CLASSIFICATION MANAGEMENT

JOURNAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XXVIII 1992

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 J. Suto, NCMS. Editorial Oversight: David E. Whitman.

CONTENTS

Proceedings of the 28th Annual Training Seminar
June 30 - July 2, 1992

PART I--Speakers and Panelists

PART II--Workshop Information and Audio Tapes

PART III--James S. Cogswell Awards

PART IV--Annual Business Meeting and Society Awards

PART I

Speakers and Panelists

Considerations that Affect the Future of Industrial Security

Maynard C. Anderson

The American Pamphletter, Thomas Paine, in his "Philosophy of revolution", included the thought that there is always opportunity to start over again.

Today, in many ways, we are starting over again in order to deal with situations never before encountered, not even imagined.

Sometimes, it seems as though we must reinvent security.

In a Pentagon news briefing on 31 January 1992, Secretary Cheney said that,"..a proper appreciation for uncertainty is ... a critical part of what any realistic Defense strategy that builds forces that are going to allow us to deal with crises 5, 10, or 20 years hence. We cannot base our future security on a shaky record of trying to predict threats or a prudent recognition of uncertainty. Sound defense planning seeks to help shape the future, to actually alter the future. And that's what the President's regional defense strategy seeks to do."

The President's strategic concepts require that the United States:

- Exercise forward presence in key areas.
- Respond effectively in crises.
- Maintain a credible nuclear deterrent.
- Retain the capacity to rebuild our forces.

Samuel Lewis, in the President's message, Biennial Report to the National Institute for Peace, 1992, wrote that, "Around the World, communism and many of its authoritarian spin-offs have fallen. At the same time, other powerful currents run in quite opposite directions. Disputes over territory (as in Azerbaijan), religion (as in Sri Lanka), political power (as in Haiti and Somalia), national identity (as in Yugoslavia), and other issues are generating bitter conflicts that range from terrorism to guerrilla warfare to full-fledged war."

Deputy Secretary of State Lawrence Eagleburger in remarks to a Business Week symposium, Washington, D.C., 3 October 1991, concluded that, "...our national well-being, including the health of our economy, is dependent on a stable international order." He reminded us that following World War II, "...for the first time in our history, we determined to assume risks, incur obligations, and make sacrifices on behalf of and in conjunction with other nations. In short, we contracted an entangling alliance, linking our destiny to that of distant people on a more or less permanent basis." That resulted in a "...whole new world in which sovereign nations would coordinate their economic policies and collaborate on behalf of a common defense.

NATO was a product of that international collaboration, as was the International Monetary Fund, The World Bank, and other institutions. Totalitarian regimes died in the face of prosperity and freedom that this collaboration produced.

Today, here, we will continue our discussions about sharing the future because we share concern for a most important issue - the security of military and civilian technologies that affect our national interests.

The major change in the United States Department

of Defense is from responding to threats from another super power to responding to regional conflicts or to threats from developing nations with enhanced military capabilities.

We will continue to develop technologies that are dependent on research and development, on manufacturing capabilities, on information systems, and the integrity of all those activities.

Our acquisition strategy will emphasize research and development over production. But acquisition will still require about $50B per year and ahead there are still the F-22, the C-17, new aircraft carriers and destroyers to build.

Are there still threats in the conventional sense? Does the threat concept make sense?

James Schlesinger wrote recently in Foreign Policy that the basis for future United States forces should not simply be the response to individual threats, but rather that which is needed to maintain the overall aura of American power.

And, as Samuel Huntington of Harvard observed, the cold war "world of good guys and bad guys" will give way to world of "grey guys" as the adversarial relationship between East and West changes.

The changing world economic and political picture is particularly challenging to us because industrial security policy is forced to change as rapidly in order to keep up with new international trade agreements, treaties, the unique aspects of joint ventures among both nations and companies, and in general, the globalization of the world defense market. The requirements to safeguard our classified and sensitive information does not diminish. The threat environment becomes ever more complex.

Our individual policies must be under continuous review because each of our national interests must be considered as we share classified information with each other.

I believe we must reorder priorities so that matters of less urgency or less sensitivity will not take up our time. We must understand that the ability of management to focus on the unimportant is remarkable. It is our fault if we do not direct management's attention to that which is significant. And, we must understand that conditions change, as Secretary Cheney has reminded us, so our advice to management must be continuous. We will always be confronted with a moving target.

Let me begin with a challenge that incorporates a great many issues. The challenge is prevention of espionage. A sub-challenge might be in the form of the question, "What is espionage?" Great minds all over the place are struggling to explain espionage. It is, of course, the activities of spies. It relates to the social psychology of unauthorized disclosure of classified information. It involves the affects of criminal activity on the protection of classified information, in the form of the crimes of fraud, waste and abuse, for example.

Espionage today is caused by many factors. It is too simplistic to say that "greed" is the motivation for the crime. Motivations change as socio-economic conditions change. Hard times, unemployment, increased competition for work and business, all stimulate breakdown of loyalty between employees and their organizations resulting in fraud, theft, threats and plots against companies which potentially affect security.

In a paper prepared for Forum Fifteen, International Information Integrity Institute, Palm Springs, California, 28-30 January 1992, ("Identifying Personnel Susceptible to Committing Computer Abuse and Crimes") Dr. Theodore R. Sarbin, Personnel Security Research and Education Center (PERSEREC), makes the case that citizen espionage, embezzlement, and certain computer crimes are exemplars of a general model the center of which is the granting and betrayal of trust.

Even in the case of convicted spy John Walker, Douglas B. Marshall, writing in "Shipmate", a publication of the Naval Academy Alumni Association, September 1991, concludes that "...The money was only a sustaining motivation to stay in the business. The reasons he continued to actively betray us were much more sinister in nature, more

a manifestation of criminal intent and treachery.

We might need to imagine espionage potential in activities of those described by Robert R. Reich in a Harvard Business Review article entitled, "The Stateless Manager," printed in the "Best of Business Quarterly," fall 1991, as "the growing cadre of global manages - supranational corporate players whose allegiance is to enhanced world-wide corporate performance, not to any one nation's economic success.

"They, as global managers, want to increase their world market shares, profits, and share prices. We, as citizens of a particular nation, want to secure national wealth and economic criteria. We feel a special allegiance to our country and to our compatriots."

Of similar concern is the possibility of unauthorized disclosures of valuable information in what is actually "traded" across the borders. Reich says it is intangible services - research, engineering, design, management, marketing, and sales-transferred within global corporations from one location to another.

From a security standpoint then, it would appear that two of the fundamental factors involved in maintaining the integrity of any operation, the personnel and the information, are increasingly at risk of possible compromise as the world, rather than the individual state, becomes the operating venue of the corporation. It is probable that some of the controls that have restricted the export of the technology are going to be enforced only with great difficulty.

I am not suggesting that these global managers who might be American or any other nationality are either disloyal or conducting espionage. I am suggesting that they represent another challenge. Like those who might be stimulated to commit other crimes that endanger the security of our classified information and material, they might succumb to moral drift as they battle the tides of technology.

Related to the global managers phenomenon are the new and different economic and commercial alliances. The question that confronts us is, "what is American?" For example, Whirlpool is headquartered in Benton Harbor, Michigan, and has recently formed an alliance with Philips, based in Eindhoven, Holland. Whirlpool International is in Comerio, Italy, where it is managed by a Swede. On the six-person Management Committee sit managers from Sweden, Holland, Italy, the United States and Belguim. This is the kind of situation that stimulates our concern for the "intangibles" that are "traded" across borders - the research, engineering, design, management, marketing, and sales data. As a security officer confronting one of these situations, the challenge must be to ensure that trading of the commodity is not detrimental to the best interests of your nation.

Now an issue and a challenge combine to emerge in the form of how well we perform the dual mission of security: the proper protection and the proper dissemination of information.

Security's objectives should be synonymous with management's objective, which is, generally, achievement of, or maintenance of, technological superiority. You might get the information to those who need it to ensure that progress and developments maintain the edge. You must ensure program integrity at the same time. There is not one easy solution within this dichotomy.

This challenge is complicated even more when we consider the relationship between government security programs for the protection of classified information and the protection of proprietary information or unclassified technology.

Over the years, we have never done a very good job of determining the effectiveness of security programs. Methods of measurement, aside from that of failure, have taken the form of articles of faith that everything is alright. How do we know the system works?

Generally, we don't know if they work. We have established and improved systems that we believe manage change because they manage risk. We have tried to continuously establish and coordinate protection and resource priorities (a definition of strategic planning). We have struggled to properly

place responsibility for protection of information with its custodian. Managing change and risk requires judgement as well as integrity at the lowest levels of responsibility.

We have established some "burden sharing" between industry and government in the belief that an effective strategy will distribute and balance both the burdens and benefits of cooperation. We have attempted to demonstrate that security will contribute to income by preservation of an advantage to the nation as well as to the industrial enterprise - a concept that has been called "beneficial cost."

In terms of the mutual objectives of government and industry, we have tried to measure success by asking whether we were adding value to the creation of wealth rather than restricting it. If I may paraphrase comments by Robert Galvin, Chairman of the Executive Committee, Motorola Corporation, we should be measuring productivity in terms of eliminating those things that we don't need to do. And, we should be raising the expectations of our employees. Productivity, and I believe proper behavior, come in direct proportion to expectations.

One of my responsibilities involves international security policy which includes developing and negotiating special security provisions for international cooperative programs, as well as providing interface between defense and security officials of allied and other friendly countries on issues of mutual concern.

Some years ago, the Multinational Industrial Security Working Group (MISWG) was formed which was devoted to working with our security counterparts in Europe to standardize and streamline security procedures so they complement rather than complicate international cooperation. Among other accomplishments, we have agreed to what is known as the "program security inspection." It is supposed to be completed at the start of a project and outline security procedures that will support program goals and schedules.

Some of the other specific areas being discussed are policies and procedures concerning visits; movement of classified information across borders; common language for use in memoranda of understanding; the role of a security officer; and development of a security plan to cover how classified information is processed on computer equipment (the U.S. has the lead). We are collaborating in development of a contract security form similar to a DD Form 254 that can be used internationally (the French have the lead); and in preparation of a general paper on the impact of EC 92 (Italy has the lead).

Because the National Industrial Security Program (NISP) is a reality, our progress in international matters is being undertaken with cognizance of the NISP as well as the MISWIG initiatives. We are attempting to better define the security requirements relating to classified information in the context of the security, trade, international cooperation and industrial base aspects of technology transfer. This is sort of a combination of foreign policy and national security risk management.

Specifically, we expect the NISP Operations Manual (NISPOM) will explain and graphically display how security regulations relate to export control regulations and security assistance regulations. Many industry and Government personnel involved in international programs do not understand control and compliance requirements.

The means by which we transfer classified material and technical data needs clarification. As we globalize our research and production efforts, the ways that we transfer classified information will become critical. Lack of planning for export licenses and transfer of information have impacts on multinational programs in terms of schedules and costs. Our allies have developed methods that allow them to ship data and material quicker.

Security officers should establish contractor-to-contractor security cognizance. Company security officials involved in bilateral or multilateral programs should know their foreign counterparts and their security programs. Professional relationships provide a better understanding of peculiar security needs and procedures associated with multinational programs.

Standard contract clauses now in the Industrial Security Manual should be expanded to include requirements for the protection of unclassified, controlled technical data, third party release and end user controls. These clauses should be mandatory for all foreign subcontracts. We have asked those responsible for the DFAR to follow this request.

International security training should be mandatory for all security and export personnel working for cleared firms involved in international trade. My International Programs Directorate is developing a three-tiered training program to meet this requirement. The first level would educate executive managers; the second level would provide a general overview of activities; the third level would be a week-long class which would end with an examination of some kind. Along with the training opportunities, we are looking at a manual that will address all international security program requirements.

The security official involved in international programs should have the same status in the company as the person who runs a marketing, or finance or legal department. The security officer should be privy to all aspects of the company's business, including details of foreign investment and marketing efforts. Both industry and Government representatives involved in discussions of this problem have agreed that corporate management has not generally given the security function the same status as others and rarely incorporates security into the international development activities. On the international level, without proper planning and coordination, security requirements will quickly hamper a company's ability to compete in the market. Without knowledge of the company's activities, security personnel will not be in a position to assist the firm in competition.

In formulating the policies that were sent to the President in the form of the September 1991 Report on the National Industrial Security Program (NISP), we tried to eliminate things that are unnecessary and we tried to raise expectations. As a result, the proposed NISP is a single, coherent, and integrated government strategy to safeguard classified defense information in industry. The NISP seeks standardization of security policies and procedures throughout all executive Branch Agencies and Departments. It is an example of what can be accomplished when senior management (both in government and industry) supports a security initiative.

The effectiveness of the industrial security management function is directly affected by its placement in the organizational structures and the degree of support it receives from the hierarchy of that structure.

In each of our nations, we must be able to show how sound security measures will enhance and contribute to national objectives. Demonstration of return on investment associated with a security policy, procedure or other initiative will gain the security director an influential ally in his Chief Executive Officer.

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

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

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

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

On the United States five cent piece, the nickel, the slogan reads, "e pluribus unum" which translates into english as, "From many, one." That slogan could well describe the economic, and to some extent, the political arrangement now intended by some Europeans. The opposite of that slogan, "ex uno pluribus," (out of one, many) seems to describe what has happened in the former Soviet Union, or what Norm Augustine describes as the "UFFR," the union of fewer and fewer republics.

There is a slogan on our dollar bill that pertains today, as well. "Novus ordo seclorum" means a "new order of things." Politically, economically, militarily, and sociologically there are new orders of things all over the world. What the future holds as a result of them is uncertain.

Among the institutions of the United States Government, uncertainty is pervasive.

It is probable that none of us knows how to deal with the emerging problems around the world. If you had to bet the grocery money on the future of the Serbians or the Croations on any given day, how would you choose? Or, if you were asked to speculate on the success of the European Economic Community (EEC), or the Western European Union (WEU), or the North Atlantic Alliance in its present form, what would you say.

The January 1992 issue of International Defense Review, "NATO's role in the New European Security Environment," (p. 24), predicts that:

> "NATO will perform core security functions: it will provide the foundation for stability in Europe based on democratic institutions; it will serve as a transatlantic forum for allied consoltations; it will deter and defense against any threat of aggression against its members and it will preserve the strategic balance within Europe."

The United States has expressed support for European integration, which we hope will be complementary to NATO.

At the same time, in the "ex uno pluribus" situation as well as in other nations of Eastern Europe, political and economic systems are failing. It appears that there is a transition from those failed systems to democracy. Those who pursue that change must learn that the search for democracy is never-ending. And, our notion of democracy is not tied to any one economic system. Nor, is our system allied with any particular form. Democracy can exist in the form of a republic, or a confederation like those of Canada and Switzerland. The United Kingdom and France are examples of unitary systems like the Governments of our individual states. What is important in this understanding for the so-called "emerging" democracies is that change is institutionalized in a democratic system. That means that "winners don't shoot losers," as professor Pat Conklin of the Federal Executive Institute so aptly puts it.

The Eastern European circumstances provide us with an opportunity to influence future security programs of some of the nations. A member of my staff has visited some of the countries where it was found that the ITAR had been translated from English into their language. We discouraged them from emulating that. Visits are planned in 1992 and 1993 to some of the nations to determine what their security systems are like and to acquaint them with the features of our systems, both good and bad.

We hope that our influence and that of other free nations will facilitate the spread of democratic institutions to all of the countries of Europe.

Shortly after World War II, then Secretary of State Dean Acheson said that we were in a time recreation. I believe that we are in a time like that now. Security has become a particular kind of institution in our modern world and there is a certain momentum an institution has. The past has shaped it powerfully and we need to see how tradition shapes present concerns. There is memory on one hand, and a dream on the other. The steward, for the time being is the one partly needed to keep the memory, but also one who makes sure the dreaming is done and the future vision established. That vision is essential if we are to recreate what is necessary to meet the challenges identified and many that we haven't yet seen.

