreign countries trying to steal US technology. And then we have in the western region an export administration office which I head up, which is here to help exporters understand the regulations and comply with them. Also, we conduct audits of some of our larger exporters to ensure that they are complying with the regulations. We handle the 10 western states, west of Colorado basically, and have offices in northern California, in the Silicon Valley, and one in Portland. We handle right now something like 2500 inquiries a week from companies like yours just to assist you, I'll give you our phone number should you want to follow up with any questions after today. We're headquartered in Orange County at the Orange County Airport. The number there is (714) 660-0014. There is a voice mail system, so you can get a lot of information off the recordings or by pressing people's extension. If you want to get right to a person when you dial that number press 0 it will go live for you and let you talk to real people. So that, in a quick summary, is how the organization fits into the department.

Our mandate is to control dual use technology. We do not control munitions items. So if your products are licensed by the State Department or you are making weapons for the Defense Department, you don't really talk to us. You talk to the State Department or the Defense Department about moving your technology. It's when you get into items that you're selling that have commercial applications that you need to talk to the Department of Commerce. We're finding and I think probably a number of your companies are involved in it, that a lot of companies are now moving to look at commercial markets. Depending on budget, its becoming smaller, our NATO allies in a number of other countries are cutting back on defense expenditures, and a number of defense contractors are moving to look at commercialization of their products. When you do that and you want to export it, you're going to need to talk to us to make sure that no license is required or what the licensing requirements are because you're probably involved with some sensitive technologies and we're going to want to make sure that the end users are legitimate.

Again, we license both commodities and technical data, know-how, and software, and try to do that in actually three basic frameworks. The first which I'm going to talk about a lot in the technical data areas are general licenses. A general license allows you to ship your products without having to get a validated license from the Department of Commerce. In other words you can determine that your product, by looking at the regulations, or by talking to our office, that your product being shipped to the UK would not require a validated license. Then you can go ahead and ship it out that day. You don't need to worry about the government clearing it or whatever. But you need to make sure that's the case first.

The second type of license we use is an individual validated license. That's where you determine with our assistance, perhaps, that your product is sensitive or the destination is sensitive and we're going to want to approve that license. You'll apply for a license with us, we review it. We might send it to the State Department or the Defense Department, or the Energy Department depending on what type of product it is or the country. And then we make a decision and if we approve the license you get it back and then you can ship, using that license and showing it to the customs folks. Typically, time frames for a validated license can take anywhere from a few days for NATO destinations to several months if you're looking at the Soviet Union or the Mid-east, some sensitive destinations in the Mid-East. Average processing time is about two weeks. A lot depends on what type of product it is and where it's going. If you're sending nuclear related stuff to Iran you might expect to wait quite some time.

The third way we license technology is through what we call distribution licenses or project licenses. A service supply license is another one, which is designed for example, for a major project in a country where you're putting up a dam or a hydroelectric system, or roads, or maybe putting a manufacturing plant. We could give you a project license that allows you to move anything related to that facility under one license so you don't have to come back to us every time you need to ship a new bag of bolts over there.

The second type of service supply license is primarily used by aerospace companies to do service and repair of airplanes in foreign countries so that they can quickly service and repair their fleets without having to come to us every time for a license.

The third type is a distribution license which is more widely used by companies who just have a lot of business overseas that don't want to come to us every time they want to ship. So a large multinational with subsidiaries around the world comes to us once with a list of their customers and a list of their products they want to ship and we authorize them for a four-year period to ship as much as they want of certain products to those particular customers. If they want to ship new products or they want to ship to new customers then they have to come back and get an amendment. But that allows a lot of our Fortune 500, some of our larger companies who have an international network to come and get it all taken care of all at once.

Those are the companies that we go out and audit as part of the deal. They get that large distribution license, but we go out and audit them to make sure they are complying with the regulations.

That's about as much as I want to say on an overview. Obviously, I'm happy to take some questions to clarify any of those points. But I'd like now to turn to the technical data side which is what we're trying to focus on today, and talk about how we control that. First off, I think it's useful to

describe and define what technical data is. It is information of any kind that can be used for or adapted for use in the design, production, manufacture, utilization, or reconstruction of articles or materials. The important thing there is information of any kind. As you see, it can be tangible, meaning blueprints or models, or manuals, or intangibles such as technical services. And that would include oral exchanges in the United States or abroad so if one of your engineers meets with a foreign national in the US to go over your products and provides them with technical data, that may require a license for him to carry on that conversation. Or for a foreign national to tour your facility may require a license. For you to send an engineer overseas to speak at a conference or to a foreign company, releasing technical data may require a license. Faxing information abroad, we've had companies call us and say I don't need a license, I'm just faxing stuff, say faxing blueprints to Taiwan. Unfortunately, that company violated the regulations. People think they're not going through customs therefore they don't need a license. It's not true. In the technical data area, if you're transferring information as defined by the definition of technical data of any kind for those uses, you may require a license and you need to check with us.

The key points there is an export is what requires a license. But an export is defined as an actual shipment out of the US or released in the US with the knowledge that it will be transmitted out of the US. So if you give it to someone here that stops by San Diego and you have knowledge that he's going to be going overseas with that information or he works for a foreign company or he's associated with a foreign company and will likely be transferring it, then you have knowledge that really is an export.

Obviously, the release of US technical data in a foreign country whether orally or in writing is an export. And a reexport of a product manufactured abroad using US technology is covered under this regulation. So if you have a license agreement with a foreign company who is manufacturing products under an offset agreement let's say in the UK and then shipping it down to Saudi Arabia, that may be covered by United States regulations and may require a US license. So you need to check that as well. Although it is really only a concern when you are dealing typically with the prescribed destinations which are primarily the Communist Bloc, or Eastern European destinations, Afghanistan, the PRC and some of the Mid-East countries.

Again, remember that release of information means a visual inspection by foreign nationals of US origin technical data, oral exchanges in the US or abroad, applications or technical experience acquired in the US. That also means service. So if you are sending a technician overseas to service equipment to set up a ground station for telephone communication and you are providing technical service, even though there are no commodities or blueprints going over there, it may require a license and you're going to need to inform us. Training. If you're going over to train foreign nationals on technology that we control, then we're going to need to talk to you. Most of this is dual use items. Strictly military, and going to a NATO country for the government, you're going to need to talk to DoD or the State Department.

So that gives you an idea of what's controlled. Now let me talk about the three ways we try and control it.

The first is the easy one. And that's called GTDA. This is the kind of information that's publicly available. We don't want to put any restrictions on fundamental research that's given out at conferences, available in the library, patents that are available in patent offices, information that people can get fairly easily, recordings, etc., catalogs from universities, that sort of thing, don't require a validated license from the department and are transferred under what we call a GTDA. So if you're exporting it on your shippers export declaration where it asks what kind of license authority you have, you just have to put GTDA which would indicate that it was general technical data and available publicly. That includes patent information. I think the important thing for you folks as a way of kind of measuring whether it falls under this regulation is whether it would be provided by your company to your competitor at no cost. So if its such basic information that you'd have it in sales literature or you give it at an open conference where you're not charging a fee because that information is valuable or sensitive, where it is open to the public or any member like this society could participate and any public person could join this society and therefore hear the conference. That kind of information is covered under this regulation and, therefore, would not need approval by the department before you export it. And that can include basic research, fundamental research on

new alloys or metals. It is basic research, the kind you would give at a research conference, that probably won't need a license.

In our regulations we cover in supplement 5 part 779, we provide a list of information and questions and answers that explain in more detail how we interpret those regulations for those of you who want to look at them.

The other important thing here is that technical data of this type is even exportable to what we call S and Z countries in our regulations which are embargoed countries. But the only thing you can send to countries like Cuba and Vietnam, etc. are publicly available and there is no restriction on any destination.

Let me move on now to the little more sensitive items which are covered under what we call a GTDR license without assurances. This type, first off, is not eligible to S and Z countries. It says restricted. What it means, is you can't ship it to S and Z. You can go anywhere else except the S and Z countries. S and Z, just for your information, are currently Libya, Cuba, Vietnam, Cambodia, North Korea, and Iraq is covered under a separate embargo. Those are the embargoed countries. You can't transfer any type of this technology to them.

Primarily what we're talking about here are maintenance, repair, and operation on a technical basis. So if you provide your buyers with information on how to maintain the equipment, repair it, etc. that can go under this type of license. Let me define with assurance. You'll see in a minute that in some GTDR means you can ship this under a general license without coming to the department for a validated license. You don't need to get any assurances from your importer as to what he has to do with the technology.

For the next license we're going to talk about, you have to get an assurance letter.

In addition, what's covered under this is sales information that you might normally hand out, information on the product specifications, etc. Except it can't reveal design, production, or manufacturing information unless the product itself is decontrolled. If the produce has been decontrolled and we're not controlling it, if you sold the product then you can transfer the technical data. But if we're controlling the product, if it's advanced aerospace equipment, you can transfer sales information like the specifications of the engine, etc. as long as it doesn't release design information or production information, assist the country basically in manufacturing or re-engineering it. Same thing with training. You can train foreign nationals on this type of technology as long as it doesn't exceed the information provided in a typical maintenance and repair and operation manual.

A key area here for a lot of companies is software. This is the way you can ship most mass market software. So it's kind of a shrink wrap stuff you can buy at Radio Shack, stuff designed for installation by the user without further support from the supplier. It's the kind of software you can ship to your customer and he can install it himself without any real technical expertise then that's probably covered. If you have to send two technicians to set up the software then it's probably not mass market software. What we mean here is software that's generally available to the public through retail selling points. The other key point here on software which probably affects some of your companies is encryption. That's a little catch for us. If the software is encrypted then we'll want to look at it. The Department of State has jurisdiction over some encrypted software. DOC, Department of Commerce, also has control. If it's standard commercially available software that has encryption in it, usually it's going to be the Department of Commerce that regulates it. If it's other type, the State Department has concerns about encryption and mail control. So if your software is encrypted you're going to want to check with us to see whether we control it or whether the State Department controls it.

The other thing you can do with software, is if you sell software and there are bugs in it, you can fix those bugs and provide that kind of service to it as long as you're not enhancing the past level of the software.

The next type of general license is called the general license with assurance. This is designed primarily for the free world countries, what we call T and B countries. Which excludes countries like Romania, Czechoslovakia, Poland, Hungary, the Soviet Bloc, PRC, and Afghanistan. But for all the other free world destinations, with the exception of embargoed countries, you can use this license. What it is it allows you to ship the above stuff we just talked about, even if related to embargoed commodities which are most sensitive

commodities, provided you get a letter of assurance from your importer. Basically what that says is that your buyer is going to put in writing the fact that he knows that he can't reexport this product to proscribed destinations. It has to be signed by someone in the company who has authority to legally bind the company or if it is an individual, the individual can sign it assuming that he is taking personal responsibility, not representing a company. If you are selling to a distributor, they must get the assurance from their distribution points and you or the distributor have to keep that letter in your files.

The last part of the regulations I want to cover are the trickier ones which are the individual validated licenses. These are the sensitive products that are going to require a license from the department. Primarily for any T and B country which is basically the free world countries, you are going to need an individual validated license if it's listed under 779.4 Section C or D in our regulations. Primarily those are when it is nuclear related technical data. That will require a license even if it's going to Canada where normally a license isn't required for anything. I know there is a kind of catch-all category that is paragraph D which primarily involves aero-space equipment. So you're going to want to look at those regulations if you are at all concerned about your technology, see if your products are covered. Again the other way is to give us a call and we'll help you determine whether your technical data is sensitive in that regard. The other reason you might need a license is if under our commodity control list descriptions in our regulations it specifically says technical data on all of these types of products are controlled. So if, for example, you make machine tools or semiconductor manufacturing equipment, or super computers, and you look in our regulation and you find that those machine tools are controlled it may also say technical data related to these types of machine tools of a certain level of technology are also controlled.

The sensitive products are under Section 779.4 Paragraphs C and D and you can also look at our supplements three and four. And you can look under specific ECC entries which are Export Commodity Control number entries which will look where you find your technology and products and then find out if the tech data is controlled.

The last Section 779.5 kind of gives the requirements of how to fill out the license application, etc. Again, our office can assist you if you are unfamiliar with how to do that, we can certainly assist you in both finding out whether you need license, what authority you can ship under, and how you go about complying.

Let me say in closing, a quick word about the changes that are in store. Our technical data regs have been some of the more complex regulations we in the exporting community have had to deal with. Three years ago, in fact, when I was back in Washington, we undertook an exercise to rewrite the regulations. For the first time, at least in our bureaucracy's history, we hired an expert in plain English to write them. We got a little tired of putting a lawyer and an engineer in a room and having them draft the regulations and then us in the policy shop trying to figure out what they meant. So we have redrafted the tech data regulations. They are in what we call plain English. It still has a certain amount of technical jargon in there simply because the products we are controlling are technical. Those regulations are due to come out this fall. What it's going to try and do is clarify where the technical data is controlled and, it's going to clarify a couple of issues that have come about in our regulations. For example, a number of companies have foreign nationals that work for them in the United States. We have a lot of engineers coming from India and China that work at various companies. We're going to clearly define when those foreign individuals are eligible to know CUS technology so you don't have to hire engineers and find out you can't show them anything. We're going to clarify that in the regulations. There is also an issue of comingling tech data and that's where US technology, let's say for semi-conductor manufacturing is transferred to Japan and then they make improvements or enhancements over the years in that technology. Currently it still comes under US license even if it was originally designed to make 286 computer chips and now it's making 486 because they've done enhancements first over the control when the argument from industry is that this is really not the same technology that we transferred, but was enhanced by foreign know-how, not by US know-how. So we're going to try and clarify that.

The other thing we're going to do, because we're getting a lot of confusion about what is GTDR with assurance vs. GTDR without assurance, we're going to change it to GTDR without assurance. It is not going to be called GTDU which means general technical data unrestricted. The type of technol-

ogy that needs a lot of restrictions will be GTDR so there will be a little better clarification there.

The last point that we are covering is that the President last year ordered us to meet with our COCOM allies which are primarily NATO countries, and totally rewrite the list of products that are controlled. This is based on what happened in the Soviet Union, the fact that our controls have for too long controlled outdated technology. That exercise was completed two weeks ago. We are in the process now of redrafting all the regulations, changing the classification numbers and everything. That regulation is due to take effect September 1. It is going to significantly liberalize what requires a license. Three years ago we issued about 100,000 licenses a year, about $100 billion in exports. By the end of this year we expect we will be licensing about 20,000 shipments a year on an annual basis. So it's about an 80% reduction in our work load and it is probably going to result in only about 10-15% of US technology requiring an export license. So we have taken a great deal of time and effort to get out of your hair and help a lot of US companies to be competitive internationally, and at the same time protect the US national security. After all, we're still going to be controlling the sensitive products. The President just came out last month with guidance on a new enhanced proliferation control initiative on which we're getting an agreement from our allies on how to control nuclear, chemical, and biological technology so that they don't fall into the hands of some of those countries trying to develop those systems. So we're going to continue to control and we're going to have focuses on some of the mid-east countries. Some of the third world countries are developing systems as well as the Soviet Union and some of our traditional proscribed destinations. We're going to limit the technology to only the most critical technology and we're also going to free up related technical data. The other thing about that is when we come up with this new list, the technical data information will be right in with the hardware so we're going to have controls set up so that computers will be in one section and the first section of that will be the hardware, the second will be the technical date related to those computers and the third will be the software related to those computers. The same thing in aerospace and machine tools. Before we had technical data and software lumped into one section and you had to figure out whether your technology was controlled or not. Now we're going to streamline the system and make it more liberal and make it easier for you to understand. We anticipate starting in August/September to do a series of briefings around the western region where I'm responsible to brief all the companies on that and you can feel free to stay in touch with us. We will have a series of seminars scheduled in August/September to provide briefings on their new regulations. ■

MAJOR CHANGES TO THE ISM

26 June 1991

Gregory A. Gwash
Deputy Director
(Industrial Security)
Defense Investigative Service

1. Introduction. Thank you for this opportunity to address your membership today. I would like to concentrate today on the issue which is foremost in everyone's mind - the new Industrial Security Manual (ISM). I would like to specifically address the following issues.

(1) Editorial Changes
(2) Major Policy Changes
(3) Other Policy Changes
(4) AIS Changes
(5) Questions/issues that have been resolved
(6) Major issues pending resolution

2. Editorial Changes. I would like to familiarize you with some of the editorial changes that have been made. Although we will all have to deal with the learning curve associated with any new format, I believe that you will find that once you become familiar with the new format, you will find it much easier to locate information in the ISM.

a. The following information has been specifically stated in the ISM. Generally, this information was true but never contained in the ISM.

(1) Requests for Waivers. Contractors have always had the ability to request waivers, however, instructions for how to do so were never contained in the ISM.

(2) Employees rights during interviews. Again, employees have never been forced or coerced to answer questions during the inspection process. However, I must call your attention to paragraph 1-203K, which requires facilities to cooperate with DIS inspectors and investigators during the conduct of inspections and investigations. (1-206a)

b. The following information has been deleted from the ISM because it was deemed inappropriate for the ISM.

(1) Self-inspection guide. This information was not considered mandatory, but more a useful tool for the facility. The guide is being updated to reflect the changes in the new ISM and will be distributed by the Industrial Security Represenattives as required by their facilities.

(2) Electronic PSQ Program. Procedures and policies for this program can be found in the User' Guide distributed by DIS to all participants. This allows us to more readily update the instructions as the system grows.

(3) Index. The index was deleted in hopes that the new format and Table of Contents allows users to readily locate information in the ISM. Please let us know if, after the break-in period, you find this to be true. If not, we will consider developing one for the next revision.