That might seem hard to do in this situation of uncertainty. But, I believe also that "uncertainty" is the challenge of the ages. It will always be with us and it makes the future seem all the more exciting. And, it reminds us of a challenge from Alfred North Whitehead: "It is the business of the future to be dangerous."

I have not seen evidence yet to indicate that there is general acceptance of the need for a comprehensive definition of security that includes economic, political and military dimensions. To compete in the world that is ahead, I believe we need to promote that definition.

And, we need a strategy, as David M. Abshire concludes. (Harvard International Review, 10th anniversary issue, 1989, "Toward a Grand Strategy") He explains the term strategy as derived from the Greek "strategos" meaning the "art" of the general, not the "plan" of the general. Art is the arrangement of elements in a manner that creates a whole. To meet future challenges our common security efforts result in a piece of modern art.

"New Directions in Protecting Information"

Nina J. Stewart, Deputy Assistant Secretary of Defense, (Counter Intelligence and Security Countermeasures)

Ms. Stewart:

I wanted to especially thank the very well-respected NCMS for inviting me back to my hometown. This is my hometown here in Dallas and this is the first time that I've been back here in an official capacity in the 12 years since I've left.

I left here as a police detective in nearby Plano, Texas. I was so excited because I wanted to bring to Government a sense of service and to help fight, at that time, the Communist threat. The world seemed so much more defined back then, than it does now and I guess that's one of the real reasons that I joined because it was right in the beginning of the early '80s and we talked about the 'evil empire' and --how things have really changed now. It seems to me that history seems to surprise us with an unexpected turn of events and that's really more the norm more than anything else. That's the expected.

I wanted to relay a little story to you while my husband is off visiting the Plaza this morning, I'm reminiscing about another national crisis, one that I know something about.

I was traveling from Los Angeles to Washington for training in 1981 and I happened to be in the DFW airport. I looked up at the monitor and I saw to my absolute shock, the attempted assassination of President Reagan and the events that surrounded that. I looked closely as the Secret Service Agents wrestled a man to the ground and much to my shock, when the camera zoomed in on his face, it was somebody who I knew very well, John Hinckly, as a meek-mannered, very shy individual with whom I had gone to grade school, junior high, high school and college. That to me symbolizes the unexpected. He would be the last person who, at that time, I would think of as a presidential assassin.

By the way, my husband, who is a Secret Service Agent, doesn't count this as my achievements and special accomplishments in my life. We have some interesting dinner conversations because he's a senior executive in the Secret Service and he recently was a detail leader for President Yeltsin when he arrived a couple of weeks ago and gave his famous speech on the floor of the Congress. He heard these amazing words coming out of the former Communist's mouth and I just wanted to repeat some of those words because to me, they seem so shocking. Yeltsin said, "The world can sigh in relief. The tide of Communism which spread social strife, enmity, and unparalleled brutality everywhere, which instilled fear in humanity, has collapsed. It has collapsed, never to rise again. I am here to assure you, we shall not let it rise again in our land. The experience of the past decades has taught us, Communism has no human face. Freedom and Communism are incompatible."

To me, he said a lot more than that, obviously but those words are incredible. But despite these comments, I must also tell you that I have a counterintelligence portfolio. And when I put that counterintelligence hat on, I can tell you that the SVR is nearly as active as its predecessor, the former KGB and the GRU is even more expressive over the last four years than before. Perhaps one reason for this is that both organizations are looking for ways to insure their survivability in an impossible budget climate and under severe criticisms for their past association and past

behavior.

But having said that, I don't think that we can make the mistake of saying that the threat from the Russian child of the huge old KGB is the same as its parent. Democratization, fragmentation of authority, poverty. All of those things strike a different tune to the old refrain that we're used to. Now Russia is only one of any number of countries, former enemies, current economic competitors who are also sometimes militarily and politically allied with us, who engage in espionage.

Colin Powell once said that the real threat to him was the unknown and the uncertain. Bob Gates, the Director of Central Intelligence constantly makes the point about the fragility of the world and how that adds to the dangers. He talks about regional instability, proliferation of weapons of mass destruction and their delivery systems, terrorism and narcotics and uneven competition. Uneven competition seems to get a lot of attention these days.

My revered mentor and friend, Bobby Inman, who was also your keynote speaker last year, said we tended to think in the past about industrial espionage as a problem between competing corporations. But with the lines blurring between government espionage and industrial espionage, we have to ask whether the industry in a competing country is totally free and market driven, or is it government-owned. I think that this question is especially central and it's probably one that we haven't focused in on as intently as we now do.

The latest proposed buyout of a key defense firm, the French government-owned Thompson CSF, proposing to buy out the Dallas based LTV missile division, stands to many pundits, and certainly is taken seriously by us in the Department, as a landmark decision in terms of raising questions about the protection of the companies involved in national security, the viability of our industrial base, U.S. companies' competitiveness, and the level of globalization.

This case, which I don't know if it gets a lot of attention here but it certainly does in Washington, because it brings out the most vocal protectionists and also the most vocal internationalists. This truly is a polarizing issue. What it has focused for me, and I've spent a lot of time on this case, is that the world is so intertwined now. This means that we must more clearly define what we mean by ownership, control or influence, much more so than we did in the past. Notice that last year, discussion on classification management issues centered around events in Desert Storm.

I was over at the President's Foreign Intelligence Advisory Board then and we had conducted a year long study of intelligence support to Desert Storm and certainly there were some dissemination problems--that's well known. But I wanted to relate something that the Chairman of the Joint Chiefs of Staff said to us when asked what he thought some of the fundamental problems were that needed to be worked on from the top level. He didn't hesitate at all. He said the green doors posed for him a fundamental problem. He said that there were occasions when he learned of a program too late to have it effect the outcome of the prosecution of the war.

The question is 'is that a compartmentation problem or a dissemination problem?' and I would suggest that it's probably both. Admiral Inman said to you last year that compartments work and they do work. But I think that you wouldn't disagree that we need to strike a balance between compartmentation and dissemination.'

I also want to draw on an earlier experience I had that deals with these issues when I was a State Department olympic security coordinator in Los Angeles in 1984. We had 154 local, state and federal agencies all trying to work together as a well-oiled machine to ensure the security and the safety of millions during the game and we worked for years at this problem.

Part of the process that we tried to instill in this Olympic planning was the dissemination of information down to the people on the street who had to respond to an incident. While the purity of the games was an unqualified success--I don't think that there were any doubts about that--there were some problems. Over and over again, we

had trouble identifying who needed the information and overcoming policies and procedures which were not designed to issue to intelligence information to local law enforcement. We spend an awful lot of time clearing what should have been already trusted personnel and we kept running time and time again into the simple problem of turf and sharing of information. You can imagine what that was like with 154 agencies, but it did work and I don't want to diminish that at all.

I'm bringing this as a personnel example that I had in trying to get information to the people who need it. I also, as you know, worked on a number of other problem-solving commissions which to me, just reenforced some lessons that I'm trying to bring to my job at the Department of Defense.

We have a huge challenge at DoD because we're trying to build a seamless, and yet secure system that will allow the delivery of timely, concise, complete and integrated information to decision makers so that they can make informed decisions. And the system that we build must also incorporate counterintelligence information as a critical part of the information mix and intelligence and counterintelligence and security countermeasures must be melded as a coherent whole.

So you can be assured that, whether it's pressing forward on completion on the National Industrial Security Program and its operating manual, or whether it's relooking at the fundamentals of how we protect information in the information age, you can expect me to push very hard for a systems approach to problems where security features are taken as a package, a complete package, rather than isolated disciplines. One example that many of you might agree with me on is the domestic TEMPEST issue. I think clearly we can and are relooking at those issues, developing whether and what kind of threat we have in certain areas and incorporating the other security features that we build in a system around the TEMPEST issues.

Physical security policy is another area, and while I don't want you to misunderstand me, I am in favor of technology to solve problems and push for that. I think that we need more research and development, particularly in security areas. Having said that, I was nonetheless as non-plused as probably anyone in this room over the original proposed requirement of wholesale replacement of classified storage container locks with the new electromechanical locks for because it was so significant in terms of cost over what we already had and it was taken in isolation of the entire security package. So, while this new electromechanical lock is a GSA requirement, in DoD we will use this in places where there's a high threat, like in certain overseas spots. We will use it to protect only the most valuable information and where other security systems in place don't mitigate the vulnerabilities of other containers. I think that we have to be more flexible, more efficient, more cost-effective in how we do business. We need to develop interactive security systems that comprise the entire set of controls for security.

I view what's happening on the political scene, the disenchantment with government, the voters' perception of bureaucratic gridlock, perception of waste and fraud, as powerful incentives to change what we do in the security business as well while keeping our eye on the end goal -- better security, but reasonable procedures.

When I came to the Department I tried to talk to various customers and find out both the praises and the criticisms, and I got a good measure of both. Some of the criticisms, whether they're overblown, or not, and I think some of them are, I'd like to go over with you. I was told that our policies are still too focused on the East-West threat. I was told that counterintelligence reporting was compartmented and stove-piped and wasn't integrated with the rest of the intelligence community and that some of it was quite redundant. I was told that security policies sometimes don't discriminate between the critical and the simply important. I was told that our security countermeasures were not based on up-to-date threat assessments. And while we were criticized for failing to halt the decade of the spy, we were also criticized at the same time for being too harsh, too brutish, too unresponsive to our employee needs. We were criticized for

overregulating our customers. We were criticized for inadequate fiscal review, in other words, not knowing what things cost and a lack of program evaluation. I was told that, in many cases, where there were information systems, we were technically in the Stone Age. It was my personal opinion in my dealings and short time at the Department, that the security professionals that I meet are professionals and that they work very hard at their jobs. But I also think that it is true that each in his discipline has worked more separately than we now can afford to do and that we really need to look sideways at our partners in the other disciplines and join arms.

Regarding questions about the credibility of the classification management system, many have asked have we broken it by abusing it, and many in the public think that we have. If the public won't support the minimum needed secrecy in government, then our job is infinitely more difficult. I don't want to intrude on others much more qualified to address this issue, but maybe it is time to think again of ways to look fundamentally at the process now and think about a top-down prioritization, even a wiseman's council to get a buy-in for the things that are truly important to the nation.

I think the DCI also has the same concerns. He recently formed the task force on classification management with the explicit statement that he wants to see more openness and less classification where it makes sense.

I think that these goals are the same as my own. We spent the last number of months trying to formulate a counterintelligence and security countermeasures strategic plan for the Department that incorporates many of the things that I've said so far. It was approved last month and we're marching forward.

This plan was based on trying to achieve four goals. One is the forging of partnerships to bring more to the security arena. The concept of total quality management is where all of our employees think it is a part of their job to instill quality in each and everything that they do and to challenge outmoded systems so that we improve. Along with this partnership comes the concept of jointness. It was something that was brought home to us during Dessert Storm and continually is reinforced by the Joint Chiefs in their operating doctrine. In DoD counterintelligence has a new partnership with the intelligence side of the house, particularly with the HUMINT side. I had the luxury of sitting at the President's Foreign Intelligence Advisory Board taking shots at how the community didn't work together in the counterintelligence area but in the last year it is amazing to me to see the partnership that has formed between the counterintelligence elements. It's not perfect, we have a long way to go yet, but there is a lot of sharing that I never believed would have taken place in such a short amount of time.

I chair the National Advisory Group on Security Countermeasures. We have the same sort of goals, common standards across the board, more implementation of such things as the single scope background investigation and of course another shining example of jointness, the National Industrial Security Program--a tremendous effort mostly driven initially by industry which needs to stand long after we're all gone. It's a tremendous effort.

The principle is managing change. One of my favorite quotes is from Dan Golden's commentary when he was going through the Senate confirmation for NASA administrator. He said "if you can't measure it, you can't manage it." And that to me strikes home about how we need to think about doing business. We need to prioritize which information is the most important to protect. We need to identify the threat through the loss of information and at DoD we have a new damage assessment committee that looks broadly across the espionage cases with the goal of incorporating in a strategic sense what's been lost; getting that information to the acquisition people and operators; and determining the protection necessary based on the knowledge we gain from these things. We'll be looking to streamline management where we can and conduct cross-discipline analysis so that we can make trade-offs where necessary. We will be looking to establish more effective and efficient processes, common

standards for security clearance eligibility. All of us, I'm sure have been subject to having your clearances passed or thinking you did, and then arriving at a location and only finding that they weren't passed or didn't get passed correctly and you didn't get into the event you were supposed to or you were an hour late. We all go through that.

The third principle is nurturing excellence. I think that it's especially critical in a downsizing force that we develop clear, attractive, career paths; that we train and better prepare our managers in this dynamic new world; that we improve drastically our security and counterintelligence awareness programs; that we have good aftercare programs for those individuals who are leaving our employ, the individuals who have had for many, many, years access to the most sensitive information. We need to help them adjust to the new life. Now the principle is protecting the infrastructure. What I mean by infrastructure is that one of the common denominators in all of these international crises in recent years has been the degree to which information, both its management and dissemination, have played in the resolution of the crisis. The Department and Government as a whole are moving towards open systems architectures; interoperability; modularity; take it with you when you deploy; integrated voice, data, and imagery on demand; as well as integrated unclassified support data with traditional command and control. What this really means is that we need to focus on research and development. We need to develop multi-level secure systems and we need rapid prototyping and speedy certification and accreditation of systems or we just won't get there from here.

Looking forward, as we approach the millennium, the measure of our success will be the degree we acquire new skills, seek innovation, remain customer-focused, and pool our talents while meeting mission requirements. And when thinking about these challenges, I'd like to close this morning with a favorite quote of mine by Frederick Wilcox. He said "Progress always involves risk. You can't steal second base and keep your foot on first."

Counter Intelligence in the 90s

Oliver B. Revell

Good afternoon. You never know when you get invited to these things, what the circumstances are going to be. I was literally on the phone with Director Bill Sessions. We had a situation in Fort Worth where we had an individual go into the County Courthouse, open fire in a courtroom on the fourth floor, kill two attorneys, one Assistant District Attorney, and one private attorney, wounded two judges and a fifth individual. If this had been a federal courthouse, I wouldn't be with you. But after ascertaining all of the facts and circumstances that I could, having agents there to assist the sheriff's office and the police, I came on, but it shows you the volatility of the times in which we live.

Of course, those of us in Texas remember very vividly the Luby assassination that occurred only a year ago.

It's wonderful to come and see old friends like Maynard Anderson and get a chance to renew many of the Washington associates and acquaintances I had over those 12 years that I was back there.

It certainly was an interesting and challenging time for me. I only came back to Texas to finish my career, because this is where I'm going to stay the rest of my life, but I would say that my time in Washington was certainly a very challenging time.

It happened to occur, as we went through the most difficult times in the Cold War, at least some of the most difficult times, the beginning of the confrontation during the Reagan years to challenge the Soviets to the point where of course they could no longer sustain the challenge and backed off and as we know the Cold War has ended.

On May 1st, I received a phone call in my office here in Dallas from Attorney General Bill Barr, and he asked 'how soon could you get to Los Angeles." I went to Los Angeles that day, and by 6:00 that day we had a federal task force of over 1,800 law enforcement officers, FBI agents, ATF, Customs and so forth and we're on the streets patrolling with the National Guard and with the 7th Infantry Division and the first Marine division, the second largest major metropolitan city in the United States-- patrolling it from hostile action from our own citizens. I've been to Beirut; I've been to Vietnam, and I've never been in a situation where it was more eery or frightening to me as an American than to drive and walk the streets of Los Angeles at that time, which were dead calm by that evening because of the curfew and the presence of the military and to see 2,000 buildings burnt out; 25,000 arrests; 18,000 people that were injured to some degree or another; 1,800 of them requiring hospitalization; and 44 deaths. To see this in an American city, is to judge the volatility of our times and how we cannot take anything for granted.