3. Major Policy Changes. Now I would like to discuss a few major policy changes which may have a significant effect on the program and your operations.

a. Company CONFIDENTIAL Clearances. As most of you know by now, with publication of the new ISM, contractors will no longer be burdened with the responsibility of granting personnel security clearances. Existing clearances will remain in effect. With the issuance

of interim clearances in less than two weeks, the impact of this change should be minimal to the contractor. (2-204)

b. Clearance Revalidation. The period of eligibility for immediate access to classified information based on the revalidation action has been changed form 5 years to 2 years. This policy represents a compromise from the original proposal to discontinue the practice of the contractor granting access prior to notification from DISCO. (2-218a)

c. Prime contractor responsibilities. The responsibilities of the prime contractor in dealing with subcontractors have been greatly extended.

(1) Signing the DD Form 254, rather than submitting it to the User Agency. (7-201, item 16)

(2) Certifying need-to-know on Category 2 Visits. (6-107)

d. Advertisement policy. The ISM now states specific language which may be used in employment advertisements for positions which require access to classified information. (2-100b)

4. Other Policy Changes. There are other policy changes which may not have a dramatic effect on your programs, but I would like to call your attention to.

a. End of day security checks are now mandatory. (5-104)

b. Express Mail. The test policy for allowing Express Mail use for SECRET has been finalized in the new ISM. However, the previous allowance for the use of curb-side mailboxes has been rescinded.

c. Pre-employment clearance actions. The period of time between the submission of the clearance request and the date of employment has been changed from 120 days to 30 days. (2-202)

d. SPP submission to CSO. This practice was, for the most part, already in effect. SPP's and changes thereto are reviewed on site by the IS Rep and a copy is only required upon request. (1-202)

e. Layoff/leave. The period for layoffs and leaves of absence, during which a clearance may remain active has been extended to one year. (2-210)

f. SF 312 repository. As you were notified in ISL 91L-1. DISCO has established a repository for maintaining SF 312's. The details are in the ISL. (3-103c)

5. AIS.

a. A new security mode has been established: partitioned. It represents better security than system high, yet less than multi-level. (8-204)

b. New section on networks has been added. (8-400)

c. Software disconnect routines can be used for remote devices to satisfy physical security controls requirements.

6. Resolved Issues. The new ISM contains some language that may be ambiguous. DIS has published interpretations that will appear in the next ISL.

a. Security violation reports regarding SAP material should be reported to the SAP customer. (1-304)

b. Individual culpability reports are based on all security violations, without exception to include SAP's, when they meet the criteria of the ISM.

c. All security violations must be reported to the FSO so that a preliminary inquiry can be initiated to determine if loss, compromise, or suspected compromise occurred. (1-208)

d. Visits in connection with a prospective contractual relationship are still covered under

Category 1 procedures. However, there must be a formal or written solicitation in place. (6-107a)

e. Shredders may be used for the destruction of non-paper products, other than microform. The information in 5-706 which prohibits their use was an error. (5-706 and 5-707a)

f. The lead time for international visits remains at 45 days. The 30 days stated in the ISM only addresses the requirement established by the foreign government. The remaining 15 days are for DISCO processing and mail time. (10-501b)

g. The prohibition against external markings on security containers only prohibits the use of the words CONFIDENTIAL, SECRET, OR TOP SECRET. Color or other methods of coding are permitted. (5-307)

h. The requirements to mark working papers with the overall classification only covers front and back page markings. Nonetheless, it is still a good practice to use page and portion markings to ensure that the proper classification is used on the final document. (5-206b(2))

i. DISCO still requires multiple copies of international visit requests. They are asking for three copies (10-501b).

j. The contractor must complete the NATO Security Clearance Certificate. DISCO will verify the clearance. (11-111a)

7. Unresolved Issues. There are several major issues that are still pending final resolution. DIS and OSD are working together to establish consistent and reasonable procedures.

a. Control of reproduction equipment. (5-603) (Resolved - ISL91L-4)

b. The four hour "container" check of bar and padlock containers with SECRET storage. (5-305b) Resolved (ISL91L-4)

c. C2 by 92. (8-303a) See (ISL91L-3)

d. Cleared personnel for unclassified software. (8-309a) (Still Pending)

e. TOP SECRET working papers. In the interim, the policy in the ISM will be followed. (5-206b(3)) (Still Pending)

f. Prime contractor's authority to grant retention. (7-105) (Resolved)

g. Category 2 need-to know certification. (6-107b and 5-513b) (Resolved)

8. Summary.

a. Study the new ISM to identify changes and to be able to readily locate requirements.

b. Work with your IS Rep to apply any new or modified requirements to your facility.

c. DIS will publish interpretations and changes in the ISL as soon as possible. ■

THE PARTNERSHIP BETWEEN GOVERNMENT AND INDUSTRY

26 June 1991

Arthur E Fajans
Director, Security Plans and Programs
Office, Assistant Secretary of Defense

I'd like to talk about the government/industry partnership in the context of some of the seminar themes--Commitment to Excellence, Developing Trends in Industrial Security, The Politics of Defense, and of course, Trends in Industrial Security are even further subtitled into Protecting Tomorrow's Technology Today.

First, The Commitment to Excellence. That's what NCMS is and has been all about over its 25 year plus history. Much has happened since we last met. The tension in the Gulf changed to hostilities pushing Eastern Europe and the Soviet Union off the front pages only to have them return with equal suddenness. We have vacillated between euphoria over the decreased military threat in Eastern Europe only to rapidly turn to skepticism about the internal course of the Soviet Union, its military and its leadership. Talk of integrating NATO with some former Warsaw Pact members has, at least for the moment, dramatically slowed. The awesome effectiveness of our forces and those of the coalition in operation Desert Storm is due, in part, to the success of information, technology, and industrial security in protecting the classified aspects of the weapon systems in use. Counters to these systems were minimized through the successful efforts of our security procedures and practices. You had a part in ensuring the security of our defense assets and you've done a good job. Your commitment to excellence as security professionals has contributed directly to the security of our nation's valued classified assets. However, as Admiral Inman intimated, the security system requires our constant skepticism, an awareness of the potential threat and our continued vigilance to preserve and protect the value of our nation's secrets--be it information, equipment, or technology. Our role is to protect and we should continue to play out that role as best we can despite its defensive nature and lack of glamour.

We continue to be on the move and this conference has covered in part some of the ongoing activities of interest to you in information, personnel, and industrial security. But we require not your passive observer status, but your active participation as well. It's all well and good to soak up as a sponge the information the seminar leaders have imparted, but you need to squeeze that sponge and give back some information, insight, and initiatives if this conference is to be truly successful tomorrow and the following day and day after that.

I'd like you to stroll down the seminar boardwalk with me a moment and we'll look back at some of the knowledge that we have acquired.

The Politics of Defense. Managing security in a dramatically changing environment, openness equals access, the globalization of industry giving rise to phrases like "good enemies and bad friends," the blurring of industrial espionage and government directed espionage, narcotics wealth, and secure communications. These are some of the things that Admiral Inman covered in his keynote address. As I wandered around I heard Dee Dee Collins giving them hell at the workshop on Security on a Shoestring. Cathy Dyl was talking about Class A and B in terms of security education. You didn't think I was listening at the table, did you? There was a workshop on the ABC's of AIS. I think it should have been titled the XYZ's of AIS. It's a tough, tough problem. I asked people what they expected to get out of the semi-

nar. One replied "how to make the world more safe for democracy." Actually, now that I think of it I believe he was attending another conference. He may have been attending the American Society of Mechanical Engineers and the ad hoc committee on Seismic Pipe Issues. As I passed from one NCMS workshop to another, I kept passing Japanese businessmen, politely bowing, being very gracious.

Another attendee said "I want more knowledge. Knowledge is job security. Knowing more today than I did yesterday so I can be better prepared for tomorrow." Gaining more knowledge. Someone gave me a relevancy matrix and try as I may I couldn't find myself on it. And who will ever forget Captain Dave Carey's presentation on challenges. What an impact.

One final thought on the Politics of Defense. Who was at the seminar two years ago in Tampa? Does anybody remember my presentation. I talked about threat, vulnerability, and value. That's right. Who was the threat at that meeting? Come on raise your hands. Who was the threat? I guess we don't have a threat any more. Who was vulnerability? Ah, thank you Roger. Who was value? Well, I'm not going to go through it again, but I've come up with another system. So again, I'm going to divide you up into three sections. And this will be one section, you can figure out who's over there in the center and the right. Now I want the left side to say "I'll find out sir. Now the right side, I'd like you to say "What did he say, huh?" "What did he say, huh?" Now the center section here, I want you to say, "I'm in charge." Let's hear it now, "I'm in charge." Good, I was afraid I'd hear that sound of one hand clapping, but you did very well. OK, let's try it now. The center, "I'm in charge." The right, "What did he say, huh?" The left, "I'll find out sir." Now do it one more time on your own. "I'm in charge." That's command and control. "What did he say, huh?" That's communications. "I'll find out sir." That's intelligence.

For those of you who may not have heard, there's been a realignment of security functions in OSD. And I currently work for Command and Control, Communications, and Intelligence. This may be repetitive for some because I know you have heard this throughout the conference, but the security disciplines that remain in policy, are international security, NATO security, and special access programs. The programs that moved to C^{3}I are counterintelligence, personnel, physical, industrial, and information security. As far as I'm concerned, every time I took out a ticket here it was like giving away a function. And now all I have left is my name.

Now for some developing trends in industrial security and other security disciplines. The Defense Personnel and Security Research and Educational Center (PERSEREC) and the intelligence community have completed a comprehensive two-year study of more than 7,000 special background investigations for access to Sensitive Compartmented Information (SCI). Based on the results of that study, the Director of Central Intelligence, Personnel and Security Working Group and the Advisory Group Security Countermeasures Personnel Security Committee, have recommended a Single Scope Background Investigation (SSBI) that will serve as a basis for issuance of both Top Secret clearance and access to SCI. The new 10 year scope investigation will include a subject interview in all cases, interviews with ex-spouses, and the usual assortment of credit checks, employment record checks, local agency checks, interviews with co-workers, supervisors, developed character references and neighborhood checks. It is expected that the single scope Background Investigation can be implemented before the end of the year. The implementation of this historic procedure across all federal agencies will substantially facilitate the reciprocal acceptance of clearances within and between agencies and should significantly reduce the time and cost of clearing military, civilian, and contractor personnel while at the same time simplifying procedures and enhancing security. Both the Personnel and Security Working Group and the SCM Personnel Security Committee deserve credit for their tenacity in bringing the intelligence and security community to the brink of a new investigative era in an area where not much has changed since World War II.

Now we heard a little bit about the National Industrial Security Program (NISP) that's been sprinkled over the last two and a half days and you'll hear much more about it after lunch. But there is an inter-agency sub-committee of the NISP that is exploring the possibility of creating a single personnel and security questionnaire, that could be employed by all federal agencies as the basis for conducting background investigations for security clearance. This is especially important for clearing contracting personnel who currently must contend with a multitude of different forms. Depending on the agency and access involved, this inevitably

leads to delays and increased cost due to lost productivity. Like the Single Scope Background Investigation I mentioned earlier, the development and implementation of a standard PSQ would eliminate duplication of effort, reduce cost by permitting contractor personnel to obtain a clearance faster, and play a key role in facilitating a reciprocal acceptance of security clearances throughout the federal government.

Much work remains to be accomplished, but I believe significant progress has been made in this regard and I am more than cautiously optimistic that a standard PSQ will be developed in conjunction with a National Industrial Security program.

We are also looking at the possibility of creating a uniform set of adjudicative criteria for issuance of a security clearance for access to SCI. Currently, significant delays are experienced, especially in the contractor community as a result of a cumulative effect of the application of different investigative scopes, non-standard PSQ's, and a variety of formal and informal security clearance and access standards, especially in the area of special access programs (SAPs).

I believe that the adjudicative standards for security clearances and SCI access are very similar in most respects and the possibilities of this as a common base line standard for access to classified information can be set for most agencies in the intelligence community. Where certain extremely sensitive programs clearly demand enhanced and possibly unique adjudicative criteria such standards can be developed and applied as an overlay to the base line requirement. There is a wide range of entrenched opinion as to whether such a course of action is feasible or even desirable, but we are working closely with other key agencies to ensure that the concept is fully analyzed and explored.

I had an uncle, he was a little eccentric, and he worked very hard at what he did. Down in the basement he worked and worked, and worked, trying to develop a formula for a soft drink. He created one that he marketed as Four-Up. It didn't succeed. Undaunted, he returned to the basement and worked, modified the formula, made some improvements and tried again. He called it Five-Up. Again, it failed. But he was a man of tenacity and he kept at it. He tried one more time--Six-Up. He died a disappointed man. If he only knew how close he had come.

In February of this year the Deputy Secretary of Defense, Mr. Atwood directed that we conduct a study of the alternatives and cost involved in centralizing the multiple DoD adjuctative functions. This study, which is to be completed by 30 September of this year, originated in a defense management review decision which raised the issue, "Can more effective security program management reduce over-all security requirements and cost without undue risk to national security?" There are currently more than 19 separate agencies within DoD accomplishing adjudications for security clearances and access to SCI. While there are numerous alternatives that might improve the current situation by reducing both adjudicative costs and delays there is little doubt that in an era of declining resources some improvements must be made. DoD has a mandate to evaluate all reasonable alternatives to include the status quo and to report its findings and recommendations to Mr. Atwood for consideration and a final decision. I am optimistic that, like the single scope background investigation, we will see some significant changes in the adjudicative procedures and organization based on this study.

It is estimated that within DoD we spend approximately $8 to 11 billion on security. Yet the preponderance of security costs are not readily identifiable in the budget. Mr. Atwood has approved a controller and a security policy design and implementation of a security budget exhibit for the 94/95 budget submission. This effort is currently well under way with the initial goal to be the development of summary budget data on information, operations, personnel, industrial, and physical security with a separate classified exhibit with special access programs, counterintelligence, and intelligence related security programs.

These budget exhibits will attempt to capture manpower and total obligation authority, for RDT&E procurement, operations and maintenance, and military construction. Over the years, we've done such a great job of telling the security professions that they need to integrate security into the operations, that we can't find the costs any more. They're all embedded. But we need to start. And we can identify direct costs. I can no longer be in a position of going to Mr. Atwood and answering his question, "How much money are we spending

on security?" I can no longer say, "I don't know, but it's not as much as you think."

I don't think there is any contractor here when his CEO asks him "What are you spending on security," doesn't answer that question to the penny. We need to be able to do that in government as well. We need to determine more accurate indicators of cost that implement industrial security requirements by contract.

With the development of implementation plans for the National Industrial Security Program, cost determinations and a mechanism for cost control, or cost avoidance will be undertaken. Survey questionnaires have been prepared and distributed to over 1600 contractors. The responses are due back from the contractors by the end of July 1991. The results will be compiled. We have also sent out similar questionnaires to the military departments. Net costs can only be described in terms of what the program costs now, but when we go to the President on 1 September of this year, we will have better data than we have ever had before.

I'm going to shift again. I'm going to make reference to Ev and a conversation I had well over a year and half ago. It was at a conference like NCMS. During one of the breaks I got him aside and I said, "Ev, I want to share an idea with you. You don't have to react to it right away. Just let me talk to you about it and when you have a chance to think about it come on back and we'll discuss it some more. I want to create some sort of logo or image that will become ubiquitous throughout the entire Department of Defense. Much like when you look at Smokey the Bear you think of preventing forest fires. I want something that when people see it they will think of security." So, up to this point Ev's right with me. He says, "What do you have in mind?" "I want a security penguin." His eyes rolled back and I said, "Don't react right away. Just think about it." So he did think about it and about six months later he sent me a memorandum. Down at the bottom it says "Excellence in security through total quality management--TQM." You know what we used to call TQM? HW. Hard work.

Lynn Fisher on Ev's staff got his Security Awareness Subcommittee together with representatives from all the DoD components. He, in an unbiased manner presented this idea to the DoD components. It was unanimously rejected. That indicated to me that I was probably on the right track. It's a low cost effort and I called up Mr Alderman one day and I said, "if you have a few moments I'd like to come down and talk to you about an idea." He said "I have a few moments. What do you want to talk about." I said "my security penguin." So I went down and I explained to him that this was a low priority, low cost, no cost effort to this point, but it's been developed to a certain level and before I proceeded I wanted to know from him whether or not he supported this idea, or was he telling me I was out of my mind, or whatever. He was not wildly enthusiastic about it. But the bottom line is he didn't say stop. So, in my own little way, in my spare time, I keep going down this path very, very slowly.

I don't know if any of you have seen this, this is out in draft form for comment. It's been put together by the Defense Security Institute. I want you to study that for just a moment.

(Shows security penguin)

Over the last two years, as I indicated in my opening remarks, tremendous changes have taken place all over the world, altering the assumptions that have driven our political and military policies since the end of World War II. Since World War II our defense strategy has centered around preparing for short notice, global conflict with the Soviet Union. Over the past two years the Soviet threat has moderated. The Warsaw Pact has disintegrated and US/Soviet relations have improved. Although the threats to US security are changing, the central focus of US defense strategy is not. Our goal remains to deter aggression against our nation, its allies, and its industry. What has changed in the US defense strategy is how we plan to deter and defeat aggression in the new global environment. First, we will still need a strong deterrent, defensive capability. Although the Soviet threat in Europe has receded, it still has a massive nuclear arsenal aimed at the United States. Furthermore, they are continuing to modernize this force. America must continue to maintain a diverse mix of survivable and highly capable offensive nuclear forces as a deterrent against a massive nuclear attack. Our defense strategy requires that we protect the current high quality and superior capabilities of US forces, especially since their total size is being reduced. We must sustain the critical elements of America's industrial and technological base by maintaining a robust investment in defense research and development. Continued investment in the development of critical

technologies is essential to our long term security. If we are to successfully encounter future aggression, then we must make the investment now in the next generation of weapons systems that will maintain our security into the 21st Century. That is a partial answer as to how to keep the world safe for democracy. What about the government and industry partnership? Partnership is teamwork. Let's together do what Captain Carey very forcefully and effectively suggested. Do what we need to do, do the best we can, keep our senses of humor, grow a little, and continue to have faith in yourselves, have faith in the knowledge that you can make a difference. Thank you. ■

Left to right: Larry Wilcher, Harry Volz, Arthur Fajans, Jack Donnelly, Frank Ruocco and Steven Garfinkel

NATIONAL INDUSTRIAL SECURITY PROGRAM

26 June 1991

Panel Discussion

Moderator:

James Linn,
Security Manager
SAIC International

Panel:

Steve Garfinkel,
Director of Information Security Oversight Office (ISOO).
Frank Ruocco,
Director of Security, Central Intelligence Agency.
Jack Donnelly,
Director, Defense Investigative Service.
Art Fajans,
Director of Security, Plans, and Programs, Office of the Secretary of Defense.
Harry Volz,
Director of Security, Grumman Aerospace Corporation.
Larry Wilcher,
Deputy Director for Personnel Security, Department of Energy.

James Linn

The one thing that originally was planned was to have Maynard Anderson chair this panel. Maynard wrote a letter and I'd like to read it to you.

"Dear Mr Linn: I recently received a letter of invitation to participate in the 1991 National Training Seminar of the National Classification Management Society in San Diego from June 24-26. I had a telephone conversation sometime ago with Mr Bob Nelson, San Diego Chapter chairperson, and I agreed to participate in this seminar by leading a panel devoted to discussion of the National Industrial Security Program.

It is most disappointing to be forced to notify you as seminar chairman that I will be unable to attend this year's National Training Seminar. It is now certain that my testimony is required before the Senate Select Committee on Intelligence at 2 PM on June 25 along with Director Sessions of the Federal Bureau of Investigation and a representative of the Central Intelligence Agency.

The good news is that the opportunity to testify will enable me to outline, for the members of that committee, our intention to better manage the amount of classified information now accumulated in our departments and agencies. We intend to find ways to reduce the volume of information classified for an indefinite period of time. We expect that better declassification review procedures can be found. Every requirement for information security must be examined to determine whether it adds value to the security system. I feel strongly that the advisory group, Security Counter Measures, which I chair, must address the potential unauthorized disclosure of United States technology to foreign governments. Non-military information is of increasing importance to the national interest and economic well being. We intend to pursue why the United States should have a policy to protect certain information, not now defined as national security information, and whether or not we can manage the risk within current policies.

Efforts to develop an implementation plan for the NISP are moving forward. In some areas we are making more progress than I had expected. A report will be sent to the National Security Council by September 1, 1991 which

Efforts to develop an implementation plan for the NISP are moving forward. In some areas we are making more progress than I had expected. A report will be sent to the National Security Council by September 1, 1991 which will describe accomplishments along with those matters still needing attention.

Some 250 security professionals from government and industry are working on the NISP. It would be appreciated if you could express my thanks to all those attending the 1991 seminar who are devoting so much time and energy and talent to this worthy cause. While I will greatly miss being with you to see and visit with friends and colleagues, and enjoy the ambience of San Diego, the panel dealing with the NISP will be in good hands along with Mr Harry Volz, the co-chairman of the NISP steering group, and with Mr John Donnelly, and Mr Steve Garfinkel, both steering group members who will be at the seminar. Also in attendance to make a presentation will be Arthur Fajans who is the executive secretary of the steering group. They should be able to answer any and all questions concerning progress in the NISP. We hope so, we know so.

And so you don't think I'm loafing while you're working hard at the seminar the morning of June 26, when the NISP panel is scheduled, I will be briefing the laboratory directors of the Department of Energy regarding the NISP. Thus the time I cannot spend with you will be well occupied.

As last year's recipient of the NCMS Woodbridge Award, I particularly wanted to attend this seminar to return some of the honor and recognition that the NCMS has granted me. Since my agenda escaped my control for a time, I will rely on members of my staff to work with the seminar participants in our mutual efforts to improve information security. That accomplishment will bring honor to all of us. Please convey to everyone best wishes for a successful seminar and a wonderful time in San Diego.

Sincerely,

Maynard C Anderson, Assistant Deputy Undersecretary of Defense, Counterintelligence and Security."

Thank you Maynard for the letter. I appreciate your indulging me to allow me to read that to you.

On April 4, 1990 the President directed a national security review of the government's industrial security programs to determine the feasibility of establishing a single program applicable to all government departments and agencies to be known as the National Industrial Security Program, (NISP). The November 1990 response advised the President that the Secretary of Defense, the Secretary of Energy, and the Director of the Central Intelligence Agency, supported the concept of the NISP, and would work together with industry representatives and conduct a zero based regulatory review, develop an instrument of authority for a NISP, develop and promulgate standardized security policy, ensure a mechanism for determining industrial security cost, and ensure completion of on-going personnel security initiatives for a single scope background investigation. On 6 December 1990 the President concurred and directed that a report of recommended policy changes be provided to the National Security Council by 1 September 1991. In accordance with the President's direction, representatives of industry, the Secretary of Defense, the Secretary of Energy, and the Director of Central Intelligence formed an inter-agency task force. This afternoon's panel consists of several members of the inter-agency task force steering group. Each panel member will say a few words on the NISP and its development from their own perspective and then we will open the session for questions from the audience and some ensuing discussion.

What I'd like to do is have shown a short video on the NISP.

Summary of Video

With inventiveness and drive unmatched in all history, America has continually expanded horizons. Today, technological advances push us through a swirl of change--socially, politically, and economically. The history of mankind is being rewritten almost daily as we speed toward the 21st century. And the greatest nation on earth is being challenged.

As the United States again defends its security as a nation, and the freedom of its people, the

biggest threat may be to our economic interests and our technological position of leadership. We have what others want. Our prize attraction is what President George Bush has called our vital technology and sensitive information. It is the opinion of the nation's top defense and intelligence officials that the globalization of industry, increased economic competition, and dramatic change in East/West relations, will lead to new and different threats from our adversaries.

Today, industry faces a broad range of threats, including foreign intelligence collection. To meet military and economic challenges of the next century, the U.S. simply must have a strong, secure industrial capability. As we prepare for tomorrow, government and industry experts are considering alternatives to government security programs for industry. Today's policies, rules, and regulations have evolved over the past 35 years. Under mandate from the President, they are working to replace today's rules with a single, coherent, and integrated industrial security program. It will be known as the National Industrial Security Program, or the NISP.

A comprehensive three-year coordinated study involving both industry and government is supported by all major federal agencies and departments. The review found significant redundancy in the government security requirements and regulations imposed on contractors. Following the study, a Presidential National Security Review was conducted in April 1990. The Secretary of Defense along with the Secretary of Energy, and the Director of Central Intelligence were directed to study the feasibility of a National Industrial Security Program. The result was a report to the President which concluded that a NISP is feasible, desirable, and timely. The report stated that the same sensitive technologies and information used by various government organizations are often protected by different security standards resulting in confusing and costly administration.

As part of the study, the cost data for industrial security implementation by 14 government contractors was evaluated. The figures show these companies spent approximately $800 million dollars in calendar 1989 on government directed security conditions. The 14 companies spent $1 billion on government required security for automated information systems. Based on this information, it was estimated that the total cost to the Federal Government to administer its industrial security program during calendar year 1989 was 13.8 billion dollars. In a cover letter with the report, the President was advised that changes in the management and organization of industrial security programs are necessary.

Using the creative talents of the private sector to assist in the development of cost effective security standards, we should be able to improve the security of our most sensitive information and technologies. As recommended to the President, an inter-agency task force under leadership of the Secretary of Defense, Director of Central Intelligence, and the Secretary of Energy was formed to design a National Industrial Security Program. General oversight is from the Executive Office of the President. The task force of experts from government and industry will conduct a zero based regulatory review to reduce unnecessary requirements, establish a single program authority, develop uniform standardized security policies to include security education, training, inspection standards, and enforcement procedures, establish ways to determine complete industrial security costs, and develop a standardized single scope background investigation which is acceptable to all government departments and agencies.

Also, as directed by President Bush, the task force will report to the National Security Council by September 1, 1991 on recommended policy and program changes.

When fully implemented, the National Industrial Security Program will be a striking example of what happens when government and industry work together toward a national goal. With the NISP we will hopefully avoid significant future industrial security costs while providing improved security to government and industry. At the same time, a strong NISP will give the United States the flexibility it needs for continued world technological leadership.

To help us understand the NISP, we'll start with Harry Volz.

Harry Volz

First, I want to test your powers of observation. That video production was done by the Boeing Company as a support effort for the NISP. Did any of you notice any other single product in the presentation that was not a Boeing product? Good. I mentioned who built it, but I guess you had a clue.

The second thing, I want to see what your power of retention is. Are you frustrated? There you go, there you go. Not bad for the last session of a three day program. You should know, those of you who have been involved in the NISP for some time, that it started in March of '88. I don't know how significant that is to you, but to be able to stand up here after a little over three years of hard work between government and industry and be this far is pretty exciting for me. It's pretty exciting for anybody who's been a part of the program. If you saw and listened to the film without nodding off it says one program. It says better security. It says lower cost. And it should include a single scope background investigation (SSBI). I think you're going to hear from the other members of the panel how many of those things have come a long way since we first stated them. It said something else that's buried in there that sometimes not everybody remembers about the NISP, but it has a really single goal. And that is to strengthen the economic and technological leadership of the United States in the world. And that's its goal. That's the kind of thing that is being worked on. Some of you are supervisors of people who are spending a lot of time on the NISP. I know this gentleman told me one day that he went out to find somebody in his office to do a simple task and they were all at a working group somewhere working on the NISP. It's a tremendous effort. You heard Maynard say about 250 people are involved. You had to know that was a little matter of concern for us. At the beginning of the program there were about 12 people involved. As we moved a little further down the line there were probably six who knew exactly what it was when they were all in a room together. Otherwise, if they were lawyers, I think I heard there would be seven opinions.

It was a real challenge to introduce, as many people as we did into this effort. I'm going to use no slides, no foils, and I did not bring the video tape. I discovered in Tucson a couple of weeks ago, a new method of visual support for a speech. It's called your imagination. For those who have been watching the tube too much, it's going to be tough for you, but let's turn on the imagination for a minute because I want you to picture about where we are and where we hope to be when it comes to the NISP.

The NISP grew out of a problem that both of us shared--government and industry. And that is that there are about 1,000 separate, individual industrial security programs in the United States operating today. Now picture them in your mind, some small circles, some triangles, some squares, some rectangles, different colors, overlapping, some way off in the corner. Now we're talking about the NISP. There are still some people who see the NISP concept as a movement of all those individual programs together and placing a box around them. That is not the NISP. You can erase both of those issues from your mind and draw a single box with just the number one in the middle. That is the NISP. It is not a collection of anything. It's going to be all by itself alone. It will be developed, as we move along, with your assistance, which by the way your society has a lot to be proud of because you were early on when it came to supporting the concept. As was NSIA and ASIS and a number of other organizations. But you were early on and have given a lot of support. I was pleased to hear that when Bud Bowers was recognized, the NISP was mentioned on his plaque. You should know that I received a resume for employment just the other day from a person who listed that he had worked on a NISP working group. You can see that somebody already thinks that it's important enough to be a part of their resume.

You heard in there a word that I put into the script. It said "striking." It was a striking example of what happens when industry and government work together hand in hand. It's a true partnership. We've heard that a lot of times. I was introduced to the concept of partnership. I believe the first person whom you recognized with your exceptional Woodbridge Award was Frank Larsen. Frank's the reason I'm still in the business. I was ready to quit because I was frustrated. But I didn't because he convinced me to stay. He said "One day," and I think the day's here," I think all of you are looking at a program that is going to make you proud to be a part of it, and that's going to be worthwhile and the duplication, hopefully, and high cost, will go away."

Somebody asked when I got here, "Is it really true that Maynard Anderson announced in Tucson that this program would not be implemented until the year 2000, because if that's it I can't hang around that long." I told that person that I would take the opportunity up here to explain where that 2000 comes from. At the Tucson meeting, Maynard said that he expected that the program would be fully implemented by 1997. Now I have an announced retirement date of 30 June 2000. I complained to him that he was shortening my retirement date by three years. So he adjusted the

time period. I heard about that the first time there was a problem or an issue. So I announced there that if you all work very hard together and can get it done by 1995 or 1996 or 1997 I would coast to the year 2000. And some wag in that group, where I have voice but no vote, said "No way, because if we finish it in '95 and you're still around, you'll be back in Washington looking for a change." They're probably right. The program has not flown yet. Those of you who are like I am build a product that has to get up in the air and move around a little bit before we are sure that the drawings were right. You know that first flight is very important. When the program gets to the point of first flight all of you will be, if you will, the wind beneath its wings because you will have helped get it where it is. I think that we're going to have a successful first flight. But we're not going to have it if we just stand around and wait for it to happen. All of you must stay involved. All of you must make a valuable contribution.

I managed to go to a number of the meetings while I was here and I began to think, very pleasantly, that this was a meeting on the NISP because in almost every session that subject came up, either from the speaker who said that this was a NISP issue, or one of the people attending who said is this a NISP issue. And if it was about the relationship between the government or any of its agencies and departments and industry on a classified basis, then that is a NISP issue.

Admiral Inman addressed a very important subject as part of his presentation. And that was what I mentioned a little bit before, the technological leadership of this nation in the world. If that does not necessarily depend upon classified information, a great deal of effort is going to have to be put forth as part of the NISP for the protection of those special technologies. That is not, and I'm speaking from industry, that is not usurping any of industry's authority over its own information. What it is doing is emphasizing a partnership that exists between government and industry in making our efforts as a nation successful. All of you want to be a part of that.

I suspect that while we will have an implementing order for this effort by the beginning of 1992, I also suspect that we will run very close to Maynard's 1997 date. There is a lot of sense to that. We're going to find out that it's going to take a while to get all those details together. Probably more important than that is the training that has to be involved. Training at perhaps seminars like this. But certainly training on a first priority basis.

I was asked at one Industrial Security Awareness Council (ISAC) Meeting how do we account for great savings of money in this program. What's the industry balance here. How many of you as directors of security would want to go back to see your chief financial officer and say I'd like you to open up all the existing contracts that we now have with the government, to replace the DISP with the NISP. Where is the one courageous person who might be foolish enough to do that? You know when you reopen a contract the hole that opens there, the money falls out, so you don't want to do that. I think that the program which we have described, even when we spoke to OMB about it has something that would avoid costs, is more important than something that will save money. If you can turn on the imagination again and look at what costs mean. We know that the current program is doing this when it comes to cost and we go right off the top of the chart if it kept going that way. It was one of the things that was a driver that began to implement the NISP. But you must know, we are going to introduce something brand new with new forms, new descriptions, new training, it's going to do this and then come down to here. Some of that, hopefully, will be accomplished by the reallocation of costs, or reallocation of funding inside agencies. You can move money here when the responsibilities may have diminished over to here where they have increased. But that's a challenge. There are 11 working groups. They reflect pretty much the 11 elements of the program as it was first described in 1988 which is something that all of us should be pretty proud of. It means that we came close to the target right from the beginning. Your continued support is needed.

You will note from some of the charts that industry's role will not end at the development of a program. It participates through the implementation of the program and throughout the life of the program, industry will still continue to play a role in the modification, in further development, in the correction of the areas that need to be corrected. We are looking forward to it. We are looking forward to a continued relationship. It sure has been one hell of a good time the last three years.

Jack Donnelly

We are in total support of the NISP and I agree with Harry that it will be one program. I see it as being one program with two levels of stan-

dards, one for collateral and one that will cover sensitive compartmented information (SCI), Special Access Programs, and energy matters. We already have in the Defense industrial security programs which is by far the largest, prestandard levels of security for collateral. And I think that we are responsible for many of the thousands of other industrial security programs out there since we are responsible for creating many more special access programs. It may appear as though we made a brilliant stroke in defense last week when as Art Fajans indicated, industrial security was moved to C^3I and special access programs were kept in policy. I don't see it as a contradiction to what we're trying to do, because accomplishing what we're trying to do is to depend on the good will and intent of the senior managers in defense who run to these program and I assure you we are all supportive. It's time has come. It will be accelerated because of the reduction in our budget and, therefore, a need to approach this job much more sanely and cost effectively.

Art Fajans

Thank you. I understand that you all have a handout that I'm throwing up there. This is how we're organized. As was mentioned, I am the executive secretary to the steering group. I think it is important to know that I'm in that position not as the Director of Secretary Plans and Programs but as Chairman of the National Industrial Security Advisory Committee which is made up of all of the 20 non DoD user agencies, plus it already has as observers from CIA, DOE and industry. So the nucleus is also there in NISAC. It is through the NISAC that I am able to continually keep the rest of the executive branch informed specifically on the progress of the NISP. The most remarkable aspect of the NISP, in my opinion, is what has already been accomplished under what I'll call the philosophy of the NISP. We're not in a position to say all right, this is what we've done so far, one, two, three, four, five, and six. We're not at that point yet. So a lot of things have already occurred that I believe would not have occurred were it not for the concept of the NISP. The single scope background investigation, I think, is the principle example of that. This was an initiative that started many, many years before the NISP. The fact that the NISP is in being and has the attention that it does have makes it absolutely clear to me that it has accelerated that process to arrive at the single scope background investigation. There are many other examples that I could point to which are already being positively influenced by the philosophy of the NISP. So because you're not seeing rule No. 1, rule No. 2, rule No. 3, don't lose heart. Things are happening and they're happening in a positive manner. That's all I have to say. The other panel members will continue from their points of view.

I'd like Larry Wilcher to give us a perspective from the Department of Energy.