Now I'm not an expert in your line of work -- I'm not an expert on classification matters. We, of course, conduct counterintelligence investigations, counterterrorism investigations, and use the product of your efforts in our work, but I'm not going to try to tell you how to do your job. What I am going to do, is take you on a little tour de force on the world as it exists today, at least from my perspective, having been in this business now for almost 35 years and let's look at how the theme of your conference 'Protecting Secrets in a World of Change' is in fact, a very, very, valid charge to

give to this community. I think perhaps that at no time since 1935 have we seen a world that is in more of a state of change and rapid transition and most of it will have some implications for the type of work that you do for the industrial and government communities that you represent.

Obviously, the biggest change in what we do came about with the demise of the Soviet Union--the breakdown of the Soviet empire which had stood since 1917 and became the largest empire in the history of the world with more power, more control and more resources than any empire in our history.

The breakup of that empire did not just happen. It was in fact, foreseen by the very people who were directing Soviet affairs. As early as 1984, the head of the KGB started giving warnings about the internal corruption within their system and the rapid development of the Western Powers in their technology and their overall economic capabilities. Yuri Andropov was a very bright man. He was a hard-line communist but he was a pragmatist. He foresaw from this vantage point of seeing everything that was happening in the Soviet Union the corruption, the decay and the inefficiencies built into that system. He saw the difficulties that the Soviet Union and its allies in the Warsaw Pact were having in competing with the West, particularly the West, as being led at that time by President Reagan and the United States.

He saw the system, as it was being portrayed from within, was totally fallacious, and yet, by the activities of the first Chief Directorate and the GRU, he was also able to ascertain the rapid increase in the use and expansion of technology in everyday life, and the expansion of the Western economies, that they were not able to keep pace.

Mr. Andropov did not last very long--he died of a heart attack--but before he died, he brought some younger faces on to the Politburo, to deal with the very rapidly changing circumstances. Two of those have become fairly well known to us: a fellow by the name of Gorbachev, and another fellow by the name of Yeltsin. These individuals were very much the pragmatic communists. They knew exactly what Andropov had been talking about and the changes that had to take place. Nothing from everything that I have read, both classified and unclassified, leads me to believe that neither Gorbachev nor Yeltsin foresaw the extent to which their system would change and the rapidity with which it would change. But certainly they foresaw the need for change and were allied for a good period of time in pursuing this change. Gorbachev, of course, through 'glasnost' and then 'perostroika' started the opening, then the restructuring of their society. Well a little bit of light shed on a very dark subject, can have traumatic results. And of course, I don't need to relate to this audience what has happened and what continues to happen.

But suffice it to say, that there is no longer a perceivable strategic threat from what was once the Soviet Union. Obviously, the Soviet military, now primarily the Russian military, has tremendous capabilities, but there does not appear to be any will to project strategically Russian forces as there might have been at various times with Soviet forces. In fact, the most likely scenarios now are area disputes and perhaps regional warfare, even perhaps with the former republics that were associated in the Soviet Union.

Every day there are new clashes that occur within the former Soviet republics, the existing independent republics of the former Soviet Union. These clashes are not only from the standpoint of philosophic, economic and political, they are also clashes from the standpoint of race, culture and religion. Race, culture and religion are perhaps the most volatile issues that man faces today and the five Moslem republics are already starting to realign their orbit and some of this realignment may pose significant threats for us. Obviously, Iran, Pakistan, Iraq, Syria, Saudi Arabia, Turkey -- they are all vying for the inside track in dealing with the Moslem republics. Within these Moslem republics, there continues to exist large non-Moslem ethnic groups, including White Russians and various other non-Moslem peoples, that try to maintain connections back with the White Russian majority in the Russian Republic.

The volatility of these circumstances certainly gives rise to the continued intelligence effort of

what is the remnants of the KGB. All during the time that we've seen the change within the Soviet system, including the dismantling of the KGB, that element of the KGB which has remained inviolate is the First Chief Directorate, which is now the First Chief Directorate of the Russian KGB. The external intelligence service, the collection service, the CIA counterpart, it is not only active, it is perhaps more active than it was in the later years of the Gorbachev era. And, they have told us that their external intelligence mechanism will remain intact and will continue to function and operate.

I can assure you from the counterintelligence standpoint that they are living up to their word. It is in fact still functioning, still operating, still engaged in clandestine operation of all types of intelligence -- economic, political, military, and technology and is extremely vociferous in its attempt to access information of this type. Now I don't know that Yeltsin will extend the apparatus of his intelligence service where it will become provocative, but it is sufficiently active that that is a possibility.

In addition, what we don't know if Yeltsin, himself, will survive. There are very significant factors and factions within the Russian republic that oppose his continuation. Not only the Gorbachev faction, but also a faction of young Turks within the military and the military is taking tremendous reductions and a tremendous loss of status and economic power within the Russian system.

As we get away from Russia itself and we go into Eastern Europe and the former satellites, we haven't seen a significant amount of change as yet in Romania and Bulgaria, but they are starting the process. In Hungary, Czechoslovakia and Poland there have been very, very, substantial changes. Unfortunately, many of the old hard-line communists have revarnished themselves and are now free trade entrepreneurs, but of course, they have maintained a network that gives us some concern, particularly on the acquisition of high technology by less than licit means.

So even in those countries where there has been a significant political change, and certainly Poland, Czechoslovakia, and Hungary would fall in that category, and of course, East Germany no longer exists, but those countries still have within them, certain elements that are certainly very much in need of and attempting to acquire high technology and information of a proprietary and or classified nature from the Western powers, including the United States.

So there is a continued concern with, particularly industrial-type, espionage from those locations. Romania and Bulgaria still remain pretty much doctrinaire problems for us. They still associate substantially with the first Chief Directorate KGB apparatus, and are still to a major extent, capable of being tasked by that apparatus. Their countries have not made much progress in the way of reform.

Now let's drop on down to the Middle East. Not only have we recently fought a war, but there has been a significant change in a number of the governments, including the government in Israel, now with the labor party coming to the forefront. And perhaps that portends very good things, but it also portends a period of instability and we already know that the Palestinian issue has not only festered since 1948 but has erupted on a number of occasions and that still, there is no clear solution. As long as the Palestinian issue and the general alignment of the Arab countries remains opposed to any sort of full settlement of Israel's existence, the existence of the Palestinian people and a homeland, then that entire area is going to continue to have security problems for the West and particularly for the United States.

There is within the United States a significant infrastructure on the part of many of these middle eastern countries through immigration, through the movement for study and in staying on in a less than legitimate basis. There has been a substantial increase in the number of middle eastern residents of the United States. Now the vast majority come here looking for economic and political freedom and have joined the ranks of our citizens and are very productive and hardworking and bear little concern.

But within this emigre community, this recent

increase in middle eastern immigration, we of course, have a residual number of both religious and political zealots who continue to adhere to the political lines of the regimes that they have represented or that they have been a part of. We have found that the development of an Iranian infrastructure in the United States has become very intensive and structured and very responsive to the needs and requirements of the Iranian government.

We found to some extent that Iraq had more of an apparatus in this country than we anticipated. Certainly, there is the potential that within the large number of middle eastern residents of the United States, there will be a small fraction that will carry out espionage and intelligence activities on the part of their intelligence services. We must give more emphasis on that within the Bureau. That is receiving more emphasis today.

We don't know the outcome of the various factions within Iran but I can tell you that Iran remains a very significant force in the Middle East and one that the United States must deal with at multiple levels and certainly their intelligence capabilities, including the ability to use their services to project terrorism is real, and it exists and it has been used and it could be used even here in the United States. So the Middle East will continue to be a Cauldron. It continues to deserve our attention from a standpoint from intelligence, counterintelligence and certainly counterterrorism.

Southeast Asia: With Vietnam now ready to open its doors more and more to the West, and its need for economic support, it does not seem to represent a very significant intelligence apparatus but it still exists as a fairly doctrinaire hard-line communist state. Its relationship with China will always be the balancing point on how much significance that we again place in Vietnam. China, itself, is perhaps the biggest question we face. Deng Xiepeng is an octogenarian, Li Peng the Prime Minister is as well. The entire leadership apparatus has been there since the Long March and there doesn't appear to be a leadership structure that has been groomed to replace them. After Tienammen Square we see that the hoped for reforms that we were looking for have not occurred and they've even retrenched and become somewhat more hard-line. There are more Chinese students studying science and engineering in the United States than any other nationality. The vast majority of them, again, have no intention of being used or tasked to carry out intelligence assignments. But I can tell you this-- mainland China considers every overseas Chinese to be a potential agent. Now, obviously they won't be able to recruit every overseas Chinese, but they will target whenever they believe that there is an opportunity for that individual to obtain information-- they will be targeted and sooner or later there will be attempts to convert that particular individual for the purposes of the mainland Chinese government. There is probably no indication of significant change, at least in the next decade with China.

On the other hand, North Korea perhaps represents an even more volatile situation. We have a dictator there who was placed there by the Russians, has been there since the end of World War II, has created a very pervasive police state apparatus, but has engaged in terrorism, sabotage and espionage, certainly not only in the Korean peninsula but elsewhere in the world. Kim L. Sung will probably pass out of existence in the next 2-4 years. His son is the heir apparent and he is even more hostile and vehement in his attitudes. The ability of the North Koreans to develop nuclear weapons has perhaps surprised the west, not that they have developed weapons, but their technology, certainly chemical and biological capabilities and the potential to be another Iraq as far as bringing us into a situation of conflict.

Again, there are a large number of Koreans in the United States, including my daughter, the vast majority are not only loyal Americans, but very patriotic Americans. But within that community, there are again, those few who can be tasked, and some have been tasked to carry out intelligence operations on behalf of the North Korean government. This is an area that should be of some concern because many of the Asian people move on into high technology positions and are very good at science and math. And so, not that they, as a race or as a culture should be singled out, but it does require us to be aware of the fact that their home countries, the countries from which they came or their fathers came, do consider them as

potential recruits in this process that continues on.

The rest of Asia, including the economic giant of Japan, will certainly pose a threat to us, as far as technology. Both technology that is acquired through joint ventures and then is essentially shunted aside for their own purposes and that which is acquired through illegal means, which has already occurred on a number of occasions. By the way, we of course have had espionage committed against us, not just by our adversaries, but by many of our allies as well or at least organizations within allied countries that have been tasked or have taken it upon themselves to acquire technology that was not available to them through legitimate means.

Perhaps the most difficult area that we will face in the United States over the next decade to deal with from the standpoint from our own security of our people overseas will be South America and Central America. We went through a very difficult time with Nicaragua, the whole situation with support of the Contras and the Sandinista regime is all fresh in our minds. The Sandinista regime is out of power but is still in place. The Sandinista regime no longer has the support of Cuba. It no longer gets a great deal of support from the former communist countries, but the Sandinista philosophies still exist.

Within the rest of Central America, we will probably see guerilla movements in terrorist organizations at least over the next decade, posing some threat to American interests and American businesses, not necessarily to us from a domestic standpoint, but at least from our people and our businesses operating in that area.

South America, probably, with the drug trafficking organizations, the guerilla movements and the economic conditions will be a very difficult area for us to function in over this next decade. Frankly, we haven't made a whole lot of progress in dealing with the drug trafficking organizations as we convict, arrest, and bring pressure upon the various cartels, Meddin, Cally and so forth. They simply replace because it is so lucrative. The money is so substantial, the risk is minimal, that they continue to ply the trade, and in fact now are moving some of their cocaine trade through the Sicilian trade through Europe and are going back into the Eastern European area where there is a tremendous increase in the amount of use of cocaine as well as heroin from Southeast Asia.

All told, and before I leave South America, Cuba remains a very difficult problem for us. The Cuban intelligence services are very good; they have compromised our own intelligence services on several occasions. They have developed excellent agents within the United States. They have been very productive and they still adhere very closely to Castro's line and he has the support of the existing government and military operations. The economy is coming apart. Cuba is in dire straits from that standpoint. Fidel Castro is a popular personal figure, and when he falls, what will emerge from Cuba will be very interesting and very challenging for us because I don't think that anyone could tell at this time what will happen.

All of this is simply that we should reemphasize the importance that we should place on security. Security of sensitive and classified information remains a very important objective for our government, for the businesses and organizations that serve our government programs.

It is not passe to be concerned about security requirements and security awareness. It is not passe to be concerned about the potential of espionage within your organizations and within the businesses and projects you are involved in. It is not passe for Americans to protect their vital interests. There may be a peace dividend but I can tell you what we do not have. We do not have a situation where we do not have those who would wish us ill, that would still take advantage of the circumstances. We still have a need; we still have a requirement; we still have a responsibility to protect the vital interests and the secrets that are so important to the maintenance of our democracy and its defense. Certainly, this organization and the community that it represents is very deeply involved in that process.

I appreciate the opportunity to be with you today and share some of my own opinions. Nobody else

has to endorse these. These are my personal opinions and you can take them as you see fit. But I do believe that it is important, particularly for the Congress to recognize, that although the Cold War per se is over, hostilities against the United States continue and security programs and security requirements are continuously essential to our well-being and the security of our nation.

State of the DISP

Gregory Gwash

Good Morning Ladies and Gentlemen.

Thank you for your gracious introduction and for the opportunity to speak before you today. It is nearly incomprehensible for many of us to fathom the array of global events that have taken place in the world since the last NCMS National Seminar - events that have radically altered the security picture of the United States and consequently the challenges that we, as security professionals must confront.

Worldwide political upheavals have only changed the environment in which foreign intelligence services target the U.S. Though the former Soviet Union no longer represents the single most serious threat to the security of the United States, the remainder of this decade of the 1990's will continue to challenge the security profession. For instance, there are now at least 22 countries with active intelligence programs operating against the U.S.! We can expect major economic, social, political and cultural stresses across the globe, particularly in the newly-established Commonwealth of Independent States. The political "dust" has far from settled in that volatile part of the world, and they're still making dust throughout Yugoslavia (or what's left of it), and new hostilities may erupt nearly anywhere at any time.

So, it's hardly a surprise that our military forces, their supporting technologies and industrial base continue to be the prime target for foreign intelligence services. The crises in the Persian Gulf heightened world-wide awareness of America's scientific prowess, ingenuity and the preparedness of its armed forces. We know both friends and potential foes covet the kind of capability demonstrated by the U.S. during that crisis.

The end of the Cold War has resulted in some surprising trends in the industrial security environment. Despite the downturn in defense contracts, U.S. defense industry continues to be of great interest to foreign investors. This is not surprising when you consider that fifty percent of the world defense market is in the United States; eight out of the 10 world's largest defense electronic companies are American; the United States sells five times more defense electronic systems and products to Europe than it buys and a large number of American defense companies have investments in Europe. To remain competitive in the global arena, companies are looking to expand their market position by forming associations with other companies (many of them American) enhancing complementary areas of expertise. It is also easy to forget with all the publicity surrounding the end of the Cold War that there are many nations who are still very much interested in remaining well-armed! The dynamic geo-political situation, as well as our domestic economic situation, has resulted in a highly charged examination of the DoD's Foreign, Ownership, Control and Influence Policy (FOCI) as it affects foreign acquisition of defense industry, and I expect that we will see significant developments in FOCI policy as the 90's progress. (For further information, contact your local newspaper!)

So, in the midst of all this conflict, controversy and consolidation, how is the Defense Investigative Service (DIS) faring? As you would expect, DIS is also experiencing significant reductions in our budget along with the rest of the DoD. Theoretically, one would think that DIS' workload would experience a simultaneous and commensurate decrease in conjunction with across-the-board departmental reductions. This, in fact, has not occurred. For example, in the past 2

years, we have only seen a 3% decrease in the total number of cleared facilities in the Defense Industrial Security Program (DISP). And, in the past year, the number of Special Access Programs (SAPs) that DIS is responsible for inspecting has increased by 20%, with that trend expected to continue. At the same time, our Industrial Security (IS) Rep ranks decreased by 7%. In addition, we are bringing the same number of initial facility clearances into the program as we were two years ago. The reason for this, we believe, is that it takes several years, as you know, for contracts which are already in place to terminate. And while it's true that we have seen a decrease in the total number of active clearances in industry, initial requests are up 13% in the first quarter of FY 92 over the same period last year. We believe many of the initial requests are due to the elimination of Company Confidential clearances, and the replacement of older workers, already cleared, by young people entering the work force for their first career jobs and clearances.