Larry Wilcher

Let me say first that it's an honor to be here today representing the Department of Energy especially on the subject of NISP. To dispel any rumors that you may have heard, the first thing I'd like to say on behalf of the Secretary of Energy and the Department of Energy is that we remain committed to the successful completion of the NISP. The future of industrial security, I think, is bound in the philosophy that you see within the National Industrial Security Program. To that end, ongoing as we speak right now, the Department of Energy is relooking at all the safeguards and security policies to bring them more in line with other government agencies to make the transition for the Department of Energy to the NISP philosophy and the requirements and regulations that are developed. As Maynard said in his letter, he right now is out addressing the directors of the national laboratories within the Department of Energy. We have had various meetings within the Department of Energy bringing up to speed our NSIE which is our contract and industrial organization for security. All the operations offices have been briefed. The Department of Energy under Admiral Watkins is currently undergoing a large philosophical change and the NISP is going to assist in that. This week I've heard a couple words such as cautious optimism, patience, and credibility in industrial security. I think these are good words, but I think the one word that probably comes out most within the Department of Energy is patience. The NISP is going to bring about a change in 45 years of philosophies in the conduct of business. Changes in philosophies don't come about over night. One of the things we've done within the Department is we've gone throughout the department to all our facilities and tried to sell the NISP. We are 100% committed to a single government wide industrial security program. The Secretary of Energy has committed resources, not only through the office of Safeguards and Security, but from the Office of Military Applications which deals with a lot of our interna-

tional bilateral agreements, and the Office of Security Evaluations who is our oversight and compliance organization. Every day you'll find DOE representatives attending meetings and trying to break down barriers in order to accomplish this single US government and industry partnership in a single industrial security program. What I do as far as cautious optimism is, I tell everyone that the Department of Energy operates under the Atomic Energy Act which is a public law and one of the things that we move cautiously on when we work on the executive order and the National Industrial Security Program Manual (NISPOM) is assuring that we do not intercede or override any types of public law. However, as I go out and speak across the DOE complex about the NISP when I hear such phrases as well we can't do those type of things because of the Atomic Energy Act, I challenge those people to go to the Atomic Energy Act and point out the prohibitions against the concept such as the National Industrial Security Program. As a matter of fact, in the opening words of the Atomic Energy Act it charges the Secretary of Energy with protecting nuclear weapons design and Restrictive Data consistent with the national defense. I think those very words amplify the philosophy of the National Industrial Security Program. Again, I think the future of credible Industrial Security lies within the definition of a National Industrial Security Program and I emphasize once again that the Department of Energy wholehearted supports this concept. Thank you.

Frank Ruocco

I'll mention a couple of things. A couple of general comments about the NISP and then some specific comments about the personnel security side of it. I co-chair the Personnel Security Committee of the NISP. I just want to give you some words as to where we stand there and what the prognosis is for the future.

First, it seems to me that this is probably one of the most opportune times to try to effect major substantial and significant changes in the security/ industrial system of the United States. First, of course, is the cost savings or as Harry indicated the cost avoidance. The incentive is there to save money. It has been clear to us for the last few years in the agency, that costs have gone down. Certainly they are not growing at the fast rate of the '80's and barely keeping pace with inflation during the last few years. With projections going on, these aren't much better than what we've seen over the last couple of years. So the economic incentive is there. Not only for us but I'm sure for everyone in the government. The other incentive is, I think, the changes that have occurred in the world over the last couple or three years. Tiananman Square, Berlin Wall, fragmentation of the Soviet Union more recently Yugoslavia. All of these things have demanded change in the intelligence community, change in terms of priority. We are still wrestling with how to react to all of this. And now it seems to me, is a good time to think of other changes we need to do in our business. Having said all that, I would endorse what you've heard from other people during the last couple of days. Also, be a bit patient. We're talking about turning around more than four decades of, as Larry said, philosophy, practices, and procedures as well that are based as much on folklore, intuition, and good old plain gut feeling, as anything else. Those are hard to change overnight. They will change. I think they will change significantly. It will take some time. What you will see are incremental changes. Not a one turn key operation by any means.

Speaking for the agency itself, I can say the present DCI and I'm sure the new DCI is committed to this program. I, in the Office of Security know that we have more than 20 people now involved in the NISP, giving about 5-25% of their time on the NISP. That's truly a significant investment for me. Particularly since I have to lose about 200 people over the next few years to cut down on the slots. When you put that much investment in something, you expect some output and I think we will see some output as a result of that investment.

Let me give you a couple of words on where we stand on personnel security. We are very close to establishing one minimum set of standards for background investigation. We have almost a unanimous agreement across the government and within the intelligence community, almost--not quite. Almost unanimous agreement on what the minimum standard should be for a background investigation. I believe we'll have that within the coming months. We have made significant progress, thanks to Pete Nelson of DoD on establishing common adjudicative standards. We probably will reach some agreement on that within the next several months or year. If we reach common agreement on what the standards should be for background investigations and for adjudication, it should be relatively easy for us to come up with a single set of forms that are needed to be

filled out and used by industry and by government. We're getting there. We've made significant progress, we believe, on getting rid of a number of forms and narrowing down the number of forms we will need. We probably accomplished about 80% of what needs to be accomplished in the forms world. That last 20% of work will probably demand about 80% of our effort.

Lastly, we've done a lot of good solid substantive discussion on due process. We will not have one single means of due process. We've agreed to have two sets of due process. One process is what we use for the DCID 1/14 standard, that's the appeal process. On the DoD side will be the trial type appeal process. We think we've made significant progress. Not one thing is nailed down yet. Art said the SSBI and the incentive for the SSBI has been around a long time. That's very true. I think he's right. Putting it all together in the NISP has given momentum to bring it to closure as soon as possible. I think we will do that. It will take some additional effort to bring these others to some meaningful conclusion. I'm fairly optimistic over the long run, but not in the short term. Thank you.

Steve Garfinkel

Luckily, everybody has said everything about the NISP that has to be said, because I didn't have anything to. . . I have old business. I'll try to go through it quickly because I know that everybody wants to go home. First of all, the results of the first competition for the Information Security Oversight Office (ISOO) cup. The final score was government 81, industry 63. The cup will be inscribed to indicate that at the event sponsored by the NCMS, government was the winner. I'm certainly hopeful that we'll have lots more occasions to compete for the ISOO cup. Incidently, the winning margin was less than one 25 point question. So if just one 25 point question had gone the other way industry would have been the winner. Something very much to keep in mind. More importantly than that is that, as stated, the goal in doing this competition was to restore the hostility between government and industry. It was achieved, let me tell you. I have been accosted over and over today by people who work for industry telling me that I asked government all the easy questions.

One last item, and that is, with respect to the NISP, I think by next year that the seminar in Dallas/Fort Worth, the one thing that you will definitely know about the NISP and know that it's not going backwards is that I think we're going to be talking about the Bush executive order on national security information and the national industrial security program. Because I think well before the program next year, that will have been signed and we will be well on our way to implementation. Thank you very much.

Questions

I think many of us are aware of the extensive amount of time and energy that has been put into the NISP so far and I was a little discouraged to hear Admiral Inman's comments on Monday that he's not necessarily encouraged that this isn't another attempt on behalf of government and industry to formulate a program that won't be successful in its implementation. What are your comments about that?

Harry Volz

Personally, I had the opportunity to brief a number of government officials and in a couple of those interviews or briefings, there were similar concerns. The fact that perhaps industry had delivered something to the door of the White House again and then after everybody thought it was great, industry would walk away from it and it would die. More than one person, and I would not be surprised that Admiral Inman said that because he has personal experience with similar efforts earlier in his career, trying to bring order into the industrial security program. The difference is that industry is not going to walk away from this and neither is government. There is a little different incentive. The cost incentive is probably the least altruistic. The position of the nation in the world is probably the great driver. So I think that this is something different. If you want to think about support, early on we thought it would be good in industry if we had high level support from our own leaders. We asked the AIA if they would form a group of chief executive officers of leading companies in the nation for support when we needed support. They agreed. There are a half a dozen from leading companies who are standing by whenever they need help. One for instance, when they briefed General Scowcroft, Norman Augustine accompanied me to the office. You think that doesn't lend weight to how industry feels about this program, you're wrong. I think if Admiral Inman could see what's been done even in the last year and a half he might feel differently. But if we let the

opportunity slip away from us, it will never come again. So we cannot do that.

Jack Donnelly

I'd like to add to that. I know where Admiral Inman is coming from because I've sat on a number of national committees in which we thought we had reached concurrence as we did with the single scope. It came out of the Justice Department, we sent it to the White House in 1987 and it's stayed in there ever since. The difference between this and many other national committees that I know about and participated in is that the pressure for this is coming from the top down, not from the bottom up so that the secretaries and the administrators of the agencies will be getting their guidance from the White House and not from people who are protecting their rice bowls from inside their own agencies.

Question

All the events that have happened so quickly in the last year and I'm sure the panel is aware of this, but in some of the discussions that I've heard take place among the members, it seems like what we're doing in the NISP is we're consolidating what we have. We're taking advantage of the most positive aspects of the existing programs, but one concern, if you would just address it, I'm sure it's a concern that you all have, too. When things happen drastically the other way, are we by somehow getting involved in this NISP making ourselves more vulnerable from a national standpoint. Are we consolidating too much that perhaps we may not be able to respond if there is a greater threat instead of a diminished threat as some people may perceive?

Jack Donnelly

I don't think that standardization and consolidation are the same thing. We're developing standards. And once there's an executive order which tells the departments and agencies of the government to follow those standards, then the departments and agencies can administer them themselves. But they must adhere to it with oversight. Probably coming out of Steve Garfinkel's job. So that's not consolidation.

Frank Ruocco

I don't think that one should assume that commonality means the lessening of security practices or standards in any way, shape or form. For example, I'll go back to the single scope background investigation again. Although we have reduced the scope of that from say 15 to 10 years, we've added some things into those minimum standards, like a mandatory subject interview which we in the CIA never did before. So I think overall, across the government, you will probably have an increase or enhanced security posture compared to the way it was before.

Jim Linn

Gentlemen, thank you again for appearing and we appreciate your insights. ■

ABC'S OF AIS SECURITY

24 June 1991

George Hall, Consultant

Remember this is the ABC's of AIS Security.

Actually, when you get down to computer security, AIS security, ADP security, whatever you want to call it, I don't think there is basic or advanced. It either is or it isn't. What we're trying to do today, is to give those of you who may not be familiar with the particular procedures, the Industrial Security Manual, involved with AIS security, a basic background in the work we're trying to do, why we're trying to do it and how we're going to implement certain, shall we say, problems with computer systems that present security vulnerabilities.

I'll just give you a brief background of where I'm coming from. You'll notice I move around. I cannot talk standing still. I think that comes from being five years in the Marine Corps from 1966-1971 and they taught me then that a moving target is hard to hit. Not impossible, but hard. I'm here, so it must be true. I've been involved in computers for quite some time. I built my first computer in 1966 as a high school physics project. I went into the Marine Corps and they gave me a machine gun which makes a lot of sense. At least it did to the Marine Corps. Since then I've gone to college and for about six years I worked for the Defense Investigative Service as an industrial security representative, a staff specialist, and then as an instructor at the Department of Defense Security Institute. When I left the Defense Investigative Service I went to work for the Computer Sciences Corporation and not surprisingly we did have a few computers that did certain work for the government, and I've developed, I think, a relative understanding of what DIS is trying to present to contractors in order to get systems approved for processing classified information.

A long time ago, I remember one thing that came out and it's been talked about quite often. It's the paperless office. The only thing that I've noticed about computers in reality is that they allow more paper to be generated in a shorter amount of time. Those of you who are dealing with the output products of computer systems realize that quite well. As far as computers go though, and security--you might say computer security or AIS Security is another one of those military intelligence kind of words--the security situation with computers is no different than any other security situation you're going to run across. The main thing is not to be concerned about this box sitting in front of you. All you have to do is think of basic security principles, the security triad. How many of you know what the security triad is. There are three items in the security triad, personnel, physical, and information. Three things that we're concerned about from a security standpoint. People, physical security--how we lock things up, and information--the data itself. How do we protect it from disclosure, unauthorized personnel and things like that. Those three items are going to be used with computers as well as with any other security programs.

Now if you were developing a security program from scratch, you'd first have to determine what do I have to protect, how important is it, and how much of my resources am I willing to allocate in order to protect this information. Generally, you're going to do that with cost analysis. Well, dealing with classified information we don't have to worry about that because the Industrial Security Manual has already taken care of that for us. It shows different levels of protection based on what? The sensitivity of the classified information being processed. And how do we recognize that sensitivity? It's classified as either confidential, secret, or top secret. The government has already told us. Confidential is down here. We're going to apply resources to protect it, but we're not going to apply the same amount of resources as we would for top secret information. We're going to spend

more money, we're going to involve more procedures for the protection of top secret information because it is, hopefully, if somebody has done their classification management properly, it is more important than confidential. So we're going to allocate more resources to protect that information. As you look at security in general that's what happens, right? For top secret personnel security clearance what do you need as far as the investigation goes? At least a BI. For confidential what do you need? A NAC. What's the basic difference? The investigation is the bottom line in everything we ever do. Money. How much does it cost to do this? Why would we spend the same amount of money to process somebody who has access to confidential as we would for top secret. Doesn't make sense. So we're going to apply the same principles in AIS security. Depending on the level of the classified information involved, you're going to find different security requirements to protect that computer system while it's processing classified information and when that classified information is removed. There are three basic things we have to look at again. Personnel, physical, and information.

When we're talking about the physical security of the hardware, it's the computer system that is sitting there, it is just as important that we protect it when there is no classified information in the system as when there is classified information in the system. Why? Why would we want to do that? What's the problem. Say I have a pad of paper and there is nothing on it, but I'm going to write classified information on it. Would I have to protect that pad of paper? No. There is really no security vulnerability there. But if I have a computer system that I'm going to process classified information on tomorrow but there is no classified information on it today, it's just sitting there. What do I have to do with it? I've got to protect it. But why do I have to protect it? What is unique about that computer system that is different from that pad of paper? It can be modified. Some unauthorized person could conceivably, do certain things to the hardware and gain access after I leave it or while I'm processing. So we have to protect the hardware to preclude unauthorized modification of the hardware. In other words we have to have a warm fuzzy feeling that based on the vulnerabilities that we recognized with computer system hardware that nobody has modified this in order to gain access to the information that we are going to process.

How many of you own your own computers? Have them at home? Then you are familiar with how computers operate. What I really want to go over basically real quick is some of the things inside a computer. What are these things called? Chips. Actually, they are chips on a board. Silicon chips. I used to call them silly con for so long. But they are silicon as in Silicon Valley. What is silicon? Sand. Actually, this is sand with various impurities put into it so that these things can act like transistors. But this is really what computers are all about. I actually have two different kinds, if you will, make that three different kinds of chips on this board. This one is a ROM chip, read only memory. Actually it's an erasable programmable read only memory. I've got RAM chips, random access memory. And I've got a CPU, a central processing unit. What is a CPU by the way. What's another word for it? A computer. Basically speaking, the CPU is the computer. You've got a box, you've got all this other hardware, you've got wires coming out of it. That's just to hold the CPU. The central processing unit is, in effect, the computer.

RAM, random access memory, that's the memory inside the machine. This is today's technology. This is the way it is today and so this is what we're going to deal with. And the RAM, the read only memory. From a security standpoint what do you think is best for us? Read only memory. Now why would that be best for us from the security standpoint? What does it mean as far as the hardware goes? It is what? It's write protected. In other words I won't say somebody can't change it, but it's much more difficult to change the read only memory than it is to change the random access memory inside a machine. Why do we have read only memory? All machines, by the way, most machines, I'll say all machines have ROM. What is specific about ROM that is important from a computer standpoint? It's stable. You turn the power off, it still remembers what's in there. Whenever you turn your computer on, you see it do that thing up there, doing a RAM check and all this other stuff. Well it's getting those instructions from the read only memory that's built into the machine. Now security vulnerability to that is it can be what? It can be modified. If somebody has the particular expertise they can modify that so that it does things at startup. So from a security standpoint we have to protect the machine. Even though we turned all the power off and done all this other stuff, the ROM itself can be changed.

Random access memory is good from a security standpoint because it is generally what? Volatile. Volatile meaning what? Turn the power off and it's gone. You will find battery backup and sometimes it's a capacitor instead of a battery.

Now when we're doing classified information one of the things we have to do when we're done is to get rid of the classified information that's been in the machine unless we want to protect it to the same level as that classified information. Now generally for random access memory, you know the memory you have inside the machine 640k, and megabytes, whatever, all you have to do is what? Clear the machine or what's another way for volatile memory to get rid of it? Turn the power off. Now I say generally because, I'll give you a specific situation. I know that the Capital Region is working it on it right now. And it's all my fault folks because I'm the one who brought this up to them. How many of you use Mackintosh computers? All Mackintosh computers have battery backed up RAM. Unfortunately, DIS had not recognized this until last week. All of them have 256,000 bytes of information battery backup. That's a security vulnerability that has not been addressed before. It turns out that certain information in the system is maintained in what is called PRAM or pram which is the programmable random access memory and what happens with this is that certain information for systems setup is stored there. So that is battery backup automatically on the machine. And that's something that's going to have to be addressed and people who are processing classified information, particularly or specifically those people who are downgrading and upgrading. That is, they are removing the classified information and protecting the system at a lower level of protection. If you have any specific questions about that, we can talk specifically about that after we're done here.

Under a typical ADP system we show a couple of things. We say system here or AIS system, because it's just not a system. It is just not the hardware although we do have the hardware. It also includes the software, the people, and the procedures that we have to take a look at as far as maintaining security. We're going to concentrate on the hardware and the software. As far as people go, generally those same rules apply. If somebody is going to have access to classified information, they have to be appropriately cleared and have a need to know. That's fairly straight forward.

As far as the procedures whether it's the company or government, the advanced workshop will go over the SPP and things like that. We're going to concentrate on the hardware and the software. This is basic stuff and I say basic although some of you are going to say hardware isn't really all that basic. But the protection of it is fairly straight forward.