Workload in the Personnel Security Investigation Program has especially not declined, for two reasons: First, past experience has shown that dramatic decreases in active duty military personnel have only a negligible impact on the military portion of the investigative workload of DIS. So - the number of military personnel requiring the Single Scope Background Investigation (SSBI) for access to TOP SECRET and Sensitive Compartmented Information (SCI) has not decreased despite the Department's downsizing effort. Secondly, the scope of the new SSBI has increased the average number of leads that we must do on each case. For example, each background investigation now includes a Subject Interview which had not been required for the old Special Background Investigation (SBI), which comprised 50% of our background workload, and interviews of former spouses are now routinely conducted if within the time covered by the investigation. (Seems like everyone has at least one of those!) Right on the heels of the National Security Decision implementing the SSBI, DoD directed a change in the scope of the TOP SECRET Periodic Reinvestigation to now include neighborhood interviews, adding several more leads to each case.

In order to continue to fulfill our security and investigative responsibilities despite the declining resources we have to work with, we have had to implement some rather innovative management strategies. In FY 91 we spent over a million dollars on the personnel security investigations and industrial security contracting-out programs to address temporary fluctuations in work, most of it for investigations. We also have approximately 50 employees who are dual trained to perform duties as both Special Agents and IS Reps, addressing fractional manning imbalances and also reducing TDY expenditures. We have also been moving agents and reps from offices where workload has decreased, such as Southern California and New England, to areas of the country where there are resource shortages (Washington, D.C. and the Southeastern area of the country). And, as you probably know, we haven't hired a new IS Rep or Investigator since 1989! We are doing everything we can to maximize our resources, and minimize our vulnerability to future furloughs or a Reduction-In-Force.

This state of flux we're all experiencing should cause each of us as security professionals to re-examine our role and the approach we take in carrying out our responsibilities. We cannot afford to be complacent and we can no longer rely on the momentum which resulted from the publicity surrounding the numerous espionage cases in this country in the mid-80's. While those events were damaging to our nation, they certainly proved to be useful awareness and training topics to convince those involved with handling and protecting our secrets that sound security was essential. Today, however, the greatest challenge that we face is dealing with the popular perception, both in industry and government, that there is no longer a hostile intelligence threat. As security managers, our efforts must shift to ensuring that management and employees alike remain convinced that there is a continuing need to maintain efficient yet effective security practices and procedures. I believe, in spite of the continuing decline in our resources, that we in DIS have a vital role to play in ensuring you continue to receive support from upper management. In

periods of declining resources, the natural reaction of our IS Reps in the field might be to spend less time doing an inspection, cutting corners so to speak, to free time up to address the many other duties and requirements placed on our Reps. But, I believe that decreased visibility and responsiveness on our part would send an improper and misleading message to your management; that is, that DIS no longer really cares, which would surely result in your already declining security budgets being further reduced. Accordingly, I am stressing to my field managers the need to conduct quality inspections, despite reduced resources. We may not always get there on schedule, but we'll do the job the taxpayer deserves while we're there.

Another vital aspect of ensuring continued credibility concerns the government's responsibility to provide industry with credible real time counterintelligence information. I'm encouraged by recent progress in this area, and I'm pleased to report that the intelligence community is working very hard to ensure that this information will be made available. The 24 active Industrial Security Advisory Councils (ISAC's) in place across the country will, without a doubt, continue to serve an important role in maximizing our security education resources. This government-industry cooperative venture led by the Federal Bureau of Investigation allows for the polling of resources to address local security awareness issues and needs. I am encouraging our IS Reps to proactively support the establishment and continuance of ISAC's in their areas and I appreciate your organization's willingness to do the same. These cooperative efforts serve to not only enhance the partnership but also makes our jobs a little easier as we continue "doing more with less."

As if dealing with the dynamic nature of the world is not enough to keep us all on our toes - in the midst of all this turmoil, we also have the emerging National Industrial Security Program (NISP), which will eventually change the way we do business. The Government-Industry Task force has come a long way in creating the framework of this program over the last year - a program which will result in significant changes in industrial security policies, standards and operations. The Task Force Working Groups delivered a preliminary draft of the National Industrial Security Program Operating Manual (NISPOM) to the NISP Steering Committee earlier this month and it is currently back out in those Working Groups for initial review. There are several major revisions to policy proposed in the draft which have the potential of significantly reducing security costs (i.e., eliminating accountability for SECRET material). We must ensure, however, that we do not become overzealous in making sweeping changes which fail to remedy the problems which precipitated the NISP, and simply result in poorer security for the sake of uniformity. Improved security at less cost was the promise of the NISP and I will work tirelessly to achieve that objective.

All of these changes should not, however, leave you discomforted. There are many contractors, who in spite of all the upheaval have been able to maintain strong, viable security programs. Some of those facilities are being honored today as recipients of the 1992 Department of Defense James S. Cogswell Outstanding Industrial Security Achievement Awards.

This award is particularly meaningful because only 42 contractor facilities of the 11,600 cleared facilities in the DISP have met the criteria of being selected for this year's award. They are being honored today because they have demonstrated sustained security excellence over a two year period and have satisfied stringent standards of evaluation. Each nomination is carefully scrutinized al all levels of DIS and it's also coordinated with User Agency and federal investigative and audit agencies. Many are nominated, but few are chosen.

What do these special facilities have in common?

- An effective on-going security education program which reaches all levels of the organization.

- Supportive senior management who set the example and the standards for employees to follow and who devote the resources necessary to ensure a viable program is

sustained.

- A professional Facility Security Officer (FSO) who is knowledgeable of Industrial Security Manual (ISM) requirements and who has developed a relationship with their IS Rep based on mutual respect and trust.

- Classified material controls and personnel security systems which have proven to be consistently effective.

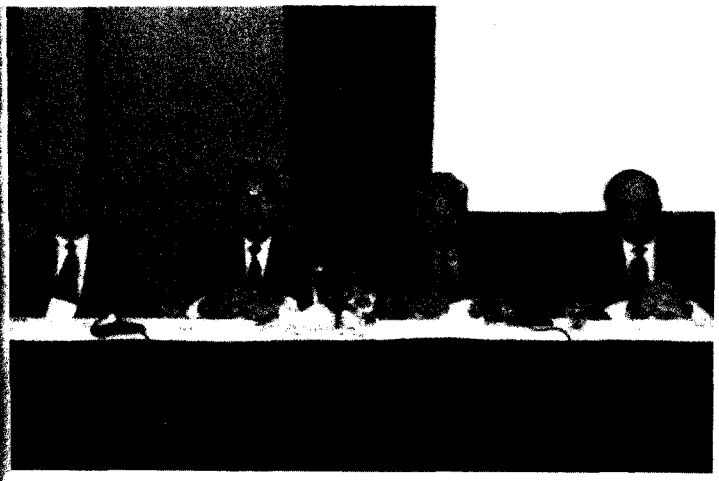
- FSO's and managers who cooperate with DIS Special Agents during the conduct of personnel security investigations.

- An informed and motivated work force who not only know but willingly implement sound security practices.

- A continuing record of commendable security inspection results.

I think we all know how difficult those criteria are to meet in this difficult time for defense industry. It's often said that anyone can successfully manage during good times, but it takes a real manager to sustain excellence during lean and troubled times.

So, without further delay, let's honor those managers and those facilities which have achieved excellence and won the Cogswell Award for 1992.



NISP Panel

Mr. Harry A. Volz
Director, Security and Transportation, Grumman Corporation.

Moderator: **Mr. Robert Schwalls**

Panel:

Mr. Steven Garfinkel
Director, Information Security Oversight Office.

Ms. Nina J. Stewart
Deputy Assistant Secretary of Defense, (Counterintelligence and Security Countermeasures).

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

Mr. Robert H. Iwai
Director of Security, Central Intelligence Agency.

Mr. William J. Desmond
Chief, Physical Security Branch, Office of Safeguards and Security, Department of Energy.

Mr. Richard Weaver
Chief, Industrial Security Branch, Office of Security, National Security Agency.

Mr. Ronald Beatty
Corporate Director of Security, Rockwell International.

Moderator:
We would like to start by opening remarks by Mr. Ron Beatty. Ron, as a member of the Aerospace Industries Association and one of the original persons who was involved in the formulation of the concept of the National Industrial Security Program, will give us a little background so that it will set the stage for the questions this morning. Following Ron, we will have some comments by Ms. Nina Stewart and she will then explain, somewhat, where we are today in implementing the concept of the National Industrial Security Program and perhaps that will set the basis so that the questions we will be posing will make more sense and fit into the overall scenario.

Ron Beatty.
First of all, I wanted to thank you all for inviting me down here. I haven't been to one of these NCMS sessions in quite a few years. You really do have quite a bit of fun here. I found out that Steve Garfinkel is a latent carnival man. It reminds me back when I was in college, I used to be into trivia and went to Yale University and we had a trivia contest. And some fellow from Princeton won and on his way up to get the prize someone who sounded an awful lot like Burt Parks, began singing "there he goes, think of all the crap he knows."

Steve also mentioned yesterday about being stale

at some of these meetings and I guess I've made so many talks too, I get a little stale too. It reminds me of last November. I had a call from a group from California and they said, "would you come down and address our group and bring us up to date on the NISP." I said "I did that last year would you get somebody else?" The program manager said well we asked Maynard Anderson and he said that he was kind of out of the loop and suggested Harry Volz and we asked Harry and Harry's doctor wouldn't let him travel so we asked Jed Selter and Jed accepted, but now he's turned it down. So with that explanation, I graciously accepted and I told them, and I'll tell you now that if you are tired of hearing about the NISP and you don't want to hear it again from a fourth choice speaker, well, why not get a jump on the weekend --it's the holiday.

I've been asked to give you a short presentation on the background directives of the National Industrial Security Program from an industry point of view. Like many of you in this room, I'm a civilian defense contractor and industry is my specialty. What may distinguish me from most of you with the exception of maybe Harry on my side is the length of time that I've been in this business. See, I started somewhere just before Project 60. Now how many in this room know what Project 60 was? A few of you do.

Project 60 was organized in the early '60s as the title suggests. Its purpose was to standardize industrial security practices and procedures, and to standardize clearance processing and place security inspection and oversight under one executive agent, the Department of Defense. The agency that handled that, if my memory serves me, was the Defense Logistics Agency, Office of Industrial Security which later envolved into the Defense Investigative Service. Project 60 was a tremendous effort on the part of the government to present one face, one voice of government to industry, and one consistent and integrated industrial security program.

To say that it was well-received is a gross understatement. Until then and dating back to the early '50s, each military agency had its own set of rules protecting classified information. Each agency adjudicated and granted clearances and they conducted compliance investigations on their contractors. As a result of that we had a mixture of regulations which were very difficult to anticipate and administer, expensive to implement and which seemed to change as often as the people of those agencies changed. The Defense Industrial Security Program has been in effect now for almost 30 years and it has been marvelously effective. When you take into consideration the number of executive branch agencies participating, some 33 at the last count, some 12,000 contractors involved, and a very highly dispersed field organization overseeing its implementation, you've got to realize that the program was built on a very, very strong foundation. That strong foundation has been a very special and unique partnership between government and industry, a partnership which was forged on trust and respect and common purpose. Like all partnerships, we didn't agree, but the mechanisms were in place, the forms were established where we could work out our differences to provide the best practices and procedures to protect our nation's technology and secrets.

You may want to ask then, if everything is so great, why the National Industrial Security Program now? Well unfortunately, as the Cold War grew, so did separate procurement functions of agencies both inside and outside the executive branch. The Atomic Energy Act of 1954 carved out the Department of Energy as they proceeded to devise their own system to protect classified information.

Executive Order 12356, signed in 1982, legitimatized a previous executive order which in effect allowed agency heads within the Department of Defense to create special access programs to control the access distribution and protect particularly sensitive information.

From 1982 on, these programs became so prolific that one was really hardpressed to call them special. They proceeded to develop their own systems to protect information and in doing so, many of them relied very heavily on the concepts employed by the CIA which is another agency that has unilateral responsibility under law to provide

protection for methods and sources for the collection of foreign intelligence.

All of the these stand-alone agencies, in addition to establishing separate security programs and the policy interpretations which shape them, conducted background investigations, adjudicated their own access authorizations and in many cases, the results of these were not accepted or even known by the other agencies.

Now we in industry offer no fault or criticism of these agencies. We have no quarrel with the reasons for which many of these programs were established. And certainly, we respect and cooperate with the people who develop and operate them -- they're our customers. We have no reason to believe that they are any less professional or less dedicated than those in the Defense Industrial Security Program collateral world. As a matter of fact, having worked on some of these programs, I can attest personally that although the procedures and cultures may be different, the professionalism and the dedication was never wanting.

In fact, there is a certain espre d'corp in these communities that is unique to them. They have a deep felt sensitivity to their programs, which on the one hand, aids in the development of good security practices, but on the other hand leaves little room to question the need.

The threat therefore, tends to become permanently postulated, the cost escalated which could make some of these programs an elaborate and expensive end unto themselves. And this has had a negative impact on industry and is the essence of the National Industrial Security Program initiative. As good as the Defense Investigative Services is, the delta between the policymaker and Washington and the operational folks in the field, sometimes gets a little wide. Add to this, if you will, a whole host of standalone independently operated programs requiring different standards, different procedures, different clearances, different access and different inspections and you begin to understand the burden to industry.

Consider if you will a contractor who has four classified contracts, one from DoD, one from DOE and two special programs, one SCI all Top Secret -- not an unusual situation. The industry employees working on the contracts are required to have at least two, perhaps three clearances, and at least three separate authorization adjudications. Three of the programs have strict accountability of documents; one uses area controls; one requires TEMPEST hardening; and three uses its own control. Data processing equipment approved by one customer cannot be used to process information for another customer. When employees travel, they require three types of visit authorization requests, and four different agencies have to be notified if they go overseas and have contact with foreign nationals. One contract requires periodic polygraph examinations, the others don't. The firm is inspected 8 times a year by 14 inspectors, from 4 different agencies, and half the employees working in security are direct charge to contracts while the other half are overhead.

It goes on and on and on. I could give you a hundred vignettes of real life examples which reflect the inefficiencies and inconsistencies these various programs create. I don't mean just mistakes, errors that we humans are prone to make. What program-driven procedures which have caused us to work around the issues at a great expense in resources. Is it any wonder then that the contractor community, a community which is generally in fierce competition with one another, united in purpose some 4 1/2 years ago and surfaced the need to take a fresh look at how well-intended security programs had become so divergent as to seriously erode our effectiveness in carrying them out. Keep in mind that the NISP initiative began before the Berlin Wall fell, and before Eastern Europe was beset by Russian history.

Two of the major thrusts behind the whole NISP initiative are to establish security policies and procedures based on an identifiable threat and at a reasonable cost. I learned yesterday that there is a third element, sensitivity. A little over two years ago the government recognized that the fresh look had mired, and initiated a feasibility study in consent with industry. Since then the President of

the United States has agreed with the study's recommendations and ordered us to proceed and fully develop the National Industrial Security Program.

To date, we have made tremendous strides. The new single scope background investigation (SSBI) with reciprocity between agencies was, I believe, accelerated as a result of this initiative. I understand that the new executive order, enabling the National Industrial Security Program, has been forwarded to the National Security Council and a new operating manual has seen its first draft.

As you all know, this didn't happen overnight. Its been a long and arduous trip involving many, many people in industry and in government--many of you sitting in this room today. What started out as an AIA initiative, has now become a joint industry task force. The leadership and membership of the National Classification Management Society have been very heavy contributors. As chairman of that task force, I want to thank you all personally and I urge you all to continue doing what you're doing.

I'd also like to acknowledge the selection of Harry Volz for the Donald B. Woodbridge Award. Harry is one of the founding fathers of this whole initiative and we are very proud of him and he certainly deserves the honor that you have given him.

Back in 1987, I gave a presentation at an executive seminar sponsored by the Defense Investigative Service in Richmond, Virginia. In the presentation, I expressed some concern about the course of the direction that the industrial security program was taking and I concluded my talk by saying, that if there was any one thing that I could point to which would materially improve the program, that one thing would be a closer nexus between user agencies, industry, and the Defense Investigative Services. I am very happy to say that in this process, that has happened. Because it had, we are making an awful lot of progress.

But there is an awful lot of progress to be made and the only impediment that I can see to affect that progress is our own resistance to change.

I had mentioned change yesterday. Let me talk about change. There is nothing more predictable in life than change. And it's not what happens, its how you handle what happens. Most people don't like change, and they resist it and become victims of it. Others, smarter, recognize the symptoms of changes, realize that it is inevitable, and change themselves before they have to.

I'm going to leave you this morning with a little story about three fellows who found an opportunity to change and it has nothing to do with the NISP. Old Joe was lying on his death bed and he knew it. He called in his three dear, life-long friends. One was a priest, one was a merchant, and one was a security officer. He told them that he wasn't going to be around very long, maybe a month at the outside. And that he had paid all of his debts and that he had donated the money he thought he should have and that contrary to the pauper adage, what was left, he was going to taking with him. He handed each of them an envelope containing $50,000 and he asked them to be the last to pay their respects and when they did, drop the money into the casket. Two days later, Joe took a turn for the worst and died. The three men attended his funeral, and as was wished, they dropped the envelopes into the casket. They later went to a bar that morning to mourn the death of their friend and after the third round of drinks, the Priest announced, "I have a confession to make." And he told the others that he had an opportunity to buy a new furnace for the parish school the day after he got the money from Joe and he took $17,000 out and bought the furnace at a greatly reduced rate and thought he could put it back before Joe died but alas Joe died too quickly. So, in the envelope that he dropped in, there was only $33,000.

The merchant then admitted that he had the opportunity to buy some merchandise at a tremendous bargain and he took $25,000 to do so, thinking that he could turn it over quickly, make a profit and then return the money before Joe died. But alas Joe died too quickly so he admitted that there was only $25,000 in his envelope.

The security officer looked at the both of them in awe. He shook his head and said that he couldn't

believe what he was hearing and he told them in no uncertain terms, "I want you both to know that my personal check for the full $50,000 is in the casket." Who saw the opportunity? Thank you very much.

Nina Stewart.
Ron pretty much explained where we stand on the NISP and the implementation of it and the history of it. I want to say that, as the new kid on the block, who kind of fell into this particular endeavor, that from my personal viewpoint, I want to give special credit to the two people who have helped lead this effort and who have inspired it. And that is Maynard Anderson and Harry Volz, my co-chair.

It made it a lot easier for me coming in as a new co-chair to a system that had already been up and running and where people were enthused. People were working well together. It's not like coming in and having to put a whole disparate group of people together. So many of the people were already working. So my job, I viewed, was to get on with the implementation of it, get on with the executive order, get on with the NISPOM, and bring us to completion.

That's pretty much where we stand now because the executive order at our last steering committee meeting was sent forward, was approved. People thought that couldn't happen and it did and Greg and his drafting team have finished the first draft of the operating manual. It's big, but its big for a lot of reasons--not the least of which is that not all of the working groups have completed their effort. So there are some gaps in it. A lot of redundancy and some issues that need to be resolved yet. But the first draft is done and the working groups are looking at this and providing more input and by the end of the summer we'll have a completed draft, at which time we will have a small team of people look at it. The first requirement is that they be real good writers and also system analysts and they are going to boil this thing down, take out the redundancies, make it smooth, and hopefully reduce the size of this and still keep intact what all of the members of the working group participated in.

That's pretty much where we stand. We've got a hot summer in front of us. We're still pushing forward to complete this. Teams are still working very, very hard and it's been a tremendous effort. So with that I think that we better get on with our questions.

Moderator
Our first question seems to fit right in with that background. The first question is for Greg. Greg, please describe for us the different working groups that are developing the National Industrial Security Program Operating Manual (NISPOM).

Greg Gwash.
There is a steering committee, as you know. Ms. Stewart and Mr. Volz are the chairs and then there are 11 working groups. I'm not sure I can remember all of them but each working group, such as Physical Security; Personnel Security; Computer Security; Threat; Resources; Inspections Oversight, and Compliance; and certainly, last but not least, is our Regulation Group, putting it all together. More importantly, each working group has both a government and an industry leader and it is generally composed of equal parts government and industry. But the important thing to know is that you are represented in each of these working groups and that no one takes a leadership role and makes a decision without some consensus.

Moderator
The next one is also for Greg. Can you just kind of tell us what this NISPOM will actually look like. For example, will it replace the Industrial Security Manual (ISM) and the COMSEC supplement and the carrier supplement of the ISM.

Greg Gwash.
Well I guess it remains to be seen what it will look like, but right now it looks like it will replace all of those documents you described as well as any other industrial security directive published by Department of Energy, the CIA, the NSA, and the Nuclear Regulatory Commission. It would be the single document that would provide source guidance to government and industry in the implementation of an industrial security program. The concept of user agencies would be expanded to include all agencies of the executive branch. So

yes, it will replace them. Now whether it will have a single format with supplements or whether the supplements that now exist, like the Special Access Program SAP supplement and the Sensitive Compartmented Information (SCI) supplement are rolled into the document, remains to be seen.

Moderator.
Next question is for Harry. Please explain to our audience, the role that industry will have in the field coordination of the NISPOM.

Harry Volz.
The first reaction to that is that industry has already had a role in the formation of the first draft that was input from all of the working groups. This first draft will be kept to the steering committee and to the working groups for review. The next step we're looking at is a coordination of similar, but not exactly the same as we have done in the past with major changes to the industrial security program, which means the various agencies, the various groups like NCMS will have the opportunity for final review. What we want to insure, is that all input that comes from industry gets fair consideration before we go to final distribution. As many of you know in the past, sometimes there have been a number of very fine recommendations that have been made that never seem to make it into a final draft. You can be sure that whatever recommendations are made, will be considered and there will be reasons why they are included or reasons they are excluded. That is the way it's going to be. How long will that take will be the next question. We expect response on this draft we've sent out by the 1st of September. The first rewrite, when you consider what the relationship is between September to the 1st of January, I would not expect something for further distribution until January, and then we'll work from there. But remember, we do not have an executive order and the schedule for that. The NISPOM implementation is one year after the executive order.

Moderator.
Our next question is for Steve. It has been reported from numerous sources, that the foreign intelligence threat will increasingly focus on obtaining proprietary company information and unclassified high technology data. Many believe that if we don't have a well-conceived and well-executed strategic protection effort, that threat will ultimately be effective. Will the NISP address the protection of unclassified technical information and require procedures to identify, categorize and safeguard, sensitive, but unclassified information.

Steve Garfinkel.
I think that what that question boils down to in terms of our approach is 'do we want a NISP in the near future?' or do we want a fully logical system that we probably won't have for years and years to come. Let me explain why I'm saying that. If we want a NISP in the near future, we will limit it to the classified world because it's the classified world that's within the domain of the executive branch and the President to control in large measure and to get things done. If we are going beyond the classified world to sensitive unclassified information of various sorts, we are going to get into the realm of a number of different statutes. We are going to necessarily involve the Congress very much in the process. And while ultimately that makes sense, and I think ultimately we have no choice but to tear down the rather artificial barrier between the classified world and the unclassified world, there's a lot of information that's classified that is not as sensitive as some information that is unclassified. It's not a clear break but, as things now stand in terms of the ability of the executive branch and the legislative branch to work on this particular subject, I just don't see that as happening in the near term. It's a subject that is extraordinarily sensitive. It's a subject that is very controversial; it gets a lot of attention from very powerful members of Congress and its obviously a subject of great interest to the news media, so it's not one that's done very easily in terms of negotiation. And because negotiation between the executive branch and the legislative branch is not currently at its all time optimal level of success, I just don't see it happening in the near term and for that reason, I think that if we're going to have a NISP in the near term, it's going to have to be limited to classified information.

Then we have to look at the long term. The thing that I hope as far as the NISP is concerned is that

the NISP makes sense, and I think it does.

Unknown speaker.
Some of you may be aware that there is another AIA task force, a very large one. A mixture of government and industry that are trying to determine at the government's direction, 'what are the critical technologies that need to be protected?' and those are unclassified critical technologies. I have attended some of their sessions and they are having a great deal of difficulty trying to make that determination. Just what is the critical technology and how do we protect it? So there are parallel efforts. Most of the people involved are engineering and procurement types so in your own corporations, you might look at that and see if any of your people are involved and get some feedback on it.

Moderator.
The next question was submitted by several so I will have to take the liberty to kind of consolidate the questions into one so that they make a little bit of sense to the scenario. Let me first read the scenario that one person submitted and I think it somewhat sets the stage for the questions:

> *"The biggest problem that I have experienced in the 12 years of being a security officer of a category A facility is the requirement to account for secret documents. The reason this is a problem is that most user agencies do not account for secret documents and do not understand why contractors can't do what we're asked to do. For example, today, a major from a U.S. Army project office came into my facility and delivered a secret document. I happened to observe him taking it out of his brief case and asked him where was the receipt. He said that he did not have one and I said that we could not accept the document. He asked my document control clerk to give him a copy of a blank receipt and then he would fill it out and give it to him. I refused and told him to return to his office and process the document in accordance with Army regulation 380-5. The major simply did not understand why he had to do that.*

Now if we all just had the same set of rules. The question for Bill, are there plans to drop the Confidential and Secret dual accountability standards?

Bill Desmond.
The question can be answered on a number of different levels and I am not prepared to answer them on all of the levels that are possible. Speaking for the Department of Energy, we have a single integrated set of requirements that are applicable to our Federal components, fields and headquarters components and to our contractor organizations. We feel very strongly as an agency that this is a policy that should be adopted by the NISP and we have recommended this to the executive leadership of the NISP. As to the consolidation of the confidential and secret levels of classification that is something that is outstanding and needs to be resolved.

Moderator.
Is there any other member of the panel that would like to comment on the question?

Greg Gwash
I would like to address that. Those of you who heard Bob read the question might notice that the facility security officer was probably a little bit unnecessarily bureaucratic in trying to enforce Army regulations on an Army officer in their facility. Do we need accountability for Secret? Well that's the question, and I guess that it remains to be determined in the process of developing the NISP Operating Manual. Many of us believe that the requirement for accountability for Secret has value and that it is not always necessary that government and industry have the same sets of rules, since we work in different environments and have different standards by which we have to live and operate. But we're open to whatever change is necessary to make the system work and be uniform and practical. But going back to this example, there was no reason why that Army major could not have prepared a receipt for that FSO to turn that document over. I don't understand why someone who has been at a category A facility for 20 years would be so rigid in the application of the rules.

Nina Stewart.
Let me tell you my personal thoughts on the issue. I've listened to both sides of the argument. I've heard the horror stories in the field about what would happen if you didn't have accountability for Secret and Confidential. I've talked to my colleagues in the other agencies. I'm not yet convinced that there needs to be a different standard. Having said that, at the same time, I think that it's my duty to let Jack Donnelly and his counterparts try to work together to try and get an agreement on a uniform set of standards. That's really what we're talking about, uniformity. I'm not going to be the fly in the ointment that stands in the way of that. On the other hand, I think that the jury's still out on that question and that we really need to look hard at that, think hard about it, look at it and separate the anecdotal information from the facts, but it is an outstanding issue.

Bob Iwai
I endorse what Nina's talking about from the Agency's perspective for the Secret and Confidential activities. The NISP, the information security working group has also made a recommendation to eliminate the accountability for Secret and Confidential documents. As Greg points out, we'll be going through that when we look at the NISPOM itself, to be processed, to be sure that equities are being protected. But you can see just within the agencies there is a little bit of separation on both what the contractors need as well on how the agencies operate. So therefore, I wanted to assure you that the working groups, which of course have both government and industry representatives on it, are working very hard. Every side of the question will be answered and we'll go back to the steering committee actually with whatever the recommendations are in the NISPOM format. Because that is the document that you all really need as an operation and maintenance manual that you have to be compliant with.

Moderator.
The next question is for Steve. The submitter says that "I think and have thought for many years that the real savings would come when the government eliminates the confidential classification. In the last year, we have already seen costs increase by having DISCO issue Confidential clearances when there are basically no protection requirements for the information other than locking it in the container. If you stop and think of the amount of dollars that could be saved by eliminating Confidential, the number may be staggering. The question for Steve is, 'is the government planning to address eliminating the classification of Confidential?'

Steve Garfinkel.
The consideration is dropping the Confidential level in the ultimate revision of executive order 12356 rather than in the executive order to the NISP, that has now been separated from that other drafting, and has moved forward as a separate entity. Second of all, I don't believe that the only requirement for Confidential information as posed in this question is that it be locked in a cabinet. In large measure, there is little difference between the maintenance of Confidential information and Secret level information. Confidential information is much, much closer to Secret classified information, and I might point out very specifically how about clearance and 'need-to-know' as the first thing that exists, than it is to unclassified information. But the fact remains that many of us, including me, believe that in many agencies, Secret and Confidential information have largely ceased to distinguish between themselves and that logically we could have a two level system, whatever you want to call them, Secret and Top Secret.

The problem is not the logic for taking that step, the problem is the practicality of taking that and the consequences of taking that step in various ways. For example, what is going to happen to all the Confidential that exists. That's a question that has to be addressed. Does it just mean that everything from now on has got to be Secret instead of Confidential? Well, if that's the case, I don't think that we're going to save a lot of money, we're probably going to end up spending a lot more money.

What are consequences on training and that sort of thing. It makes sense, again this is another situation like the previous question I had. Why don't we consider the protection of information in

a totality? What needs to be protected instead of just concentrating on classified rather than all information but sometimes what makes sense may not be practical in the near term. We are considering the effects of that. It will be on the agenda next year as we go forward with a draft of a rewrite of executive order 12356 and so I would encourage all of you to give us your views on the subject and if we should do away with Confidential, how should that be handled. Give us your views, we've heard from a number of people, from some Congressional staff, and we'd like to hear from you. Not just on that issue but on any other issue, obviously, any other issue dealing with 12356 as well.

Moderator.
Would anyone else like to make a comment?

Comment
I want to support some of Steve's position on this issue. How many of us remember when we had a category of classification in the 50's called 'restricted.' The problem was that we did away with the restricted category and we had to make a determination at that point, 'should it be Confidential or should it be unclassified.' It was a very practical exercise. 90% of it wound up being Confidential. Why? Because somebody had to make a specific determination whether to downgrade or to upgrade. So if we do away with Confidential we had better develop a very simple and direct system for accountability for what we're doing, because most people that were involved were afraid to downgrade. That something would pop up in the future that would threaten the fact that they made that decision. So they took the easy way and upgraded it. Now suddenly we have tons of Confidential material that had to be protected with much more defense if you will. As Steve said, that can be very costly. So when we do it, and if we do it, we had better develop very firm rules.

Comment
I would like to add to that. By eliminating Confidential and in the same forum discussing the abolition of accountability for Secret, we run the risk of seeing Confidential material updated to Secret and than protecting it the same way that was described in the question 'by merely locking it in a container.' I think that we have to be very careful before we start tinkering with a system that we know what we're doing and what the consequences would be.

Moderator.
I am going to go ahead with my original plan because today is Steve's 25th Wedding Anniversary and Steve has to leave us in a few minutes and for some reason he wants to go home and celebrate that 25th, so he has a 26th. So I would like to move ahead with my notes and ask those questions for Steve if I may. Steve, what is the status on the executive order that will replace 12356?