Now those systems with the hardware when we remove all the classified information from the system, and we do certain procedures, we are allowed to protect it at a lower level. We don't have to store it in a safe, or a closed area, or a vault, or strong room. That benefits the company and benefits the government, because the government is going to have to eventually pay for whatever the company is doing. It's a benefit in the sense that we don't have to spend so much money. In other words our resource allocation or our resource expenditure is lowered. So what we'll want to do generally, is to try to remove classified information existing in a system. Now how are we going to do that? What is the basic storage medium for classified information these days? Floppy. Some sort of magnetic media. We've already talked about the RAM, which is the random access memory, inside the machine. But most of the classified information that we're going to be dealing with is going to be stored on some sort of magnetic media. Although not always. How many of you remember these things? I don't dare give these things away because you just don't find these any more. This is a program that I wrote in college. I don't remember what it was for, but it must have been real interesting at the time. I think, as a matter of fact, this particular program is designed to convert Fahrenheit to centigrade. It's quite a bit of information. Now the nice thing about this is it's what? It looks like a document. It's paper, you can hold it together and all this other good stuff. You can stamp it, this is secret. So it was a lot easier to deal with at the time as far as recognizing that this is classified information. After that we generally came into magnetic media. Why did we go to magnetic media by the way? Speed and capacity. I'll go mostly with capacity. Speed on the older systems wasn't that much different although today these magnetic systems are very fast. But speed and capacity, now with capacity we're talking density of media. Everybody familiar with what we're talking about when we say density of media? How much can you cram into as small an area as possible. From a security standpoint, what implications does that have for us? It's easier to take

away, steal, purloin larger amounts of data with less effort, maintaining it in a small space.

How many of you are familiar with the Industrial Security Manual? I thought there might be a few of you. I've got the Industrial Security Manual on two of these. And these aren't real high density media. On high density I can put the Industrial Security Manual on one of these. I've seen one recently which will hold eight or nine Industrial Security Manuals. And how many of you are dealing with a classified program that the entire amount of classified information for that program will fit on one of these. In other words somebody can destroy your whole program just by walking out of the facility with that in their pocket. How many of you do strip searches for people coming out of your facility?

We're talking about density of media. How much information can we pack in a minimum amount of space. And what that means from a security standpoint again is that more information can walk out the door. From a productivity standpoint it's great. That means that we can work with a lot of data. You can bring everything together, put it all on one disk. It's all right there, everything is available. It says for training purposes only. It is not secret. This is a red disk, for training purposes. You'll also see that some idiot put it right across the shutter so it won't open anymore. When you're marking media, be aware of that. The nice thing about this is that you can mark this just like you can the cards. You can put all kinds of nice good information on it, the entire classification, declassification instructions, all that good stuff. Again the bad point is that you can put it in the wrong place, the engineers will be upset with you.

Now we're talking density of media. This is what kind of media? Rigid or non-rigid? It's non-rigid, why? Because if you open it up you'll find this is what's inside. It's floppy, flexi, non-rigid. I like to use rigid and non-rigid. That way you get away from floppy and hard. And this is why you call it floppy media by the way, because it does flop around. This is from a 5 1/4" disk which is one of these things. These have been around awhile. This is a 3 1/2". Which holds more data? Generally this one will hold more data. Why is that? Because although it's floppy, what happens is the case here is rigid so it holds it steadier where this has to flex a little bit and what happens with the read and write drives, they have to account for movement. The more solid your media the less they have to account for movement and for error detection and therefore they can pack more information into a smaller amount of space.

We also have a hard disk. This used to be rigid media before we sandblasted it. There used to be a magnetic coating on this. You'll notice if you take it apart, it is about the same size as a 3 1/2". This will hold, generally, about 40 or 50 more times of information. Again, rigidity allows the read and write heads to move in a much smaller, exact manner, so therefore you can put more data in the same amount of space.

From a security standpoint, I've got one other, bernoulli cartridge. You open it up and you'll find you've got a floppy inside there. Again, by its design, when it's spinning at high speed, it flattens out. But again, it's still floppy media. Now we're talking floppy, non-rigid, rigid. From a security standpoint, Industrial Security Manual, what is the significance between rigid and non-rigid media. How we do what? How we dispose of it. What we have to do in order to get rid of it. Why would we want to get rid of it? Eventually everything has to be gotten rid of. Unless you plan on keeping the contract for 20, 30, 40 years or whatever. Eventually these things will wear out, by the way. How many of you had a hard disk crash on you? You've very fortunate if you never had one crash on you. But floppy disk, rigid media, or any kind of magnetic media is eventually going to fail. And when it fails, catastrophically sometimes, we have to destroy it.

Now there are various ways that the Industrial Security Manual allows for the destruction of media. Most recently, however, they have become much more flexible, I should say much more non-specific about that. The new Industrial Security Manual says to do what? Check with your COG office. Keep the old manual so you don't have to ask them stupid questions, is what I'd say. They'll say, "What do you mean how do you get rid of this, don't you have the old manual." One of the reasons that they changed that is that there are different types of media coming on line and they don't want people using the wrong way of destroying, declassifying, classified media inadvertently. So they want you to go to them and say this is the kind of media I have and this is how I proposed to destroy it to get rid of it. Now floppy media, how do we destroy it generally? You could shred it, you could degauss it I heard. What's degaussing by the way? Having a strong magnetic applied over

it. How many of you are familiar with the Perry Mason show? Well, that was one of the first times I ever saw degaussing. Do you remember that particular program. This is the guy I want for my lawyer. Perry's got a client. Client is accused of murder. They've got a tape. Not one of these kind of tapes. Of course, Perry used an old style tape off one of these tape records. A tape like this, similar to it. And supposedly there is some incriminating evidence on there and Perry says to the prosecuting attorney, Sir I think that's been spliced together. I want to take a look at it to make sure it hasn't been spliced together. And Perry's standing there, they hand him the tape and he pulls it out and he's going through it, and says you're right, it hasn't been spliced and he hands it back. They come into court and they put it on the machine and start it up and what happens. Garbage. Why? He had a magnet in his hand. That's the kind of lawyer I want. But essentially that's the same thing with degaussing. Unfortunately, or fortunately, depending on your point of view, from a security standpoint in the industrial security program, what is specific about degaussing? You have to do what? Use what? Approved degaussing. Approved meaning that they have been certified that the magnetic field strength meets a certain standard for the type of media you're going to destroy. You have to tell them the type of media and you have to have the appropriate degausser. I'm not real familiar with what NSA has approved recently, but at one time they were saying that high energy media can not be degaussed. They are still saying that, I believe. If you can't degauss it what's another method of getting rid of it? You can always burn it. I still think that's still the one thing you don't have to have prior written approval from the cognizant Security Office in order to destroy stuff, right? There is a problem with burning this stuff though, what's that. Yes, EPA will object. Because these will give off toxic fumes. Anybody ever been in a fire with a tape library? Firemen do not like that. Something about their health insurance, their longevity, and that kind of stuff. These can give off toxic fumes so before you start burning this stuff and get cited by your local fire marshall, the EPA, whatever, you might check and make sure that's legal.

Degaussing, burning, there's a phrase they'll use overwriting. Why don't we just overwrite this? That is put unclassified information on it. You can go below layers. Who knows about this firsthand? He lives not too far from here? Or he used to, I think he's in New York now. Nixon. When did he find out about this? Depending on who you believe, what was it, 18 times, it was magnetic media on a dictaphone and a certain company outside of Fort Meade was able to recover some of the information off those tapes even though it had been overwritten 18 times. The reason for that, at least according to NSA, is why NSA does not allow overwrite of nonrigid media in order to destroy the classified information, in order to make it unclassified, is that you can go down layer by layer by layer by layer. An infinite number of layers is really what they're saying when they say you can't overwrite it period. I think you're going to find, or they will admit, that you're going to have a certain degradation of the ability to recover information that goes down layers, but they say they can still recover it. Especially the digital information as opposed to analog information as on the dictaphone tape. So we're not allowed to overwrite this in order to destroy it, to make it unclassified. But we can do that to what? To clear the media. If we're going to clear the media all that means is that for nonrigid media we do a one time overwrite and it's clear. Why would we want to clear the media? We could then use it for something else. We're all cleared, why would we want to do that from a classification management standpoint? Need to know, but what are you required to do upon the completion of a contract? Destroy, or get rid of, or make proper disposition of all classified information received under that contract. Now you could just go through and shred, burn, or whatever all your floppy media referring to that, but another way is to just do a one time overwrite. If we do a one time overwrite on floppy media, is it still classified? Yes. But what have we done? We have accomplished what? Have met the requirement to make proper disposition on all classified material received or generated under the contract which we no longer have. If we've got engineers what's going to happen? They're going to request retention authority. Because if you don't, I'll keep my set at home and I'll still have it anyway. Hopefully, they don't have it at home. Of course they don't have it at home. When's the last time you checked one of your engineers at home by the way?

One thing I found with these is that you can get them with colored little pieces of plastic and you can do the same thing with other floppies. One organization I was working with at one time said we'll use, say red, for all classified information. And it is illegal for anybody to have a red disk that isn't classified and you can't bring red disks in and you can't take red disks out. As a matter of

fact, it got to the point where they said you can't bring any disks in. Is that a good idea? It's the best idea. Because if they take something in they can copy it, take it home, work on it. Is it enforceable? Not really. But what are we dealing with when we say we have a personnel security program? What are we really saying? We expect what from people who are cleared? We're anticipating a certain degree of integrity on our personnel's part. What do you think the main thing is to preclude them from doing that? How can you do that? Briefcase search. But again it's the old stick it in a pocket and you're not going to do strip searches. I think the main thing you have to do is inform them of what the rules are. Most people, most, not all, are going to follow the rules if they know what the rules are and they agree with them and even if they don't agree with them at least they understand the rationale behind them. One of the biggest problems with my mother wasn't that she told me what to do. She would never tell me why. Don't do that. Why? Bam! I find it's much easier to get people to do things if you tell them why they should do it. So you don't just go up and say "you can't take this stuff home." Why he can't take this stuff home is that you don't have the proper facilities to secure the classified information at home. If the FBI catches you, you're going to jail. To give people some incentive and also some understanding of what the rules are as it applies to classified information. Particularly today, because I saw how many of you had computers at home? How many of you do work at home. Don't you wish you'd gotten rid of that computer? Sorry boss, I don't have a computer at home. It's either pay me overtime here or wait until tomorrow or after the long weekend. A lot of people have computers at home. Particularly your professionals are getting computers at home. Usually they are the same type of computer they have at work so that they can take the work home with them. Most of these people are now being divorced. They are having to sell the computer in order the pay the lawyer. So we're all going to get even eventually. But it's a potential problem and to mitigate that at least to an acceptable degree, is to inform people of what the rules are and why we're trying to enforce them.

Let's see. Hard disks. Floppy Disks. Talking about getting rid of, eliminating, destroying the information on them. Now with hard disks we do allow a what to destroy on there? Not a reformatting, No. Maybe we should talk about some terminology here. When you delete a file off one of these, delete it, it's gone, non-recoverable right? Because Norton Utilities and several other programs will undelete files for you. Not only that, if you say format the disk, is anybody not familiar what we're talking about when we say formatting the disk? That's setting it up in order to put data on there. The machine has to understand the format and the media has to be formatted in order for data to be on there. If you just format guess what Norton Utilities can do for you? It can unformat it. That's why you should all have Norton Utilities or something similar to it because you may have some disgruntled employee who thinks they are really going to fix you, they're going to get on your hard disk and say "format." It formats a disk and suddenly it looks like there's nothing there. With something like Norton Utilities you can unformat a format. You're still possibly going to lose data, but it's possible. So formatting does not necessarily destroy the data on there. Or delete does not destroy the data because all it does is it changes the directory and says you can now use this space, but it doesn't go through and erase or overwrite the data existing on that disk.

In order to destroy the data, the Industrial Security Program requires for rigid media a three time overwrite of that media by alternating binary high, binary low, and random alpha numeric character. Random usually turns out to be an "H" in the particular program I used to use. Just puts all H's all over the disk. What's the problem for doing that for one of these things though? Time. It does take awhile. Even a 20 megabyte hard disk will take time. There are some other problems you'll have to be prepared for when you're doing this. Right now the Defense Investigative Service, before they will allow you to overwrite a hard disk, they require before you go into classified service to have a map of that disk. A map meaning that you have to be able to show where the bad sectors, bad clusters, or whatever are. What do we mean by bad sectors or bad clusters? That a portion of the disk of the magnetic media for whatever reason is unusable. Now the disk still works. But for whatever reason a portion is bad which precludes the secure writing and retrieval of data. When these hard disks are usually mapped out by the manufacturer in order to find those and you can usually find a little tag affixed to the hard drive which is inside the machine which saves you a lot of good, in order to look at that and see what those bad sectors or clusters are. You have to have that map available so that you'll know where data could not have been written to be used for classified.

Another problem is that once you've been using it sectors and clusters can go bad. Now if you put classified on one of these hard disks and then a cluster or sector goes bad, you cannot overwrite it in order to destroy the data. By going bad all it means is that you can not reliably read or write to that cluster, not that the data is unrecoverable anymore. So what you would have to do before you could do an overwrite in order to destroy the data would be to do another check using something such as Norton Utilities to find out where the bad clusters, sectors or whatever are at this particular point in time. Compare that against the previous cluster report and make sure they are the same. If they are not the same anymore you're not allowed to overwrite.

Again, the reason is when Norton Utilities starts doing the write, it can't write to those bad sectors. So it's going to skip them. So you're not going to have a way of finding out if classified data is existing on those bad or unusable clusters. Once you do the overwrite, assuming that all your steps check out, what are you also required to do? Verify it. You have to verify that that information was indeed overwritten. How are you going to do that? Can't do a directory because what we're requiring is that you look at the disk. Read the information on the disk. And something such as Norton Utilities will do that. You can read it cluster by cluster. It doesn't say you have to read all the data. Thank God. But you do have to take spot checks around the disk, different clusters, different sectors, to assure that that has indeed been written. Any questions on that? That's the general way of destroying it. How about physically destroying it? What's wrong with physically destroying a hard disk? You have to pull it out of the machine. You have to be somewhat technically competent in order not to mess up the rest of the machine. But assuming you don't care about that, it's not really difficult to smash one of these things open and get to the magnetic media. Once we get the media removed, how do we get it off this metal plate? You can sandblast it. What's another way of doing it? Acid. That was my favorite a long time ago when I was with the Industrial Security Program and this was back when they had chrome bumpers. Before they came out with plastic, you could find a chrome shop every now and then where they would rechrome bumpers or whatever. They generally had an acid bath and every now and then you could call up and say I need to get rid of this and go down there and show them how to do it. Not with their hands. They'd have something to dip it down in there and bring it back out and you've got a nice shiny piece of metal. It's gone. How about sitting there with an emery board and taking it off? Would that be acceptable. I'd say generally it might be acceptable, but it's a lot more trouble than it's worth. In all of these procedures we'd have to have the approval of DIS because the only thing we don't have approval for is what? Burning, and this doesn't burn very well, I guess you could go to Pittsburgh and dump it into the steel mill foundry. Any other ways of getting rid of the data on this? I'm sure we could think of something. The main thing is to get rid of the magnetic coating. How about degaussing this? Could we do it? In order to degauss these things, you have to dissemble the disk drive because the disk drive is hermetically sealed. You've done what? You've really destroyed the disk drive unless you're technically competent to put it together. And where do you put these things together? Clean rooms. What if your hard disk crashes and you've got classified information on there and it's your only copy? You haven't copied anything else. This is it. This is your whole program, the project you've been working on for the last five years. Your company is about ready to deliver and the hard disk crashes. You can't access it anymore. What do you do then? Get your resume out before you tell the boss. There are cleared companies which are authorized to receive media such as this and try to recover. I say try. Depends on how bad the crash is. Generally at least a crash will damage some of the media. But there are companies in some government facilities which have the technical expertise to dissemble these things, hopefully correct them, and at least try to recover the data off of them.

There are cleared companies, companies that are cleared for nothing other than doing this. Generally they are not just in the business just for classified, what are they really in the business for? Corporations assistance, because corporations make the same mistakes everybody else does. They fail to backup, the hard disk crashes. There is really more unclassified data out there then there is classified, although some of you find that hard to believe sometimes. So we do have at least the possibility, if you do have a major crash and you've got to get the data back off. Contact DIS. They will generally be able to tell you how to get to somebody in order to try and recover the data. Again, that's only a try. When I say try that means you should have done what to begin with? Backed it up. Put it on some other media. Some

other form of protecting this information. Again that's just common sense from a business standpoint. If we back up classified data it is what? It is classified.

How many of you are in a situation where you're using hard disks as a, how shall I put this, you're using a hard disk, your system files are on it and your applications files, but you're telling DIS that we're not going to put any classified information on this thing, we're going to put all our classified information on this kind of media. Removable media that we can take out and put in a safe. How many of you are involved in that situation? How many know you can do that? DIS will allow a situation where you are allowed to use the system and the applications on a hard disk and use only removable media for the classified information. There are several caveats with that. One of the caveats is that this hard disk must be what? It must be write protected. In other words you have to have some means of assuring that even accidently no classified information is going to be written to this disk during classified processing. How are we going to manage that? How do you write protect the hard disk? It's inside the machine. Ok, there are two ways of doing it. Hardware and software. Do you know if DIS is still promulgating Protect Com? They are. There is a program out. DIS at one time would give you a floppy disk with Protect Com on it. Why won't they give anybody any magnetic media any more? Viruses. Just in case there's a virus on it or somebody said there was a virus on it. They don't want to be involved with any litigation about loss of data or whatever. So generally, you're not going to get anything on floppy media directly from the Defense Investigative Service. But Protect Com will tell you can use a program which I believe was developed by Lockheed or somebody like that called Protect Com which, when you run it, locks out the write interrupt to the hard disk. By doing that, it is essentially software write protecting the hard disk. What's the problem with a software disconnect? It can be modified and also defeated by another piece of software. As a matter of fact with Protect Com comes UnProtect Com. That makes sense. If you're going to protect something you should have some way to reverse what you've just done. Running Protect Com and doing what periodically? Checking your system, verifying that it's functioning properly. You've got to do that for any kind of software disconnect. In other words you can still use the hard disk in your machine. You can use the system, you can use all those applications because these days some applications require what? Nine or ten of these things. Anybody ever been involved in disk swapping. Please insert disk 16. Please insert disk 15. Please insert disk 8. That's disk swapping. That's what this allows you not to do. It makes you more productive. And that's what we're always talking about, productivity. Speed, we want to get some good use out of this machine that cost us $2,000 or $3,000. So there are ways of software disconnects. I mentioned Protect Com. There are other programs that can do essentially the same thing. The bottom line again is you have to have to have who's permission to use them? DIS. And where will that program, the use of that program, software disconnect be reflected? In your AIS SPP.

You can also do a physical disconnect. A hardware disconnect. How would you do that with a hard disk? We're talking about while its on line. You open up the box. You can unscrew it. I like cutting. That's permanent until somebody comes along and splices it. You can do a physical disconnect by cutting, disconnecting, removing the write wire. There is a write wire and read wire. It's a good trick if you know which one. As a matter of fact I would much prefer that instead of just cutting it because if you just cut it what happens? You can't change your mind until you go back in and splice it back together. But you could put a toggle switch on that wire. Stick it between there. Flip it for write, flip it down for write protect. What we're talking here is the ability to use these applications, this system, take the classified material out on removable media, put that media in a safe and not have to physically protect that hard disk while it's in the machine. What if we said we're just not going to write anything to the hard disk? We're not going to do it. You can trust us.

What's one of the big problems with various types of software you're going to find out there. There's a thing called scratch file, temporary files, hidden files, whatever you want to call them. Certain programs used these days look for a piece of media to store this on. Especially the large programs. MicroSoft Word for instance. On the Mackintosh or on the IBM, automatically makes a little scratch file on your hard disk in case you have a crash you won't have lost all your work so it can recover, it can remember certain things. Also there is a thing called Disk Casher. We already talked about Random Access Memory, the memory inside the machine. It's possible these days, not only with some programs but in some

entire systems, that the system itself is going to use the hard disk like it was RAM, like it was part of your Random Access Memory. So you've only got 640k of memory inside your machine, this can make it believe it's got 20 megabytes or whatever depending on the type of system. And what it does is swap information out of that Random Access Memory inside the machine out of the silicon memory and puts it on the hard disk. It only keeps in the RAM what you're using right then. You can only see so much on that screen anyway, right? Let's be honest there's not a whole lot of information you're getting directly from the screen. So we can put some of the information that you're not using right now on to the disk. So it pretends you have more memory than you really do have. You won't even see it. You won't even know what's going on. It doesn't say "By the way, I'm writing to the hard disk now." What's one way of spotting that if it is? A lot of the machines, not all of them, have a little light that comes on when the hard disk is working, or the floppy disk or whatever. Mackintosh's don't do that. At least in some of the system. So you can't trust it. So you've got to disconnect that if you're going to have a protected system.

When we protect that system, we've taken all the removable media out and stuck it in the safe. Do we have to physically protect the computer sitting on our desk? Yes, we do. Why? Because of the possibility of what? Sabotage, I'll go back to the phrase unauthorized modification. Because ordinarily we authorize modifications. So we want to preclude the possibility of unauthorized modification. We're not going to totally be able to preclude that. If you take a look at the handout with the little computer diagrams on it, you'll see that we've got a little system that shows the central processing unit, memory, input, output and what not. These diagrams were put together by a gentleman by the name of George Orstead. You'll see that we've got some bugs in the system. And what these bugs indicate are vulnerabilities. That's all. There's a possible vulnerability there. There's a potential for a problem. Not necessarily is there a problem but it's something that we have to address, have to think about, and put procedures in place in order to mitigate the danger of those particular vulnerabilities.

There is one device that from a security standpoint you should be running screaming down the hallway. The modem. How many of you have modems hooked up to classified systems? If you've got a modem hooked up to a classified system what are you essentially telling somebody? What you're going to be doing what with that classified system? You're going to be telecommunicating over what kind of transmission lines? Well, generally it's going to be a telephone line. Because that's what a modem is for. If you're just going to hook one computer to another, you wouldn't use a modem generally. You'd use hard wire to run a cable from this one to that one to use some sort of local area network which is not using phone lines. The modem tells us that we're going to be using a phone line. What is particular about a modem? Why do we have to have a modem for one computer to talk to another over a phone? Why don't we just take the wires from the telephone into the back of the computer? The difference is the type of system that we have. A telephone system here in the United States is an analog system. It uses a sign wave carrier in order to transmit the information. Computers that we're using, most computers that we're familiar with are digital computers. And the information, the type of electronic signal from a digital computer will not travel over an analog line. So what a modem does is modulate that digital signal into an analog signal so it is compatible to travel over a phone line. When it gets to the other end it takes that analog signal, demodulates it, turns it back into a digital signal so that a computer can understand it. That's really the only reason we have modems. In France they've now got a completely digital telephone network. So they hook the computer up directly to the phone line and send it out. They don't need modems. If you've got stock with Hayes or any kind of other people who are making modems, be aware of that in case we ever go to a digital network. Why are we not likely to go to a digital system here in the United States any time soon? Money. Bottom line as always. Because a digital phone system is better, it's faster, it's more secure, it's cheaper, it's more reliable, it's clearer, but we've got the analog stuff in place. It would be billions and billions of dollars to replace it and the telephone just isn't going to do that anytime soon. Unless you pay for it. You can pay for digital lines. They will run digital lines for you, but you're going to pay for it. So that's the purpose of a modem.

Now if we're talking transmission over telephone lines, from a security standpoint what are you going to tell people flat out? NO. Why no? Because a modem does not do what? It does not protect that information in any way. Now if I say I have an encryption scheme on my modem, it will

encrypt to DES standards. NO. What if we're going to transmit classified information over any kind of unprotected line, what must that line be? It must be physically secured or the transmission itself must be encrypted to what standards? It has to be encrypted to government classified standards. There is an NSA specification out which says what those specifications have to be. It used to be if you wanted to get some sort of encryption equipment in order to do that, how long did it take? A year or two years, three, maybe never. Because you had to procure that kind of equipment from NASC through who, usually through your contacting office, they had to sign off on it, the stuff is expensive to say the least. And there wasn't that much of it lying around, so generally you didn't have too much of that. What do we have today that it's changing a lot of that? STU-III. How many of you have STU-IIIs hooked up to computers? Why do you do that? Why don't you send them a letter? We all know, speed, volume, immediacy of passing information back and forth. Now there are some specific problems involved with a STU-III in using them to transmit classified information from one computer to another. What is that particular problem? You have to know who you're talking to. All your STU-III knows is what key is stuck in and that key says what? The person has a secret, or top secret clearance. It doesn't say who they are. Doesn't say if they have a need to know for the information that may be coming over the system. It doesn't tell you a lot of stuff. You could be sending information to somebody who doesn't have a need to know. Maybe not the proper briefings or whatever. So we require some sort of positive identification, right. And how do you get positive identification from one computer to another? You talk to them first. "Is this you, Joe?" "Yeah, it's me." "OK, I'm going to be sending you classified information." You know what I'm talking about. Can't tell them over the telephone specifically unless you're in what? Secure mode as far as classified goes as long as you maintain the proper level of discussion.

Is there anyway for unattended processing for the STU-III, that is computers talking to each other all night long when nobody's there? When we're talking STU-III unattended processing, there is only one company that makes a STU-III which is authorized by NSA for unattended processing. I think it's AT&T, don't quote me on that. But you can get a special STU-III which is designed for unattended processing. It's a very complicated machine and it's very expensive. So far it's relatively rare. Otherwise, you have to have people there, point to point, transfer the information, shut down the system, whatever. Even if it's in a closed area and you have a STU-III hooked up. They are not authorized for unattended processing. They have to be in use under the control of properly cleared, need to know, authorized persons.

How many of you have problems with viruses? You heard that viruses were mentioned this morning. Jim Linn's not here. I came in Thursday, looked at Jim Linn's computer in his house, turned it on, stuck in my virus disk, virus protection disk. I call it my virus disk, people start freaking out. Ran a couple programs and just about every file on his system was infected with different types of viruses. I removed all for him free of charge, since he let me stay at his house. Viruses these days are generally nondestructive. I'll say generally nondestructive because people write viruses, write these programs that attach themselves to your data or your programs for various reasons. The most prolific viruses right now are those "nondestructive." They say nondestructive, that's a misnomer really. They're not intentionally destructive, but people writing these viruses are generally not what? Not really good programmers. If they were really good they would be writing the programs to get rid of these viruses, making a fortune at it instead of just passing things around that "infect" systems. Because they are not well written they sometimes do things inadvertently like crash the hard disk. Which is not fun. Other programs are destructive. They are intentionally destructive. We don't have five or six days in order to go over all the different viruses that have been identified. But viruses generally run into a couple of categories. I think one of the most deadly is the Trojan Horse. Generally what we're saying with a Trojan Horse, what does that do? It comes in disguised as doing something that you might want to do, but it's really going to do something else. I think the best example of that is what's called the AIDS Staff virus. That was essentially on the Mackintosh a Hypercard type virus, a Hypercard program which supposedly let you know all about AIDS and all this other stuff, how people contracted, how it spread, where the centers of AIDS infection is right now. But it really did when you ran it was it sort of put the screen up and it was overwriting your hard disk. Which was not a real nice thing to do, all things considered. But that looked like one program that was going to do something and it did something else. You also have to be careful of any kind of sexy programs

because they are really likely to have that particular situation because guys are guys and guys are usually doing this stuff on computers and that is a potential avenue to get information in there.

How many of you preclude running non-company software on your systems? You can't bring in anything from home? Anything not bought by the company. That's a good policy. How are you going to enforce it? Check their disk. What if they bring it in on a floppy and run it and then put it back in their pocket? Well, if you have a policy, you have to trust up to a certain point. If you're going down the hall and you hear bing, bing, bloom, you may know they are probably not using the company software. There's an Apple computer at the Cupertino headquarters, did a lot of stuff on a VAX. Matter of fact they did all the development work on a VAX and they found out that so many people were playing Star Trek on the VAX that it was crowding out the other work. Now being Apple what did they do, they bought another VAX so people could play Star Trek on it. You can only play Star Trek on this VAX. This VAX is for work. That's what they did and it worked. They finally freed up their VAX and everybody could go on about their real business and still play Star Trek. That's fairly realistic because people are really going to do certain things, do mindless things on computers because they're bored, they need to refresh their minds or whatever. What's another reason for not allowing people to bring in software from home by the way? Other than possibility of viruses? Pirated copyright laws. Technically if they bring it in from home and put it on your computer at work, what's that? Makes you liable. Makes you as the company liable for what? Copyright violations. How are they ever going to catch you? They have people go around, plus your employees can inform on you. You're a big company, or medium size company, maybe you're a small company and buy one copy of Microsoft Word and give everybody a copy. No problem right. Get a disgruntled employee, he calls up Microsoft and says "I'd like to have your reward. I know a company that's got 18 copies of Microsoft Word, all the same serial number. Maybe you ought to check these people out." Other than, of course, our just standard moral behavior, I know a lot of people do not agree with the copyright laws on software. Whether you agree or not they are there and they have been found legally enforceable although it is hard to catch people pirating. Which isn't really a nice word. Stealing is really the right word to use. Pirate sounds romantic. Really all they're doing is stealing software.

While we're talking about people bringing in stuff from home, what does DIS say about that by the way? What does DIS say about software used on systems to process classified information? It has to be controlled, protected, and what? It has to be what? We're not going to go into marking really. What you have to do, according to DIS, according to the new Industrial Security Manual, is to assure that that software has not been modified. You have to find some means of assuring that that software is going to do what it is supposed to do. Generally they're going to tell you you have to do what in order to assure that? You have to buy it commercially. That precludes doing what, generally? Generally they'll say you can't take it off a bulletin board, you can't download it off a modem. That's one of the big ways that viruses, Trojan Horses, trap doors or whatever are brought into systems is that they're taken off bulletin boards, people pass them around or whatever. You'll have to tell your specific I.S. rep about this. But what they're getting to is that in the old Industrial Security Manual it addressed system and data integrity only in passing. It says really what we're concerned about is the security of the classified information. In other words, in the old Industrial Security Manual all we're saying is "we want to try, within a reasonable degree, to preclude unauthorized access to the data." I think one of the phrases in the old Industrial Security Manual was "we recognize, of course, that you may institute other security controls to maintain system and/or data integrity." What we're really looking for was to preclude unauthorized access to classified information. Now in a stand alone system that's not hard. If someone had written a virus that's going to destroy your hard disk, was that a big concern to DIS at the time? Why not? Because it did not impact on what? Did not impact on the security of the classified information. It wiped out a hard disk, you didn't have it anymore, but it did not allow an unauthorized person to have access to it. Under the new Industrial Security Manual, January 1991, the Industrial Security Manual now addresses data integrity. It addresses data integrity by saying essentially the software that you run in conjunction with classified information has to have a reasonable degree of assurance that it is going to perform the way it is intended to perform. That is, it should be virus free. And it's up to you to institute a system for either approving systems or adding software to systems to provide that assurance.

Now one way to do it is to just go out and buy software, shrink wrapped, off the shelf, take it back, put it in the safe, take it out, put it in the machine, put your master copies back in the safe. You got it commercially. You bought the stuff commercially. That doesn't necessarily say there are no problems with it. But what it says is that you've made a reasonable assurance that a commercial program is going to work in a certain way.

There was a big discussion, a teleconference with all the AIS security specialists several months ago, within DIS about the data integrity situation. That is how they're going to assure that for instance, on systems that have been used for unclassified all along, and suddenly we say we're going to use this system, starting next week, for classified. But we have not protected the software on these systems to preclude any unauthorized modification or whatever. How are we going to certify that this system is going to perform as reasonably expected? How would you do that? How would you, with an existing system that's been sitting on the floor for six months or six years, say that the software in there has no problem with it? I know of one, and I've only heard of one situation where an I.S. rep told people that they had to go out and buy all new software for this system. Does that sound reasonable? Certainly not reasonable from a cost effective standpoint. Now I understand that was tossed, by the way. He had a little over aggressive situation there. Essentially what they decided on, as I understand it, and again you'll have to check with your own I.S. Rep if you run into this situation, is that you start protecting the system when? As soon as you identify the need for using that system and software on the system to process classified information. How are we going to preclude viruses or the possibility of viruses existing on there? Because we really don't know, right? What DIS has said is that they would expect you to run some sort of anti-viral software. Usually go out and commercially buy a program which is going to inspect that software existing on your system against known viruses. That's generally what they do in those situations. There is a multitude of commercial and even some share ware or free ware programs that are available that will do that. They are generally cost effective, $80, $90 somewhere around there. Some cheaper. Which means that you could run that. Say we certify that as of this date, according to this software, we didn't have any problems and DIS would generally accept that as an assurance that we're not in a problem area with the software.

Do viruses generally infect data? No. Generally we're talking about viruses affecting programs that run in and of themselves. That is the program files, either the system program or quite often the application programs themselves. The in virus on the Mackintosh. There is a thing called the Desk Top which is really no more than a directory. The Desk Top becomes the whole disk. Once that happens you have a disk crash or it says sorry disk full or whatever and you can't use it any more. It's really easy to take off. But once it gets on there, you don't recognize what's happening.

We've just covered really the basics on protection of hardware, most particularly talking about the media, and software.

We talked about protection of the hardware. I will now talk about tamper resistant seals. When would we use seals on a system? Why would we use seals on systems? Will seals prevent unauthorized entry. We want to act as a deterrent to and provide evidence of somebody having gained access to the inside of the machine. Remember what we're talking about here are those machines that are not continually protected as classified. If we were to take out a machine and stick it in the vault, we'd have to use something to preclude unauthorized modification. What's providing that? The container itself. We could have it stored in a Class A vault, a closed area, a strong room and seals would not be required in those situations, because the computer is being protected by that barrier. As a matter of fact, not to pitch Mosler or anything, but they do make a GSA approved security container which is designed to do nothing but store your computer. Is anybody familiar with a map and plan file? You know the one with just one big door, I call it the refrigerator. Anyway, you just open this one big door and it is a full size GSA approved security container. They can slide your computers in there, you turn it on, do your stuff, slide it back in, close the door, and spin the dial. It is a little cramped and you're bumping your knees against the printer. That would be one way of doing it. But that's expensive. How much does a GSA approved security container cost? A couple thousand dollars at least and we're talking about a specialized container with power source and that kind of stuff. A Class A vault and strong room closure also are not cheap. What would be a lot cheaper is, we already have a safe over here. It would be a lot easier if we could just take the removable media, whatever kind it is

and stick it in the safe and just leave the computer sitting on the floor. We can do that if we can take all the classified information out of the system, put it in the safe, erase any internal memory, declassify internal memory to preclude unauthorized disclosure of classified information. In other words we've declassified the entire system. We could just let it sit there. We still have potential problems. Mainly, that somebody could come in and make some sort of unauthorized modification to the system which either would affect the system integrity or the data integrity on the classified information that we were to process on there.