Steve Garfinkel.
As I just mentioned in passing, we are going to have revisions to 12356 and I believe those revisions will come about next year. We have preliminary drafts that we have worked on. Those drafts are going to touch largely on two areas, but again I solicit your suggestions in any areas. The two broad areas that we are looking at are the areas of enhancing our ability to declassify information, to deal with the build-up of a classified mountain of information that we will have to be able to deal with more effectively. The second is to increase individual responsibility and accountability. By individual, I mean the person, the original classifier, the security manager. We want everyone to be trained, to be educated, and to perform his or her duties with respect to classifying and declassifying and safeguarding national security information, as much as they are required to do in other areas. It's going to be back on schedule in terms of the creation of a working draft, I would say early next year. If any of you have any comments, I would urge you to provide them. A number of comments from members of NCMS are already incorporated in the preliminary draft.

Moderator.
Another question for Steve. Since executive orders frequently do not get published in an election year, will linkage, if any of the NISP to this new executive order to replace 12356, delay implementation of the NISP.

Steve Garfinkel.
Well, they are no longer linked. But I'm not going to tell you why they are no longer linked. I will let you interpret that from the question.

Moderator.
One other one Steve. How will the NISP improve our control of technology exports?

Steve Garfinkel.
Again, the question is whether the NISP, in making sense is going to have ultimately an impact on other security areas and other security disciplines. When we talk about the export of technology, we are generally talking about the export of unclassified technology as the separate problem area. There is within the NISP, an entire working group that's devoted to international issues, including export and that will be incorporated in the NISP. To the extent that I interpreted this question to mean the export of unclassified technology which is the one that comes up more often as the problem area, I think only in the sense that the NISP might be the first step in being able to look at a number of these disciplines logically and hope that ultimately the system that we develop will make more sense in that it will provide an avenue in which the executive branch and the legislative branch can work together more effectively on these issues because that is ultimately what we have to see happen.

Moderator.
Steve, the last question, the big one. Is the single scope background investigation (SSBI) achieving its objectives and are the various agencies satisfied with it?

Steve Garfinkel.
I'm going to have to limit my answer here for a couple of reasons; one, I'm often told by others that as Director of the Information Security Oversight Office I'm reminded that I have no oversight over the personnel security system for one thing. Two, I don't know, I really don't know and maybe Greg can fill this in. I don't know how well the SSBI is working in industry. Within government, I would refer to the remarks yesterday of Coach Gibbs and say that of the SSBI, there's good news and there's bad news. The good news is that there was a start made in terms of the single scope background investigation for Top Secret and Sensitive Compartmented Information.

That start has very much been kind of like a stutter start. The word hasn't gotten out like it should have. There are lots of people who are continuing to be investigated even though they have clearances that should qualify them for acceptance by reciprocal acceptance by other components but investigations continue. I've seen that repeatedly that we get a number of complaints, again, even though we don't have oversight of the system. That's a problem. I think eventually that will work itself out.

The bigger problem that I see is that people tend to look at the SSBI like it's a big deal, like we've really accomplished a whole lot. What we've accomplished is a beginning for making sense of the personnel security program. It's a very small beginning. How is it that we can have a single scope background investigation for TS and SCI but we don't have one for Confidential and Secret which account for 80 percent of the clearances. Now we have the anomaly that in some cases, the requirements some places for a Secret clearance are harder than a TS SCI clearance in terms of the investigation. The tougher questions also remain. The adjudication questions. They also have to be resolved. The "due process" question. So we've made a beginning but I hate to see us point to the SSBI and pat ourselves on the back. That's a tremendous mistake.

If that's my last question, Bob, and I appreciate that, I would like to make just a couple of comments on first of all, those of you who were in attendance and I have had questions from people who were not, the winner of the security pursuits game for the entire session was industry. Congratulations. That was rather dramatically done on the very last question of the game.
Second of all, a number of people have asked me about Coach Gibbs and Coach Johnson. Rudolph Waddy of our office was Coach Gibbs and Laura Kimberly of our office was Coach Johnson and Phil of our office played himself. I'd love to

have them stand up and be recognized but I just saw them walk out about 10 minutes ago. With that, thank you very much.

Moderator.
Our next question is for Bob. It kind of relates back to what we were just talking about on personnel security. We are waiting for the uniform personnel security questionnaire. Where is it and second, will it be adaptable for all government agencies and contractors?

Bob Iwai
Before I answer that question, let me just endorse what Steve talked about on the SSBI from the agency's perspective in the SCI work that we're doing. We think that from the investigation's point of view, it's been a tremendous step forward for the agency because now we can conduct subject interviews which we were not able to do before. So from the SCI world as far as the agency goes, we think it's a step forward for us. The idea about reciprocity is still being worked. So I think Steve's right. The assessment on the effectiveness actually of the SSBI is still out yet because we still need to get protocols done. But I know one of the agencies that endorse the SSBI, we think it's been a great find for us in helping us.

Sure, the fact that the personnel that we give access to have our personal trust. From the agency's point of view, we still strongly endorse the SSBI in finding it very useful because it empowered us actually now to talk to the subject. In the past we were not able to do that. Going back to the question that concerned the uniform personal security questionnaire. I've been working very hard on the problem. We were one of the ones behind the power curve in getting our annex into the initial draft of the NISP. We're working hard to meet the 1 September deadline that Nina has mentioned.

On the questionnaire itself, a sub working group within the committee, did outstanding work in coordinating the activities of both the government and industry. On our last meeting on the 12th of June, we approved it for submission for inclusion into the NISP. It will be part of the 1 September review.

The question about adaptability of it for government agencies and contractors. The questionnaire was initially formatted to be for industry. Larry Howe, some of you may know who is my co-chair from SAIC, was very firm in trying to make this thing government-wide as well as applicable to industry. This is maybe too big an elephant for us to eat right away. But we should not hold up the NISP work because we need the form for industry's use. We agreed in a committee that the form that we approved for inclusion into the NISP is applicable for the industrial world. We will continue to work about the applicability of that to the government side. Some of you know, actually to get some of this approved, by the Office of Personnel Management and the other bureaucratic change that we have to make it applicable to all government personnel, is really a tough hill to climb. We didn't want to hold up saying that it was linked to the government approval. This is a questionnaire to be used by industry for the government. So therefore, we approved it as an applicable questionnaire for use solely by the industry side of the house. So the work has been done. It will be out in initial draft. We wanted to thank actually both the industry and the government side of the house for working so very hard on trying to integrate multiple forms to protect each and every one of our equities, and also to make it a useful document for the contractors to utilize. We thank you for your support there. The committee has done this particular portion a little bit late but we'll still meet the 1 September deadline. Thank you.

Moderator.
Thank you, next question for Dick. Doing away with TEMPEST in the continental United States has made good sense. What will the NISP do to restrict requirements for performing the equivalently costly TEMPEST assessments by facilities in the continental United States?

Dick Weaver
I've been able to escape all the other questions up to this point and let me qualify my answer by saying that our Deputy Director for Information Security performs the TEMPEST policy functions at the national level. The question here begins

with a statement that doing away with TEMPEST in the continental United States makes sense. I'm not sure that that's a view shared by all members of government and industry at all levels. But let me try to bring you up-to-date on what's happening at the national level. Currently the TEMPEST requirements exist in the NTISSI 7000 regulation. That document is still current as of today. However there are meetings occurring as we speak to adapt and to adjust those standards that are contained at the various levels. Hopefully a product will result at the conclusions of today's meetings. And in early August that final change to the NTISSI will be presented to the TEMPEST advisory group for subsequent submission to the Committee which is chaired by Nina.

Currently, the policy specifies that TEMPEST requirements (and I'm going to speak primarily to the SCI level) can be met by shielding facilities, purchasing TEMPEST equipment or zoning. I have to say an implementation that we have stressed, continually zoning is a cost-effective alternative and I'm sure that the new guidance is going to stress that as well. I do expect some relaxation, however, to occur. Hopefully we will have a change that will hit the street and subsequently be ready for implementation very soon.

Moderator.
Anyone else on the board wish to make a comment with respect to the TEMPEST requirement?

Bob Iwai
Yes. From the agency's perspective on what we've been looking at, we're the ones, actually, that have looked at the TEMPEST threat and what can be monitored against our particular facilities as far as the people that deal with the CIA. We're the ones that are... by making the threat assessment are saying, that it has been minimized and therefore we have tried to relax somewhat the requirements actually on us. We're asking our contractors and our own people that before they start to build shielded enclosures or buy very expensive TEMPEST equipment, come and ask us the dumb question about whether they really need to do that.
Right now within our headquarter's activities, we talk about the 100 foot rule, that if you can control the 100 foot zone, you don't need tempesting equipment. If you are intruding within the 100-foot zone, come and ask us and we will try to provide you some guidance. It's still the program manager's responsibility to assess what the risks are. That's why we can tell him. People were asking us questions based upon threat, whether they had to go to the expense. We took the proactive stance of trying to be responsive actually to them. So for those activities that deal with the agency, we have reduced the level based upon the threat. The office of security is always there to provide them guidance, especially the program manager is finally accountable when we provide them the risk assessment. So that's where the agency is right now working very diligently with the other folks in order to try and apply realism actually to the assessment that they are making right now. Thank you.

Nina Stewart.
Let me also comment that if you heard my remarks yesterday, you know that this is an issue of concern for me. I've been trying to work with NSA to bring this study and all of these views together in as rapid a manner as possible so that we can bring a little more realism to the issue.

Moderator.
Ok, next question for Nina. Much of the cost of industrial security is involved with providing unique security measures for individual Special Access Programs (SAPs), Special Access Required (SARs). Will the NISP help standardize SAP/SAR security requirements and second, will the NISP require reciprocity of SAP/SAR facility accreditations?

Nina Stewart.
The goal of the NISP as you well know is to standardize equitable security issues at each level. The goal of the NISP is clearly to standardize SAP/SAR security requirements. SAP/SARs, particulary in the Department of Defense as you know, is a very high-level issue. Deputy Secretary Atwood personally approves each new SAP proposal or disapproves it, and he disapproves a number of them. I think the department is trying very hard to get a reign on the issue from the most

senior levels. The goal of the NISP is to make these reciprocal and to make them standard. You may want to add something to it, Dick, but that's my view. Ok, he concurs.

Moderator.
You all realize that as elements of the NISP are completed, they have the potential for being implemented immediately. Such was the SSBI. In connection with SAPs and SARs, one of the things that we propose as an experiment is that in the area of inspections of SAPs, where in a single facility there are several SAPs with the same customer, rather than having several inspections that a single inspection would occur for all of the SAPs from that separate customer. As part of the pilot program in that effort, we have just had such an inspection. Instead of six different occasions, with six different inspection teams, one inspection team handled all six programs. It was accepted as working. So that's an effort now that's part of the NISP that's going to be further experimented with, but eventually you must see that eventually the ideal is is that all of the SAPs and SARs could be inspected by single agency. That's not easy but we made a step forward by consolidating all the programs from a single customer.

Moderator. x
Next question is for Greg. In the past, a frequent answer to the industry challenge to excessive customer user agency security requirements has been shut up, do it, we're paying for it. Question, will the NISP provide a more effective means for challenging excessive security requirements laid upon contractors?

Greg Gwash.
I'm not sure why this question was pointed at me. Obviously the defense industrial security program doesn't operate this way. I don't think anybody's ever said, "Shut up, we pay for it." We might have said shut up, the ISM says so but that's a slightly different issue. I think Nina and Harry both addressed this question already by saying that excessive security requirements won't exist in the NISP and if a requirement is levied on a contractor that's beyond the scope of the NISP operating manual or the appropriate supplement that that would be an improper requirement and would not have to be followed, that there would be a recourse to the policy officials of the agency involved to resolve the problem. There's also going to be a NISP policy advisory committee comprised of government and industry that would also be a forum for resolving something like this or at least surfacing it. I don't expect this to be a problem. If it is, the NISP will not work.

Nina Stewart.
Let me just add to that too. You know, a lot of times when you set policies and procedures we sit back in Washington and think we've done our job, but sometimes there's a wide gap or maybe a small gap between what we think the policy says and how it's being carried out and individuals who are carrying out the actual implementers may interpret something a little differently. That's always been the problem.

Because we have a new NISP, just like Steve was talking about the implementation of the SSBI, it seems a little jerky, there are some people who don't have the word. I wrote that down. I'd like to go back and see who doesn't have the word. But you know, those kinds of problems, unfortunately I think are going to plague us until the end of time. I think the fact that the NISP has a forum with the NISPAC where industry is represented, I believe is to allow some of these issues, if they can't be resolved at the executive agent level to be brought up. I think that is a difference that exists or that will exist in the future.

Harry Volz
I have two comments. The first is that the quotation is not exactly correct. The quotation is, "What the hell do you care so long as you get paid for it?" That's the contracting office's comment. Now the worst comment, the one that is even more difficult for me in this issue is the contractor's comment. The contractor's comment, those of you who know me know I get all upset over and that is the one that where the contractor says, "I'll do anything you say, just bring your checkbook." These are basic elements of the NISP that says we are not going to do that anymore. One of the things we built into the NISP is oversight. One of the responsibilities that the Information Security Oversight Office (ISOO) will

have is kind of casual inspections that look for deviations from the NISP. The Executive agent has the responsibility for implementing the program, there's no doubt about it. He's going to do the inspections along with DOE and the CIA. But to make sure that we don't have those two quotations in one form or another anymore, there will be oversight so that if it happens, by if you will, the person I refer to as the "rogue." The rogue will be revealed and the executive agent will deal with that person. The system has these checks and balances built into it. The government and industry in this country can no longer afford that kind of cost attitude if we wish to be competitive in the world.

Moderator
Next question for Nina? What relationships, if any, do programs such as Operations Security (OPSEC) and SSE or Systems Security Engineering have with the NISP?

Nina Stewart.
The relationship is that they're part of the NISP. These are program issues that are addressed like personnel security and physical security issues are addressed in the NISP. That's the relationship.

Moderator.
The next question for Bob. The NISP takes a refreshing position that requisite security measures should be keyed to threats. Question; How will the government provide threat information to contractors so that they must assess vulnerabilities in proposed realistic protections and countermeasures?

Bob Iwai.
Well, the question was addressed to myself, but within the NISP itself there is a threat working group that makes threat data available to industry on a timely basis. The upcoming publication of Harassments and Provocations will be given to the threat working group for distribution. I don't know whether Nina would like to answer this question on what else the threat working group will be looking at as far as future plans go.

Nina Stewart.
Part of the problem early on was just simply cataloguing the available material that is out there and then identifying requirements for other kinds of information. That's something that the threat working group is cataloging the products. We're trying to go out and identify the shortfalls and fix those shortfalls. The threat working group had to handle really two issues; the first to make very clear the determination that industry was indeed a legitimate consumer of intelligence data. It seems like it's easy to say but a determination had to be made. It was made by the work of the threat working group. That's a major issue to overcome.

The second thing of which you had to deal with for years in industry is that everybody who walked through the door was the source of threat. You were never quite sure on any one given day that you wouldn't have four or five different people walk into your facility with different concepts of what the threat is. So the next goal of the threat-working group was to determine if a single source could be developed for distribution of data. That also has been accomplished. So that when a time comes for determination of threat, it will come from a single source to you, that you don't have to worry about, that you have built a room to spec, that you may have to paint it a different color blue. That's over. Those determinations have been made and will appear in a manual.

Moderator.
Next question. Greg. The traditional concept for transmission of classified information from one facility to another has involved paper transfers. The emergence of electronic transfers, computer to computer and fax to fax, by means of encryption devices adds a new dimension to the concept of transmission. The current ISM is ambiguous on the marking and recording requirements necessary to transmit or receive classified information electronically. Question; Is there additional guidance on this subject proposed for either the existing ISM or the impending NISPOM. If so, is there any indication as to how it will be addressed?