There are a couple of things you can do in order to maintain what used to be called continuous detection which they now call something else but it essentially is still continuous protection. In other words you have enough barriers or whatever around this piece of hardware which is going to allow the detection of unauthorized access to the system. This continuously protected area, although they don't call it that anymore, there is a new phrase. This continuously protected area generally ends up as a seal. That is we apply some sort of seal that would break if somebody messes with it. We can't just peel it off. Some sort of breakable seal over the access areas to the computer hardware. Now I say computer hardware, and we're talking about the entire system. Not just the little box that has the CPU in it. We're talking the monitor, we're talking printers, and we're talking about the box with the system in it. We're talking about scanners, external hard disk, whatever we may have hooked up to this. It isn't going to be locked up in a safe. We have to protect all those access areas so that if somebody does open it up to do something untoward to our machine, they'll have to break those seals. You'll have to have a seal log, where you put all the seals, number them and the seals have to be unique. What's the quickest way according to that to make that seal unique? You can put a serial number on it, you can also date it and put your signature on it. I used evidence with the Computer Sciences Corporation. Anybody familiar with evidence tape? You see it on television all the time. Evidence tape is really thin, usually red, says evidence on it, and it's generally used by the police in order to seal up small pouches. They take the old cartridge case out or here's a bloody knife and they stick it in a plastic pouch, seal it up. The rules of evidence say that they have to assure that nobody has tampered with this. So they do that, then take this tape and put over there, date it and sign off on it. What this does, in order to open that bag up they have to break that seal. Every time they open up the evidence bag they put that and the old evidence bag into a new evidence bag and the evidence, seal it back up and do the same thing. That's so that when they get to court they can hold this up and say "I can guarantee that I'm the only one who's had access or only authorized people have had access to this evidence." So the detectives can't say the evidence has been tainted in some way. That works the same on computers. Once you put it on there it makes a mess. It's hard, but not impossible to get off. These seals do break accidently. Generally they will put them over areas of access. That is around seams. Computers get hot, they get cold. They expand a little bit and that can break the seal. If that happens, what do we have to do? What do we assume if we find a broken seal that we didn't intentionally break? We assume that there is at least a possibility that it's been tampered with. What do we do to use the system after that then? Do we say, OK, we can't use this system any more? We have a knowledgeable person inspect that part of the system that has the broken seal to see if there is any evidence of anything untoward having been done to the machine such as somebody putting a transmitter in there. That would be one way of doing it. Now we say knowledgeable person, we're not talking you have to go out and get the owner of the company and say you've got to come in here and check this thing out. All we're saying is that somebody generally familiar with what the inside of this thing is supposed to look like, takes a look at it and sees if there is anything new in there. There are all kinds of things that can be done.

In closing I'll give you my favorite evidence of tampering. Anybody here familiar with Crystal City in Arlington, VA? I used to be an IS rep for the capital region and I used to inspect down there. This doesn't involve classified so I can talk about it. I don't know if you're familiar with the place but there are lot of small contractors there who are actually sometimes big contractors with small offices. They're jammed into buildings and floor space is a premium and all this other stuff. There is this one company that lost four contracts in a row to the competition that just happened to be next door. Four. Now he lost them by one or two percent on the margin. Their bid was one or two percent below and they got the contract. They couldn't figure it out. So they are bidding on another one. The secretary's in there, she's got everything done, she says print. The printer stops.

Something happens, she has to stop the printing, then she starts it up again. She gets a little curious because the printer next door starts and stops at the same time her printer starts and stops. So she stops and next door stops. She says start and next door starts. Everything was going fine. So she calls the boss. What's this. This is really a coincidence. She goes through it a couple times. The boss says this is really strange. So he gets over there and goes over the printer and there's this wire coming down from the back of the printer, it goes along the wall, goes along the carpet and through the wall on the other side. He takes the wire, pulls it off, starts their printer and nothing happens over there. So it doesn't have to be a transmitter. It can be hard wired in there. With that I think we'll stop. Have a nice evening. ■

PART IV

SPEAKERS' BIOGRAPHIES

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 the Contractor SAP/SAR Working Group Personnel Security Committee and is a member of 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.

Jacqueline F. Baker

Ms. Baker is the Program Manager for Security Education and Awareness for 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 Security arenas. One accomplishment this past year has been the development of "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 "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. She has been an active member of NCMS since 1982.

Dr. Lawrence Martin Bittman

Dr. Bittman is currently located at Boston University College of Communications and works with the Program for the Study of Disinformation.

Dr. Bittman speaks several languages including, Czech, English, German, and Russian. He graduated from Realine Gymnasium, Prague, Czechoslovakia, 1950; Charles University, Prague, J.D., International Law, 1954; and Charles University, Prague, M.A., Journalism, 1967.

His professional experience includes: 1953-54, a five month diplomatic mission in Korea as a member of Neutral Nations Repatriation Commission; 1955-61, Chairman, Educational Dept. of International Relations, Ministry of Interior, Czechoslovakia; German Desk Office, Czechoslovak Intelligence Service; 1961-63, Third Secretary (Cultural Attache), Czechoslovak Embassy, Berlin, East Germany; 1964-66, Deputy Chief, Department of Active Measures and Disinformation, Czechoslovak Intelligence Service, Prague; 1966, German and Austrian Desk Officer, Press Department, Czechoslovak Ministry of Foreign Affairs; 1966-68, Press Attache and Public Relations Officer Czechoslovak Legation, Vienna, Austria; 1968. After the Soviet invasion of Czechoslovakia, he was granted political asylum by the U.S. government; 1969-70, Research Associate, Fletcher School of Law and Diplomacy, Tufts University, Medford, MA; 1971-72, Lecturer, School of Public Communications, Boston University, Boston, MA; 1972-78, Assistant Professor, SPC, Boston University, Boston, MA; 1984, Visiting Professor of Journalism, Tel Aviv University, Tel Aviv, Israel; 1986, Director, Program for the Study of Disinformation, Boston University, Boston, MA; 1990, Professor of Journalism, College of Communication, Boston University, Boston, MA.

Dr. Bittman has several publications including; Prvni Zemrel Kancler (The Chancellor Was the First to Die), Prague, Magnet, 1968; Department D: The Role of Disinformation in Society

Diplomacy. Fletcher School of Law and Diplomacy, Tufts University, 1970; rewritten in 1972 and published under the title, The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare. Syracuse University Research Corporation, 1972; "Images, Immigrants, and Their Press" in Bernard Rubin, ed., Small Voices and Great Trumpets: Minorities and the Mass Media. published by Praeger, 1980; Spionazni Opratky (Spy Gallows), personal memoirs written in Czech. Published by Czech Exile publishing house, 68 PUBLISHERS, 1981, Toronto, Canada.

Irving Boker

Irv has spent the last 13 of his 36 years with the General Accounting Office (GAO) as the Evaluator-In-Charge of reviews of the protection of national security information. During that time, his group has issued 27 reports on information, personnel, and physical security, covering subjects such as classification management, systematic declassification reviews, 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.

Capt. David Carey

Dave Carey is an accomplished consultant and sought after professional speaker and trainer with over 20 years of highly successful hands on experience in senior management. Dave is uniquely qualified to assist organizations with leadership training and organizational development.

A graduate of the U.S. Naval Academy, Dave is a retired Navy Captain. He was three times a Commanding Officer and served as Director of the Navy's Premiere Sight of Leadership and Management Training. In this role, he personally conducted seminars for prospective commanding and executive officers.

During the Vietnam era, while flying a combat mission over North Vietnam, his aircraft was destroyed by a surface-to-air missile. He spent the following 5-1/2 years as a POW incarcerated in numerous North Vietnamese prisons. Among Capt. Carey's military service awards are the Legion of Merit, five Bronze Stars, two Meritorious Service Medals, the Purple Heart, eight air medals and the Navy Commendation Medal.

In addition to running a successful speaking business, Dave is the director of development for the SYMLOG Consulting Group. He has extensive experience as a trainer and consultant in both the private and public section. He is one of only 13 consultants certified by the state of California to conduct team building programs for Law Enforcement Agencies throughout the state.

Deborah Russell Collins

Manager, Security Administration & Training
ESL, Incorporated

Ms. Collins has worked for ESL Incorporated since 1980. She held the following positions, Security Administrator, Training Program, 1980-82; Security Education Specialist, Corporate Staff, 1982-86; Sr. Security Administrator, Program Security 1984-86; Manager, Corporate Security Services, 1986-89. She currently holds the position of Manager, Security Administration and Training, which includes directing a management development and training program for 150 employees. This includes development and delivery of classroom instruction, field training and organizational effectiveness programs. As a senior fellow position, one of five within ESL, she provides for participation in company-side management issues with an emphasis on achieving a total quality work environment.

Ms. Collins also provides consulting services in industrial security management through Collins Consulting Group, Pleasanton, California, since 1988. With emphasis in delivery of effective security management systems to include security awareness, training and education programs. Clients have included PERSEREC, SRI International, and Special Security Services.

Ms. Collins received her Bachelor of Science degree in Business Administration, Marketing/Management from Radford University in 1980. She received her Masters of Science degree in Human Resource Management and Development from Chapman College in 1987.

Ms. Collins' publication/lecture credits are extensive. She has written and presented such topics

as "Counter-Intelligence Employee Security Awareness" and "To Instill Positive Motivation-The Employee Security Awareness Challenge."

Ms. Collins holds memberships in the National Classification Management Society, and the American Association of University Women. She was on the NCMS National Board of Directors from 1987-90, and was the national president from 1989-90. Among her awards are Who's Who in America, 1990; Who's Who in Security, 1989; Who's Who in American Women, 1989; ESL Presidential Citation, 1986; and Outstanding Young Women in America, 1982 and 1986.

Thomas J. Conner

Director of Security, Center for Night Vision & Electro Optics, Fort Belvoir, Virginia, a combined research, development and readiness activity specializing in Night Vision Devices, Laser Research and Infrared Technology. Responsibilities include the implementation of the full spectrum of security support services but with particular emphasis ion Information Security, Computer Security, Classification Management, Industrial Operations and International Programs. Prior to joining Night Vision, he served as Chief, Security Operations Branch, Counterintelligence Division, Communications Electronics Command, Fort Monmouth, New Jersey, where he managed the Information Security Program to include Security Awareness Training, Classification Management, Inspections and Computer Security for a geographically dispersed Major Subordinate Command with over 15,000 employees.

An active member of NCMS since 1977 and one of the original members of the Mid-Atlantic Chapter, he was Chairman of the Education & Training Subcommittee in 1986 & 1987 and then Chapter Chair in 1988 & 1989. Tom has been chairman of nine (1981 through 1989) chapter one-day seminars and recipient of the NCMS Society Award in 1988. A native of Philadelphia, PA, he graduated from LaSalle College with a Bachelor of Science in Accounting. As an active duty officer in the Army he served as an area studies specialist and counterintelligence special agent in various assignments to the Republic of Vietnam.

Trisha Dedik
Deputy Director
Technology Policy Division
Office of Arms Control

Ms. Dedik has been with the Department of Energy, (DOE) since its inception. Since that time, she has spent most of her career working national security related issues. She currently serves as Deputy Director of the Division of Technology Policy, Office of Arms Control for the DOE. She is responsible for directing the development of DOE policy related to U.S. national security and strategic export control. As such, she participates in multi-national deliberations on the formulation of international export controls related to strategic commodities, as well as items/technologies of nonproliferation concern. She has formerly served as senior staff at the Nuclear Weapons Council, as well as holding senior management and policy staff positions in the Office of the Assistant Secretary for Defense Programs for the DOE.

Ms. Dedik has a Masters in Public Administration from West Virginia University, and has attended numerous management training courses. She is also listed in Who's Who in the East.

John Patrick Dolan

As a trial lawyer, John Patrick Dolan has handled everything from preparing a simple will to death-penalty murder cases. And that's not only a testament to this wide-ranging legal experience, it's proof that John Dolan has helped all types of people. John prides himself on the ability to relate well to all people in all situations. And as you'll soon see, he knows how to identify - and meet - the needs of any particular audience.

A veteran seminar leader, John began his professional speaking career as a way to build his legal practice. Now, he's the principal speaker for his own company, LawTalk, a consulting firm that provides training and development presentations for business and legal professionals. In addition, he continues to practice as a trial lawyer, specializing in criminal defense and estate planning.

John sees his dual career as a natural match. After all, trial lawyers must be excellent public speakers and seminar leaders must be excellent problem solvers. He's combined these talents to become a favorite presenter among clients like Xerox, Rockwell International and the California Trial Lawyers Association.

John F. Donnelly
Director, Defense Investigative Service

Mr. Donnelly is a native of Glenolden, Pennsylvania. He is a graduate of St. Joseph's College, Philadelphia, Pennsylvania, 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, as Director, 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 Collindale, 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 informational 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 Scientific and Technical Agreements with the Government of Japan.

Prior to joining the staff of the Deputy Under Secretary 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.

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, he 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 included the Presidential Rank Award of 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.

Gregory A. Gwash
Deputy Director (Industrial Security)

Greg Gwash is a native of Minnesota. He has a Bachelor's Degree in Russian area Studies, a Master's Degree in Far Eastern History and a Juris Doctorate degree. In his current position, he is responsible for the Department of Defense Industrial Security Program administered by the Defense Investigative Service. Prior to his appointment as Deputy Director (Industrial Security) in October 1990, he was the Director of Industrial Security for the DIS Pacific Region, headquartered in Long Beach, CA. Preceding his appointment as DOIS in April 1987, he was Chief of the DIS Office of Industrial Security, International, Mannheim, Germany Field Office, responsible for inspections and assistance to U.S. contractors in Europe, the Middle East and Africa. He has also held positions as an Industrial Security Representative since 1972 in Santa Barbara, Phoenix and Chicago. Greg also served in the U.S. Army's Special Forces, including duty in Vietnam from 1965 to 1967. He is an inactive member of the California Bar Association.

George S. Hall

A native of West Virginia, Mr. Hall currently resides in the Washington, D.C. area. From 1979 to 1985, Mr. Hall worked for the Defense Logistics Agency/Defense Investigative Service as an Industrial Security Representative, Industrial Security Staff Specialist and, finally, as an instructor at the Defense Security Institute.

Upon leaving DIS in 1985, Mr. Hall worked for Computer Sciences Corporation in Beltsville, Maryland as the FSO. Mr. Hall currently works as a security consultant to government and industry specializing in Industrial, Physical, and AIS Security Areas.

Bob Harman
FBI DECA Program Coordinator

Bob Harman has been a Special Agent for the Federal Bureau of Investigation (FBI) since March 30, 1964. Before joining the FBI, he worked in the Personnel Department of the Autonetics Division of North American Aviation (now Rockwell Corporation) in Los Angeles, California. Bob has been assigned to San Diego since June 1985, and is responsible for the FBI's Development of Espionage and Counterintelligence Awareness (DECA) Program.

The purpose of the DECA Program is to develop good working relationships between the FBI and Defense Contractors to improve security.

Zander Hollander

Zander Hollander is an Export Control Specialist in the Department of Energy's (DOE) Technology Policy Division (DP-323) whose primary responsibility is administering the Department's regulations 10 CFR Part 810. These regulations implement Section 57b of the Atomic Energy Act, which requires the Secretary of Energy's authorization for U.S. firms and individuals intending to engage directly or indirectly in the production of special nuclear material outside the United States.

Mr. Hollander is a former newsman. Before entering U.S. Government service 16 years ago, he was for 14 years a United Press International correspondent and editor in Europe, Africa and the Middle East and for six years a reporter and editor in Saginaw, Michigan, and Arlington, Virginia.

Born in Brooklyn, New York, Mr. Hollander graduated from the University of Michigan with a B.A. in Political Science and pursued graduate studies in international affairs at Harvard University and West Berlin's Free University and the German Institute of Politics.

Mr. Hollander also is involved in the Department's effort to govern the dissemination of Export Controlled Information in support of U.S. nonproliferation policy and national security. He helped to develop the "Guidelines on Export Controlled Information" issued by Troy Wade, on January 19, 1989.

Lawrence J. Howe (Larry), CPP
Corporate Vice President and Director of Security
Science Applications International Corporation

Larry has 30 years experience in national security-related activities. He has been the Director of Security at SAIC for the past 13 years. Prior to joining SAIC early in 1978, Larry served 15 years with the Central Intelligence Agency. His most recent CIA assignment was as a Regional Industrial Security Officer. His prior CIA assignments included overseas assignments in counterintelligence operations and investigations, and polygraph. Larry completed military service with the Marine Corps with a specialization in intelligence.

Larry has given testimony on security subjects before congressional committees and has served as a panelist on the Congressional Office of Technical Assessment review of the use of the polygraph by the DoD. His graduate work is in political science and he is active in several security professional societies. Larry was the 35th President of the American Society for Industrial Security (ASIS). He has been serving on the ASIS Board of Directors for the past four years.

Admiral Bobby R. Inman, USN, (Retired)

Admiral Inman was born at Rhonesboro, Texas on April 4, 1931, and graduated from the University of Texas at Austin (B.A., 1950). He entered the Naval Reserve the following Year and was commissioned as an Ensign in March 1952. Over the next nineteen years he served on an aircraft carrier, two cruisers and a destroyer as well as in numerous assignments ashore in Naval Intelligence.

He graduated from the National War College in 1972, was selected for promotion to Rear Admiral in January 1974 and was promoted to Vice Admiral in July 1976. In February 1981, he was promoted to the rank of Admiral, the first Naval Intelligence Specialist to attain four star rank. He retired with the permanent rank of Admiral on July 1, 1982. Between 1974 and 1982 Admiral Inman served in tours as Director of Naval Intelligence; Vice Director of the Defense Intelligence Agency; Director of the National Security Agency and Deputy Director of Central Intelligence. From January 21, 1983 until December 31, 1989, he served as Chairman and Chief Executive Officer of the Microelectronics and Computer Technology Corporation (MCC) in Austin,Texas. From December 31, 1986 to December 31, 1989, he served as Chairman, President and Chief Executive Officer of Westmark Systems, Inc., a privately owned electronics industry holding company. Admiral Inman served as Chairman of the Federal Reserve Bank of Dallas from January 1987 to December 1990.

Admiral Inman is a member of the Board of Directors of Dell Computers, Fluor, Science Applications International, Southwestern Bell, Temple Inland and Xerox Corporations. He serves in a volunteer status as a Director of the Council on Foreign Relations and the Center for Excellence in Education. Admiral Inman is a member and a trustee of the National Academy of Public Administration. He serves as a trustee of the California Institute of Technology and Southwestern University. He also serves as the Vice Chairman of the President's Foreign Intelligence Advisory Board. Admiral Inman serves on the Executive Committee and as an active participant on the Business-Higher Education Forum, the Carnegie Commission on Science, Technology and Government and the Council of Competitiveness.

Linda Lindsey Kimbler
Education and Training Specialist, Pacific Region
Defense Investigative Service

Linda is a native of Longview, WA. She has 17 years of Federal Government service. Her career began with the Internal Revenue Service as a Revenue Officer working the Los Angeles and San Diego areas. She joined the Defense Investigative Service as an investigator in San Diego and eventually became the Special Agent-in-Charge of the Santa Ana Field Office. After a two year sabbatical which included travels to New Zealand, Fiji, Mexico, Canada, and western parts of the United States, Linda returned to Defense Investigative Service. She was selected as the Pacific Region's Education and Training Specialist in February 1987. She is an active member of the Industrial Security Awareness Council of Southern California and holds the positions of Treasurer, Archives Committee Chairman and FSO Seminar Chairman.

Larry J. Larsen

Larry has twenty years experience as a private investigator, with experience in product liability cases, financial institution fraud, and investigating large accidents. He was also a Deputy to a Los Angeles County Supervisor with responsibility for investigating public corruption. He has been a consultant to local and national media on major fraud and disaster stories, and has done investigative reporting. He was also Recording Secretary for the Los Angeles Chapter of the Information Systems Security Association, Inc. (ISSA).

Mr. Larsen has extensive experience in applications development, including most business applications software, word processing programs, database management, financial spreadsheets and communications.

Michael W. Liikala

As Director of the Western Region for the United States Department of Commerce since 1988, Mr. Liikala is responsible for ensuring U.S. companies comply with U.S. export control laws. In 1990 this involved over $50 billion in export licenses from the 10 Western states in his jurisdiction. Prior to 1988 he served for three years as Chief-of-Staff and Senior Advisor to the Under Secretary of Commerce responsible for coordinating the administration of U.S. trade laws involving U.S. industry, foreign investment in the United States, and U.S. export control regulations. Mr. Liikala led the team of negotiators which successfully concluded trade agreements with Japan and Taiwan.

During Mr. Liikala's distinguished career he has worked at the highest levels of Government on complex economic issues. From 1982 to 1985, he was the Economic Advisor to the Under Secretary of Commerce and was in charge of developing positions for the Cabinet- level committee responsible for U.S. Economic Policy, including international trade, finance and monetary issues. Prior to joining the Under Secretary's Office, he was with the United States Senate Banking, Housing and Urban Affairs Committee and was involved in the drafting and passage of major legislation in areas within the committees jurisdiction.

Mr. Liikala has also worked with the U.S. Treasury Department on investment issues, and the Executive Office of the President on financial issues, the National League of Cities on Housing and urban development issues and at the California State Legislature. Mr. Liikala had a successful career in business, establishing his own company which achieved a million dollars in sales in it's first year.

He has a Master's degree from the Johns Hopkins School of Advanced International studies in International Law/Economics and a Master's degree in Finance from the University of Southern California. He received a BA in Law and Public Policy from the University of California. Interviews with Mr. Liikala have appeared on Business Television programs and in numerous publications, including the Wall Street Journal, Business Week, the Los Angeles Times and the Washington Post.

James P. Linn, CPP
Assistant Vice President Deputy Director
Corporate DoD Security Program
Science Applications International Corporation

Jim is a native of Baltimore, Md. with over 20 years of experience in the intelligence and industrial security field. His military experience included assignments wit the U.S. Army Military Intelligence and Combat Infantry Units. He recently retired as a LTC, Military Intelligence, U.S. Army Reserves. Jim has been an Industrial Security Representative with DIS, a Command Security Manager with the U.S. Army, and an instructor at the U.S. Army Intelligence School, Ft. Holabird, Maryland.

Jim joined Science Applications International Corporation (SAIC) in January 1987. Prior to SAIC, Jim operated Industrial Security Associations (ISA) Incorporated, a security training and consulting firm specializing in the DISP. Jim spent over 9 years within the Defense Investigative Service (DIS). In his last DIS assignment he served as the Chairperson Industrial Security Department DoD Industrial Security Institute, from 1980-86, and was responsible for the development and conduct of the one week Industrial Security Management Course. Jim earned his BA degree from Chapman College, and an MBA from the University of Baltimore. He is currently a Director with the National Classification Management Society, a certified CPP, and member of the Government Security Committee for the American Society of Industrial Security (ASIS). In addition to his corporate security duties, Jim is the

Facility Security Manager of the SAIC Campus Point facility.

Ernest Mayerfeld

Mr. Mayerfeld is currently employed at Cleary, Gottlieb, Steen & Hamilton in Washington, DC His prior work experience includes: the National Security Agency, Legislative and Regulatory counsel, March 1986 to September 1989; The Central Intelligence Agency, Counsel to the Deputy Director for Operations, August 1984 to February 1986; Central Intelligence Agency, Office of General Counsel, Chief, Litigation Division from February 1975 to March 1980; Served in Washington , D.C. and abroad with the Foreign Service, Department of State and Department of the Army.

Mr. Mayerfeld has received several awards. Among them are the John Marshall Award from the Department of Justice in 1983; and the Intelligence Medal of Merit from the Central Intelligence Agency in 1985 and 1986.

Mr. Mayerfeld has bar memberships in Michigan (inactive), New York, and the District of Columbia. He graduated from he University of Michigan, A.B. 1950, J.D. 1951.

Dick McGuire

Dick McGuire is the Director of Corporate Security for the Grumman Corporation. He holds a Bachelor of Science Degree in Behavioral Science and Criminal Justice from the New York Institute of Technology. Dick is the former Chapter Chairperson of Chapter 22, New York, Connecticut and Long Island.

Robert Lee Morris, Jr.

Robert Lee Morris, Jr. (Bob Morris) is the C.I.A. spokesman concerning the espionage threat posed by Soviet bloc intelligence services in the United States. He began this effort in 1972. In recent years, he has traveled throughout the Untied States to conduct security awareness presentations for government and industry, entitled, Soviet Espionage in the United States, and Soviet Espionage in Industry, respectively.

Bob Morris attended the U.S. Naval Academy and Randolph-Macon College prior to joining the C.I.A. in 1955. He has completed over 35 years of government service, and has been posted to assignments in all 4 major directorates of the C.I.A. Most of his career has been spent in a variety of undercover assignments within the Office of Security.

Gary Murphree

Gary has been the Vice President of Government Business Development for Sargent and Greenleaf, Washington, D.C. since 1979. He began his security career in engineering from 1972 working for Yale, Ilco-Unican, and All-Lock. For the last 13 years he has been active with product engineering and new product development responsibilities of high security locking devices. He has a degree in Engineering from Memphis State University, a Business degree from Vol State Community College, and a Marketing degree from the University of Kentucky. He is an active member in NCMS, ASIS, ALOA, DHI, and ASTM.

Robert C. Nelson

Robert C. Nelson has over fourteen years of industrial security experience serving in positions as FSO, CSSO, COMSEC Custodian and Classified Hardware Control Custodian and has worked as a Security Specialist/Manager for firms including SRS Technologies, Hughes Aircraft and Lockheed Missiles and Space Company. Bob is experienced in all aspects of the DISP and has specialized background in AIS Security, Contract Management, Export Control and Competitor Intelligence. Currently Bob is President of his own company, Cypher Solutions, Inc., Specializing in consulting services to Defense Contractors, development of customized security related software and performing competitor intelligence investments.

Bob has a Bachelor's Degree in Liberal Arts and has Master's work in progress and is a certified FSO having completed both the Industrial Security Management Course and the Essentials

of Industrial Security Management Correspondence Course.

Bob has been an active member in the National Classification Management Society (NCMS) San Diego Chapter since 1987. He is currently serving as Chapter Chairperson, and has served as Chapter Secretary, National Training Seminar Training Program Chairperson, Mini-seminar Training Program Chairperson, and Mini-seminar workshop guest speaker. Bob is a member of Information Systems Security Association (ISSA) and American Society for Industrial Security (ASIS), and the Overseas Advisory Committee on Terrorism through the State Department.

John N. Petzel
Senior Computer Security Specialist
United Technologies Corporation

John N. Petzel has been responsible for computer security for Government contractors for the last 10 years. This period is highlighted from 1982 to 1985, when he served Lockheed Missiles & Space Company as their Chief, Classified ADP Security. United Technologies Corporation attracted John to his current position as a Senior Computer Security Specialist in 1987. He is Vice President and a Director of Cypher Solutions, Incorporated, a computer security consulting firm. John received an MA in Education from the University of St. Thomas, St. Paul, MN, in July 1981 after maintaining a 4.0 average through his graduate studies. In May 1974, he was awarded a BA from Drew University, Madison, N.J. His undergraduate major was psychology.

His current professional memberships include the Computer Security Institute, Pacific Region AIS Security Forum, and American Society for Industrial Security. He was a founding member and a past President of the Information Systems Security Association (ISSA), San Diego Area Chapter and currently serves as a Director of this Chapter. He was Vice-Chair of the San Diego Chapter of NCMS from 1988 to 1990 and served as an Advisor to the 1991 Annual Training Seminar Planning Committee.

James C. Rowley

Mr. Rowley presently works as a reporter for the Washington Bureau of the Associated Press. He began his employment in May 1983 with the bureau. Since January 1989, he has been assigned to cover the Justice Department beat that ranges from FBI investigations to the politics of judicial appointment, civil rights and abortion.

He previously spent two years covering the U.S. Courthouse, writing about major criminal cases, notably the prosecutions of Oliver North and his Iran-Contra codefendants as well as the trials of former White House aides Michael K. Deaver and Lyn Nofziger.

In 1986, he followed domestic policy issues in Congress. His other bureau assignments have been as a desk editor, general assignment reporter and weekend supervisor, a position he held for nearly a year. In that capacity, Mr. Rowley oversaw the Washington bureau's news operation on Saturdays and Sundays, directing the coverage and editing of stories.

Mr. Rowley's previous experience includes being a reporter for the Baltimore bureau, The Associated Press, September 1980 to May 1983. His duties included doubling as a state-desk editor and general assignment reporter, writing features as well as covering breaking stories. He also served as weekend editor in the bureau. From February 1979 to September 1980 he was a reporter, Baltimore bureau, United Press International. He worked as a desk editor and general assignment reporter. From August 1973 to January 1979 he served as a reporter, Rochester, N.Y., Democrat & Chronicle. He started as a news clerk, and became a police reporter and later switched to general assignment and the courthouse beat. Mr. Rowley and a colleague were nominated by the newspaper for a Pulitzer prize in 1977 for stories that detailed a police conspiracy to fabricate evidence at three Mafia murder trials.

Frank J. Ruocco

Mr. Ruocco received a BA degree from St. Peter's College in New Jersey in 1961. His major area of study was economics with a minor in phi-

losophy. Mr. Ruocco was commissioned as a reserve officer in the U.S. Navy in 1961. He served for three years in the Naval Security Group in Charleston, South Carolina.

Mr. Roucco joined the Agency in 1965. From EOD to May 1980 he had several assignments in the Office of Strategic Research or its predecessor organization. Virtually all assignments were on Soviet strategic forces. In July 1975, Mr. Ruocco was appointed as branch chief, in April 1978 deputy division chief, and in May 1979, division chief in the Office of Strategic Research. He attended the Naval War College in 1974-1975.

In May 1980, Mr. Ruocco was named Deputy Director of Imagery Analysis. In November 1982, he became Chief, Collection Director of Central Reference, and in June 1986, Director of the newly formed office of Information Resources.

Mr. Ruocco was named Director of the National Photographic Interpretation Center in February 1988. On 2 January 1991 he was appointed to his current position as Director of Security.

Augustina K. Scardina

"Gussie," a native of Baltimore, Maryland, received her B.A. from he University of Maryland Baltimore County campus. Shortly following graduation, she joined the Defense Investigative Service as a case controller at the Personnel Investigations Center. After four years in Personnel Security, Ms. Scandina transferred to Industrial Security as a Representative in the Washington, D.C. Field Office. In August 1986, she became the Education and Training Specialist for the Capital Region, DIS, where she served until her assignment to the Institute in November 1987. She is an active JIGSAG (Joint Industry Government Security Awareness Group) and NCMS (National Classification Management Society) member.

Gerald A. Schroeder
Senior Attorney
Office of Intelligence Policy and Review
United States Department of Justice

Responsibilities include assisting the Attorney General's Counsel for Intelligence Policy in the analysis and resolution of issues related to national security programs and activities, including programs related to information security, industrial security and access to classified information.

Alternate Chairman of the Department Review Committee, which resolves on behalf of the Attorney General all issues concerning implementation and administration of Executive Order 12356, "National Security Information."

Mr. Schroeder received his B.A. in 1969 from Georgetown University, Washington, D.C., and J.D., in 1972 from Indiana University Law School, Indianapolis, Indiana.

Carolyn Shugart
Computer Specialist
Defense Investigative Services

Ms. Shugart, born in Dallas, Texas, attended several colleges, including Pepperdine University. She began her Civil Service career in 1974 in Pensacola, Fl., with the Department of the Navy. She held various positions within Government, to include working in the computer room at DCASMA, San Diego, until accepting a position in 1982 as an Industrial Security Representative with Defense Investigative Service's (DIS) San Diego Field Office. In 1986, she accepted a position as an AIS instructor with the Industrial Security Department at the DoD Security Institute. In January 1988, she returned to DIS's Pacific Region as an Education and Training Specialist, and in June 1988 she was assigned to the Santa Ana Field Office as an Acting Computer Specialist, which included supporting the Ontario Field Office. In September 1990, she was transferred to San Diego County and is currently the Computer Specialist for the San Diego and Vista Field Offices.

Larry Stitt

Larry retired from the Navy in September 1975, and began his second career as an Army civilian 10 months later. He is Chief of Security Division, Office of the Deputy chief of Staff for Intelligence, U.S. Army Information Systems Command, Fort Huachuca (USAISC) Arizona.

During 1989, he developed the first of a series of computer aided instructions as new and innovative means to fill training voids created by the loss of manpower and resources within USAISC worldwide. He felt that self-paced automated tutorials would heighten interest and general security awareness where full-time Security Managers were not available to conduct formal security awareness training. The tutorials received high praise from all recipients.

During December 1990, Larry was personally invited by the PERSEREC to demonstrate his products at the 1991 DoD Security Awareness Symposium. High interest from participants led to being asked to develop his "reporting" tutorial into a DoD product for DoD-wide application.

Dr. Tom Steiner

Dr. Tom Steiner has been a professional speaker, entertainer, management consultant and teacher for the past 15 years. He has provided presentations and training programs to more than 100 major corporations in the U.S. and Canada. He performs more than 200 engagements annually.

He combines his talents in a way that makes learning FUN! By using humor, magic and advanced common sense, his highly stimulating management training programs motivate participants to consider new ways of behaving in the work place.

He has worked as a Director of Corporate Training, University Professor, Elementary School Principal, Stand-Up Comic, Rock and Roll Guitarist and part time U.S. Postal Employee. However, he credits most of what he has learned to driving taxi cabs and selling door-to-door in New York City. He knows what makes people tick and he talks about it.

Education: B.A. Psychology, 1969; M.A. Social Psychology 1971; Ph.D. Organizational Psychology, 1975; M.B.A. Management, 1983.

Deborah Donovan Varljen

Deborah has been on the Subcommittee on Civil Service, Committee on Post Office and Civil Service, U.S. House of Representatives General Counsel since November 1989. She is responsible for direct oversight and legislative actions regarding due process in security procedures, EEO, medical conditions and fitness for Federal employment, personnel issues at land management agencies, and Federal employee appeal processes. She advises the Chairman and Majority Members of the Subcommittee on substantive, procedural, and legislative matters relating to all aspects of Federal civil service employment.

Prior to her General Counsel experience, Deborah was a law clerk for Cooper and Kelley in Denver, Colorado, where she conducted legal research, drafted motions and briefs on medical malpractice and product liability issues. She has been a nursing manager for Mercy Medical Center, The Children's Hospital, and the University of Colorado. She is also a member of the Pennsylvania Bar.

Sandra (Sandy) J. Waller

Sandy began her government service in 1958 as a fingerprint technician wit 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 the 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 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.

Eugene J. White, Jr.

Mr. White was assigned as Deputy Director for International Security Programs, Office of the Deputy Under Secretary of Defense for Security Policy, on 15 May 1989. He is responsible for formulation and effective implementation of DoD policies governing the release of U.S. classified military information to foreign governments and the application of the various security disciplines to international agreements and cooperative programs. In coordination with the Department of State, Mr. White develops and negotiates bilateral General Security and Classified Military Information and Industrial Security Agreements. He arranges and conducts reciprocal on-site security visits to discuss procedures developed by each government to protect classified military information.

Mr. White has occupied various positions within the Department of Defense in the counterintelligence and security fields since 1976. He served as the Chief, Classification and Industrial Security Branch, Headquarters, Air Force Office of Security Police from 1984-1989. He was the director in Information Security for the Strategic Air Command from 1982-1984. Prior to 1982, Mr. White was with the U.S. Army Material Command, The electronic Proving Ground, Ft. Huachuca, Arizona, White Sands Missile Range, New Mexico, and Aberdeen Proving Ground, Maryland.

Mr. White is married and has two sons. He has a Bachelor of Arts degree from the University of New Mexico. Mr. White is an Army veteran with service in Vietnam.

David E. Whitman

Mr. Whitman has been employed in the Directorates of Information Security and Security Plans and Programs in the Office of the Deputy Under Secretary of Defense for Security Policy, and earlier OSD organizations, since January 1975 as a security classification specialist and, more recently, as a security specialist. He is responsible for development of the DoD Information Security Programs and has participated in the drafting of Executive Orders 12065, 12356 and the revision of 12356 that is ongoing. He has been instrumental in developing DoD policies regarding unclassified technology transfer, unclassified, but sensitive, information control systems, and counternarcotics security policy. Prior to his present position as Assistant for Information and Technology Security, Mr. Whitman had a number of assignments from 1966 in the DoD internal, personnel, and industrial security areas. Mr. Whitman holds a Bachelor of Science degree in economics from Villanova University and is an honorary faculty member of the Department of Defense Security Institute. He has been on the Board of Directors of the National Classification Management Society for the past 6 years and is taking the reigns of the Washington, D.C. Chapter of NCMS. Mr. Whitman served in the U.S. Army from 1964 to 1966, including duty in South Vietnam. ■