Greg Gwash.
I'm not sure I remember the question. It's a good thing I have it written down. The guidance and the ISM is a little ambiguous about transmission by fax and computer. We think it's all there but

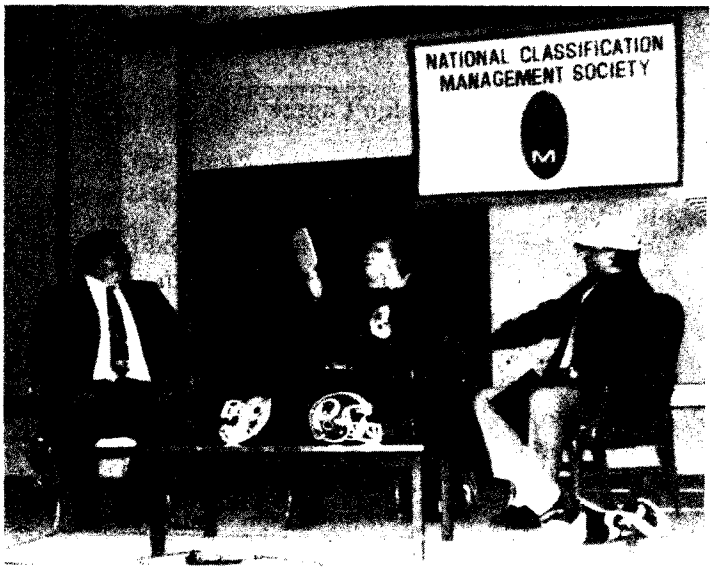
it's scattered throughout the manual. We will consolidate it. We are consolidating it in the NISPOM and hope to have a clear policy in that area. This involves network policy as well. That's an evolving problem that NSA is currently dealing with just the issues of how we transmit and secure information in this changing technology state is a challenge to all of us. The ISM says hardcopy receipts are not required for fax and that also applies to AIS transmissions. You need a record of receipt and dispatch within the facility for these documents as they come in or are dispatched. Marking requirements are the same for all documentation. We've also given guidance in various publications on the marking of AIS media. It's there and it will be consolidated in the NISP.

Moderator.
I'll ask one more question and then we'll use a couple of minutes for questions from the floor. The last question is for Nina. NSA is now the central office of record for Industrial COMSEC accounts except, perhaps, for one or two more Air Force accounts. As such, NSA conducts COMSEC inspections and DIS also inspects the same account. Savings to industry and the government could be realized by having NSA or DIS perform all COMSEC inspections. Could DoD affect this in conjunction with or before the NISP?

Nina Stewart.
I don't know if this is one of the problems in implementation. I sort of suspect it is because the Defense Investigative Service and NSA have an agreement about these inspections. For exactly the purpose to avoid the duplication of the inspection. This fall, DIS will be doing STU III accounts. That frees up NSA to do the more traditional COMSEC inspections. But NSA is supposed to come in and do the audits. If DIS comes in right behind them, they're not to do the audits. That's in the agreement. I don't know whether this question related to a particular problem that someone had where there were dual inspections in a short period of time but it shouldn't be that way. Both NSA and DIS may want to comment further on it.

Dick Weaver
I would like to. There is a difference between what we do. NSA, the central office of record audits the account. They're auditing the COMSEC material in the account. Generally, that is not a security inspection of the COMSEC account. The NSA auditor is looking at the accountability of the material, not the physical security, personnel security, need-to-know issues that are associated with the account. That's the role of DIS and that's what we look at. If we come in within 120 days of an NSA visit, we'll continue to look at physical security and what have you but we do not audit the account. We don't look at the classified material system at all. Beyond 120 days, if it's been more than four months, then we do a 25 percent sample of the COMSEC accountable material. It's really not a duplication of effort, although it may seem to be, if you're not watching what we're doing. I would just add that the COMSEC auditors are not security professionals and therefore are not knowledgeable of some of the issues that DIS is looking at and performing those security inspections. I think it's a big step that the COMSEC audit functions, however, have been transferred for the STU III accounts to DIS. That's going to result in significant cross-savings. Also my understanding is the frequency of those audits on COMSEC accounts is going to relax somewhat to probably a two-year cycle.

The last thing I want to mention here is those Air Force SAP/SAR COMSEC accounts that are out there. We are slowly gathering those in and I understand 25 of those were transferred back to NSA for their inclusion in the NSA central office of records. So we are making progress in that area as well.



State of the Union for the Information Security in the U.S. Government

Steven Garfinkel
and ISOO Staff

Mr. Steve Garfinkel, Director of the Information Security Oversight Office.

I know that all of you have been hearing about change. You've either heard me say it. You've heard Nina mention it this morning. You've heard it from all over. All of the geopolitical changes that are going on in the world are having a major impact and will have even a greater impact on security professionals in the ensuing years. Right now and even in the next few years. One of the problems that I've noticed, and one of the things that I've seen is that most of the voices telling you this are the same old voices.

For example, this is the 12th NCMS National Seminar that I've had the pleasure of addressing and, while I would like to avoid it, when you've been heard that many times, your voice and your message become just a little bit too familiar and perhaps just a little bit too stale. It is for that reason that newer voices, voices like Nina, some of those who bring into this field a wealth of other experience are so critical to what we're doing. I thought that rather than you hearing me again, I would bring before you this panel. I was lucky to have join us a couple of people who, over their careers, have demonstrated their ability to cope and adjust, and to change and to be successful in what they do. Now neither one of the these two individuals happens to be a security professional, but I have had the opportunity to hold lengthy discussions with both of them to describe the various policy areas that we deal in, so I'm comfortable that their insights will be very worthwhile as we cope with change.

My first guest has led the Washington Redskins to four superbowls over the past 10 years, including 3 Superbowl championships. Please join me in welcoming Head Coach Joe Gibbs.

Coach, first of all I want to thank you for being here this morning and, especially, I want to congratulate you on January's latest superbowl win.

Joe Gibbs (Impersonator).
Well, thank you very much Mr. Garfinkel, but I want to make one thing very clear. My role was insignificant. I couldn't have done it without the support of our owner Mr. Cooke, the dear Lord, our great coaching staff, players, and most of all, our wonderful fans.

Steve Garfinkel:
Well coach, I want to tell you that I'm very proud to count myself as one of those fans.

Joe Gibbs.
Well, Mr. Garfinkel you make up a large portion of our fans.

Steve Garfinkel.
Well, thank you Coach, I guess. Our next guest has also been very successful in the same field of endeavor, coaching. Previously, he led the Hurricanes of the University of Miami to the mythical

national championship. In recent years, he's turned around fortunes of one of the National Football League's previously most famous teams. Please join me in welcoming the coach of the Dallas Cowboys, Jimmy Johnson.

Jimmy Johnson.
The lord ISOO trophy has just hung up on my microphone.
Steve Garfinkel.
Well, coach I want to thank you for joining us here this morning. We very much appreciate your being able to take part in this discussion about security.

Jimmy Johnson.
Yeah, yeah, enough to be here and all that. Hey, haven't I seen you on one of those Pillsbury commercials?

Steve Garfinkel.
Enough of that. Coach Gibbs, I'd like to get started in our first area of inquiry. That's the area that we call Information and Security in National Classification Management, the system under which we classify, safeguard, and declassify national security information. I wonder if you could give your audience some insight on that.

Joe Gibbs.
Thank you for asking. It seems to me that the critical task facing the government and information security is similar to our situation with the Redskins. By that I mean, with limited resources we must better understand what it is we really need to protect and not spend a lot of time, a lot of money and a lot of effort protecting information that is not critical to the protection of our national security. For example, why should the Redskins spend a lot of time protecting the fact that we might have an 'in the round' play in our game plan. Everyone knows that we ran an 'in the round' play in 3 of our past 4 games. It's the same in government, Mr. Garfinkel. If the world already knows something, ordinarily we shouldn't be spending our limited resources protecting that same something. This is why the whole area of classification management needs to receive equivalent attention, just like information security.

Steve Garfinkel.
Well, coach, I just couldn't agree with you more. That was an excellent answer.

Joe Gibbs.
Oh, you don't need to give me any credit Mr. Garfinkel. I couldn't have done it without the support of our owner, Mr. Cooke, the dear Lord, our great coaching staff and most of all our wonderful fans.

Steve Garfinkel.
Well, I guess you'r right. Coach Johnson, what are your views of the information security program? Coach Johnson? Coach Johnson? Information security.

Jimmy Johnson.
Huh? Information Security? Mmmm. From what I can tell, the information security is a little too passive for my taste. For example, you all are too hung up on leaks. Instead of trying to protect information, my idea to create all sorts of information. What you might call misinformation. Then its your job as the head coach to ferret out the real information from the chaff and communicate that to your players.

Steve Garfinkel.
Well coach, that idea might work on the playing field but do you think that's a good idea on the battlefield where real lives are at stake?

Jimmy Johnson.
The battlefield is the playing field-- you meatball!!

Steve Garfinkel.
OK coach. Coach Gibbs, if we could go to another line of inquiry, I'd like to see if you could comment on that's the personnel security program. You know, the program where the government grants access to classified information to eligible individuals.

Joe Gibbs.
I'm concerned. I'm very concerned, Mr.

Garfinkel, that too many people and too many agencies are looking at that single scope background investigation (SSBI) for 'Top Secret' and sensitive compartmented information and thinking that they've accomplished a great deal in the area of personnel security. There are some other questions that need to be asked, Mr. Garfinkel. What about an SSBI for Secret and Confidential. They account for 80% of the clearances.

And by the way, Mr. Garfinkel, what about standard forms? Tell me, how many forms do we have to fill out that all do the same thing? And what about adjudication criteria. These are the critical issues that always get our poor security person in hot water. And from what I understand, the SSBI for TS and SCI is experiencing a rough beginning. In fact, in some case cases, it's totally ignored.

Steve Garfinkel.
Well, coach I have to say that I've been expressing many of those same thoughts in some of my talks around security professionals.

Joe Gibbs.
You know that I couldn't have expressed it so well without the support of our owner, Mr. Cooke, the dear Lord, our great coaching staff and most of all, our wonderful fans.

Steve Garfinkel.
Yeah, they must have been in one of my speeches. Let's talk about personnel security with Coach Johnson. What are your views on personnel security Coach Johnson?

Jimmy Johnson.
Personnel Security?

Steve Garfinkel.
Personnel Security.

Jimmy Johnson.
I can't understand what you have against people with criminal records. What I found is that a convicted felon can bring some respect to your team. Why, when you come right up to the line of scrimmage, its good to know that your guy is a little bit scared about what my guy might do.

Steve Garfinkel.
Well coach, a while ago I might have said that those ideas are rather unusual about personnel security, but the way things have been going in the courts for us, I'm not sure they are so farfetched. Well, Coach Gibbs, that brings us to a subject that is going to occupy a lot of this seminar. It's already been mentioned but it's going to be talked about a great deal more. And that is the National Industrial Security Program (NISP). We had an opportunity to discuss it at length and I'm wondering if you could give us your ideas and your feelings about that.

Joe Gibbs.
Be happy to Mr. Garfinkel, I'd be delighted. I think that this is going to have a very positive impact, and not just in industrial security, but ultimately on Government security as well. And I tell you, industry deserves a lot of credit for getting the game started on the NISP but you know, we're not even finished with the first quarter yet, and I tell you, it's in that second half where it really gets important. But I do believe that government and industry do need to work together. As I was saying, government and industry need to keep working together, especially in creating an outstanding manual. I tell you, that manual is going to be the Bible of the program, the Bible of the program, Mr. Garfinkel. You just have to keep moving before the rains come and cancel the game.

Steve Garfinkel.
Coach, I hate to interrupt on your metaphor. You started out in the first quarter, and well, I thought rainouts happened in baseball, not football.

Joe Gibbs.
I'm sorry Mr. Garfinkel, it must have been Jimmy's hairspray. What I really wanted to say is before Mr. Cooke takes his football and goes home.

Steve Garfinkel.

Well coach, I have to say that I share the same sentiments with you about the NISP. I want to thank you for that excellent answer.

Joe Gibbs.
Well I couldn't have given you that answer Mr. Garfinkel without the (in unison with Steve Garfinkel) the support our owner, Mr. Cooke, the dear Lord, our great coaching staff and most of all us wonderful fans.

Steve Garfinkel.
That's right. Coach Johnson, I was wondering if you could share with the audience your views on the NISP.

Jimmy Johnson.
NISP? NISP? Oh yeah, NISP. 6'5" 285 lbs., runs the 40 in 4.75, dumb as a goalpost. Yeah, I like that NISP. Ain't like your typical Redskin sissy player. Heck, if you listen to Mr. Gibbs here, you would think that his Redskins players were Marine Biology majors from Stanford and worked on global warming in the off season.

Steve Garfinkel.
Well, coach I really have to agree with you. There is a world of difference, a world of difference, between your typical Redskin's player and your typical Cowboy's player.

Jimmy Johnson.
Yeah!

BUM
Hey pal, could you spare a dollar for a working man, down on his luck.

Joe Gibbs.
No, my friend. I think a dollar won't do you half as much good as this will. Here son, take the words of the Lord. Let that Bible go and embrace this book. God bless you son. Where did you come from?

BUM
Hey mister, do you want to play?

Jimmy Johnson.
Who knows? There must be something in this here book that helps the Redskins. Tell you what, I'll give you two bucks for this book.

BUM
She's right. 100% profit in under a minute.

Steve Garfinkel.
Gentlemen, I apologize for that interruption. The people at the office said that you couldn't take Phil anywhere, and I didn't listen. So sorry. Coach Gibbs, with your indulgence, I would just like to address one last question to you. You know, the people that do the traditional security disciplines - Information Security and Personnel Security - are very often different people, and as a matter of fact, very often, in completely different organizations than the people that are working on Information Systems Security. I'm wondering if you could give us your ideas about whether you think that dichotomy is a good idea both from an organization and a security perspective.

Joe Gibbs.
I'm a little concerned about this fellow back here, Mr. Garfinkel. He reminds me a great deal of Dexter. We helped him out..I think he gets three chances. Now to get back to the question you asked, Mr. Garkinkel, the answer is 'No'. To me there must be far greater integration between information systems security and the other security disciplines. It seems to me that most of the greatest stress to our security, particularly in the present and the in the future are in the area of information systems security. Now, as I see it, channeling these threats requires technical expertise, particularly in some cases. But on the other hand, our good-ol' traditional security countermeasures can still be utilized. The other point that I want to bring up is that technical people should not dismiss the expertise of the security specialist. And now that I think of it, Mr. Garfinkel, our security specialists must not be threatened from pursuing information systems security because of a phobia about the advancement in technology that our great country has made. God bless our country, Mr. Garfinkel. One other point I want to

make. Unless we can integrate these disciplines, I feel that we're just certainly waiting for disasters to happen.

Steve Garfinkel.
Well, coach I want to thank you for that insightful answer. And I also want to thank your owner, Mr. Cooke; I want to thank the dear Lord; I want to thank your great coaching staff and players; and most of all, I want to thank us wonderful fans.

Joe Gibbs.
Well said, Mr. Garfinkel.

Steve Garfinkel.
Well Coach Johnson, I'm wondering if you have any final words before we end our program here for the seminar.

Jimmy Johnson.
Well, yes I do, Mr. Garfinkel. Just one last thing. And it's the most important thing that either of us have said here today. (Plays tape record "Hail to the Redskins" theme.)

Applause.

Security Impacts of the Revised DoD Acquisition Management System: DoDD 5000.1 and DoDI 5000.2

Ronald L. Taylor

Imagine yourself at a World War II B-17 Bomber base, somewhere in England, in the year 1943. Imagine the posters on the walls of the operations facilities (for those of you not old enough to remember, remember the scenes from old movies shown late at night, or the recent movie "Memphis Belle") - the posters emphasize the motto "Loose Lips Sink Ships". In your imagination, look out the window at the flightline to see the "modern" security provided the airdrome - the pride of young America in uniform vigilantly guarding the bombers with their M-1 rifles slung over their shoulders, braving the adversities of the British weather, proud of their country.

Now, picture the 1992 state-of-the-art security provided our critical wartime assets and stealth aircraft, and the modern behavioral science security awareness methods we employ to protect today's sensitive operations - posters emphasizing the latest security motto; and the pride of young America in uniform vigilantly guarding the bombers with their M-16 rifles slung over their shoulders, braving the adversities of the weather, proud of their country. NOT MUCH CHANGE?

How can we get the security dollars and technologies to provide a more effective security system, to employ state-of-the-art security educational and awareness techniques. In California, we are spending thousands to educate and change personal habits of commuters to reduce cars on the freeways. Over one billion dollars was spent to protect the identity of DoD spacecraft flying on Space Shuttle missions, while the newspapers and TV commentators degraded the DoD's efforts with their own analysis of activities.

The answer to these questions and issues, as well as the challenge to our security and classification management professionals, lies in the recently fielded DoD Instruction, Acquisition Management. For the next few minutes, we will look at this directive, its implications to the security professional, and classification management in particular. Through this look, we can begin to see that there is a system that has been harnessed to assure that acquisition programs, the intended use of a significant segment of the DoD budget, consciously understand what needs protection, against defined vulnerabilities, with specifically defined countermeasures and costs.

Let's look first at the new Acquisition Management Directives. In an effort to both streamline the acquisition management structure with DoD and to assure cost control, a senior acquisition executive was appointed for the DoD, and for each of the services. For major programs, a Program Executive Officer was appointed who reports directly to the service chain of command. The structured acquisition program was redefined to place emphasis on first, that the acquisition would be reviewed by a Defense Acquisition Board (DAB) at specific milestones; that the system user, or operating command define what they needed BEFORE establishment of an acquisition program office (the source of most of our DoD contracts); and that specific information be provided to the DAB related to costs, performances and schedule.

How did this impact security? Section 5F of the DoD Instruction 5000.2 requires the development of a Program Protection Plan which clearly defines what requires protection in the form of Essential Program Information, Technologies and Systems (EPITS); a phased security concept for protecting

the EPITS at all locations, against defined vulnerabilities; associated costs; technology control plans; and disclosure lists. Section 6J directs the establishment of a System Security Engineering Program to assure that security is treated as a system engineering task to design in security measures to counter vulnerabilities identified to exist in the weapons system's intended operational environment. These actions are a recognition that national security considerations exist in not only the protection of classified information, regardless of location, but also in the protection of sensitive technologies against economic and political adversaries throughout the acquisition process.

The basic issue being addressed is whether our security and classification management programs are meaningful, myth, or magic. Often, development of security classification guidance tends to be relegated to a junior staff officer who, through schedule or manpower constraints, often resorts to reincarnating an existing guide for a similar system, changing names and titles, and publication. When the guide is coordinated through the security office, a typical response, due to the same constraints placed on the action officer, seems to be a review of the guide's format and distribution for consistency with service regulations, leaving the content without critical review. When inspecting agency offices for compliance with security directives, the inspectors often evaluate the contents of the safe, of what had already been determined to be classified without questioning the custodian's knowledge of what required protection, marking, and handling. The Program Protection Plan approach provides a system to correct this problem.

Although we are moving in the right directions within the DoD we still have no centralized security management structure that manages all security discipline areas and concerns itself with mitigation of all security threats, not just those of intelligence collection. Government responsibility for computer security, communication security, TEMPEST, physical security, and operations security policy often falls under separate functional organizations, even when all activities are directed toward protection of classified information, equipment or operations. To confuse matters more, there is no single "Security Risk Analysis" management approach. Computer security espouses one methodology, TEMPEST another, physical security another, and operations security their five step approach. A myriad of "security plans" are required. We often find ourselves in opposition to our program management who wants security based on cost effectiveness, and others who want a "standard approach", regardless of location or environment. In days of reduced DoD budgets, this conflict can reduce our credibility, or enhance it. Recognition of the problem is the first step to getting well. To that end, we are now beginning to focus on economic threats, technology losses, and how these can be stemmed during the acquisition design and production periods. The centralization of many of these responsibilities under the Deputy Assistant Secretary of Defense for Counterintelligence/Security Countermeasures is another step. An Acquisition System Protection Office has been formed within the acquisition community to review program protection measures at each program's Defense Acquisition Board. Making security make sense requires the efforts of all of us. We need to understand the details of the programs we support. The program managers will look to us to assist them in meeting contractual requirements - determining what needs protection, when, where and at what cost - all potential contract tasks from DoD program offices. The Program Protections Plan approach provides a system to do that.

Why can you expect to be tasked through the contract Statement of Work? Why would this be an area of proposal evaluation? Because acquisition managers have a central focus. One general officer stated, "There are two kinds of decisions - budget decisions and others. The others don't count. To assure that security costs and risks are identified and considered with the numerous other system requirements, security must be integrated into the system for consideration. The new acquisition directives have done just that. Examples of this can be seen in many programs. Over $39 Million was avoided in the Consolidated Space Operations Center Program. Several million more in the Titan IV Program. Approximately $100 Million in the Air Force Satellite Control Program. He doesn't always have the manpower to accomplish this task. But he can contract the

effort.

From this discussion, we can understand the need for Program Protection/System Security requirements to support identification of what must be protected, provide documented rationale for education, understanding and implementation purposes, provide a risk analysis approach that is accepted by the different "security communities", and provide a sound rationale for acceptance of security costs. In essence, the Program Protection approach is a method to make security make sense - ensure that we are protecting the right things at the right time in the right places the right way.

DoD customer requirements are the basis for technology development, concept definition studies, system acquisition, and theater operations. We, as classification management professionals play a part in each area. The acquisition process consists of four distinct phases leading to operational use of the weapon system. The first phase is the Concept Development Phase (Phase 0) which begins after DoD acceptance of a service Mission Need Statement (MNS). The concept phase is the period in which contractors develop a system concept which will meet the requirement defined in the MNS. Phase I begins after the concept approval by the DAB and seeks to demonstrate, or prove, that the technologies conceptualized can meet system requirements. Once approved, Phase II provides the engineering and manufacturing activities to put shape to the concept. Phase III is the production and deployment phase where the prototype system is tested, produced and provided to the Military for operational use (Phase IV). A Program Protection Plan is developed during Phase 0, the Concept Definition Phase, by the government, or by the government through one of its contractors, which provides the analytical basis for protection through the entire developmental cycle. It also provides the system security management approach to assure that as the system is deployed, that security measures are defined in those activities to provide the secure operational capability in its eventual operational theater.

The focus of the program protection is to determine what to protect and the costs to protect the system throughout this developmental period. The analytical process to determine these is the heart of the protection plan. Once the EPITS are identified and assessed against their value to an adversary, their importance and vulnerabilities at specific locations can be determined. In turn, candidate security measures can be assessed for effectiveness, cost, ability to implement, and other critical trade off factors, the most effective security measures for computer and software systems, communications, facilities and operational procedures can be determined, the degree of risk to be accepted determined and costs identified. The results of the plan analysis is presented to the DAB at the Milestone I decision point for approval, funding, and inclusion in program directives. The DAB is concerned with assuring that all program costs are identified and budgeted. Although the contractor agrees to implement provisions of the Industrial Security Manual at no cost to the government (as stated on the contracted signed DD Form 441), other security costs for OPSEC, TEMPEST, protecting unclassified sensitive information/technologies, Product Security, System Security Engineering, and perhaps supporting development of the Program Protection Plan are direct, reimbursable costs. Through this analysis, program protection costs are identified and presented to the DAB. Using this process to determine the system EPITS, changes to existing classification guidance may be indicated; changes to contractor DD Forms 254, Security Classification Specification, may be needed; and potential changes to contractor statements of work to assure that those elements of information or technologies that are sensitive but not classified are protected.

How is the analysis in the Program Protection Plan different from System Security analysis described in MIL-STD-1785, System Security Engineering Management, and directed in DoDI 5000.2 Section 6J. System security is a "system design" activity, used to assess vulnerabilities in the operational rather than the developmental environment. System security activities take place concurrent with and as a part of other engineering design, fabrication, test and production/installation and deployment actions. Development and secure software operating systems during the design

system security impacts. Program protection assures that the development is conducted in a secure environment and system security activities include software design measure to assure that the processing system cannot be subverted or penetrated when used in the operational computer complexes. System security activities are not industrial security, overhead costs to the contractor, but are direct cost, statement of work tasks. They involve development of a contractor System Security Management Plan as a contract deliverable document, and similarly a System Security Concept, Vulnerability Analyses, Security Trade Off Analyses, Security Manpower Impact Assessments, Security Software Specifications, Security Test and Evaluation Plans - but only as directed by the contract Statement of Work.

In many instances, contractor support is tasked through the Statement of Work to develop or update security classification guidance and to prepare analyses required for the Program Protection Plan. As the system integration or Prime System Contractor, they are in the best possible position to understand, analyze and determine critical and sensitive system capabilities, state-of-the-art technologies, technical interfaces, operational employment concepts, and single failure point vulnerabilities. With that information availability, they will be frequently tasked to provide the Program Protection and System Security Vulnerability and Adversary Value/Mission Analyses.

As this program concept matures and expands, the role of the security professional is sure to expand. The program management elements of both DoD and contractor organizations will seek advice and assistance. New positions are already being established. Your support and experience is invaluable. Your expertise is needed. At the newly organized Space and Missile Systems Center, we offer industry orientations to assist you and your corporate staffs in both understanding the process and the tasks being placed on the Request for Proposal. We have provided workshops, seminars, and are in the process of developing updated training sources for these activities. A security database is being developed to interface with the NAVY TECNET system to provide an information sharing computer assisted network of acquisition security professionals.

We look forward to working with each of you as we continue to make security make sense through our classification management process. Major Don Proft, Space and Missile Systems Center Director of Acquisition Security, encourages your requests for further information. Thank you for your attention and participation in the NCMS.

BIOGRAPHIES OF SPEAKERS

ROBERT L. AMICK, JR.

Mr. Amick is the Director of Ethics, Security and Industrial Safety Services at E-Systems, in Greenville, Texas. He is the Ethics Program Director, and responsible for the management and direction of all Security, Industrial Safety and Medical Center activities within the Greenville Division. Mr. Amick began his present assignment in 1986.

Born in Beckley, West Virginia on 21 August 1939, Mr. Amick graduated from Gordon Military College in 1959; Marshall University with a BBA in Banking and Finance in 1962; and Michigan State University with a MS degree in Criminal Justice in 1971. His military schooling includes the Thai Language Course, Special Forces Officers Course, Counterterrorism Courses, U.S. Army Command and General Staff College and the Air War College.

Mr. Amick began a second career as Project Manager and Security Manager for the EC Corporation, Huntsville, Alabama in 1984. He was responsible for the implementation of a Security and Law Enforcement contract for the Kwajalein Missile Range, Republic of Marshall Islands.

In 1985, Mr. Amick became the Assistant to the Resident Director and Security, Safety, and Support Services Manager, Huntsville Engineering Center, Lockheed Missiles & Space Company, Inc. He directed all security, safety and industrial hygiene activities; planned and coordinated budgetary functions, facilities management; and managed transportation functions for the Engineering Center.

Mr. Amick assumed his present position in 1986. He provides direction for the Ethics Program and plans and directs all Security, Industrial Safety and Medical Center activities for the Greenville Division. Uniquely, his organization has become a key element in the marketing and acquisition of many special access programs. Operational Security is an essential ingredient in the application of security to new business acquisition.

Mr. Amick is married and has two children. Adam is assigned to the 17th Special Operations Squadron in Okinawa, and Erin attends Belmont University in Nashville, Tennessee.

MAYNARD C. ANDERSON

Currently, as the Assistant Deputy Under Secretary of Defense (Security Policy), Office of the Deputy Under Secretary of Defense for Security Policy, he is responsible for policies and procedures concerning international security programs, special access programs, NATO security and foreign disclosure and technical information systems. He chairs the National Foreign Disclosure Policy Committee which determines what classified weapon systems the United States will share with friendly countries.

Mr. Anderson's prior experience includes: Assistant Deputy Under Secretary of Defense (Counterintelligence and Security), 1988-1991, with responsibilities for the management of DoD investigative, security and counterintelligence programs. He served as the focal point for counterintelligence and security policy matters within the Department of Defense and provided day-to-day oversight of world-wide DoD counterintelligence activities. In addition, he served as Chairman of the Advisory Committee for the DoD Security Institute, the DoD Polygraph Institute, and the Defense Personnel Security Research and Education Center, and chaired the National Advisory Group/Security Countermeasures. He was Director for Security Plans and Programs, Office

of the Deputy Under Secretary of Defense for Policy, 1982-1988, with responsibilities for reviewing and formulating policies that govern the security practices and programs of the Department of Defense. He also served as the United States Representative to the NATO Security Committee; Member, Director of Central Intelligence Security Forum; Chairman, National Industrial Security Advisory Committee; Chairman Physical Security Review Board, Department of Defense; and Chairman, US/Canada Security Committee.

Deputy Director for Security Policy, Office of the Deputy Under Secretary of Defense (Policy), 1978-1982, with responsibilities as principal deputy for Special Access Programs and Sensitive Compartment Information Programs.

Director, Special Security and Special Activities, Department of the Navy, 1973-1978, with responsibilities as principal staff and operational advisor concerning Sensitive Compartmented Information Programs. Served as a member of the DNI Security Policy Committee and as the Navy Member, Director of Central Intelligence Security Committee.

Assistant Head, Internal Security Division, Naval Investigative Service Headquarters, 1969-1973, responsibilities for the supervision and conduct of investigations concerning protection of classified information, sabotage, espionage and subversive activities, as well as counterintelligence operations. Supervising Agent, Naval Investigative Service, Guantanamo Bay, Cuba, 1968-1969.

Special Agent, Naval Investigative Service, 1962-1973, with supervisory or special assignment duties including: Special Operations Group, Headquarters, 1966-1968; Senior Resident Agent, Saigon, 1964-1965.

Investigative duties with commercial firms concerned with insurance and labor relations matters, 1954-1956 and 1959-1962.

Mr. Anderson's military service was with the United States Army Counterintelligence Corps as a Special Agent, 1956-1959. He was born in 1932 in Iowa, is a graduate of Luther College and the Federal Executive Institute. He has served as editor of the journal of a profession law enforcement and security association. He is an Honorary Faculty member of the Defense Security Institute, and has been a guest lecturer concerning intelligence and foreign relations at the George Washington University. He received the Presidential Rank Award of Meritorious Executive in 1985. In October 1989, he received a Distinguished Service Award from Luther College. He is the 1990 recipient of the National Classification Management Society's Donald B. Woodbridge Award of Excellance.

RON BEATTY

Ron Beatty has been in industrial security for over thirty years. He is currently the Corporate Director of Security for Rockwell International. Prior to this, he was Director of Security for Rockwell's North American Aircraft Division; Director of Corporate Security for General Dynamics Corporation, St. Louis MO; Manager of Security for the Electric Boat Division of General Dynamics Corporation; and Director of Security for the Lycoming Division of Avco Corporation.

Mr. Beatty has been very active in security organizations throughout his career. He served for several years on the Board of Directors of the American Society for Industrial Security, and is past President and Chairman of the Board. For the past two years, he has been Chairman of the National Industrial Security Program Industry Task Force, and is immediate past Chairman of the Industrial Security Committee of Aerospace Industries Association. He is a former member of the State Department's Overseas Security Advisory Council, the International Association of Chiefs of Police, and several other professional affiliations.

Mr. Beatty has a BS degree from Fairfield University; did post graduate work at George Washington University and served in the U.S. Army Counterintelligence Corp.

STEVEN BOSSELER

Steve Bosseler, Special Agent, U.S. Customs Service, joined the Federal Government in 1983 as a Special Agent with the Central Intelligence Agency's Directorate of Security. In 1984, he transferred to the U.S. Department of State and served as a Special Agent with then Secretary of State George Shultz' protective detail, as well as an assignment with the overseas Counterterrorism branch. In 1989, Bosseler transferred to the U.S. Customs Service, Office of Enforcement, Los Angeles, as a Special Agent investigating violations of the arms export control act, and more specifically, illegal exports of military weapons systems. Investigations have included the undercover role of international arms broker, and lead investigator on a recent prosecution of a Los Angeles based engineer/businessman for exporting an Air Force owned software program utilized in missile and SDI research.

Agent Bosseler holds a Masters and Bachelors of Science Degree from Northern Arizona University. He is currently assigned to the Tucson, Arizona office where he continues to specialize in illegal arms exports.

LOUIS J. BOUCHARD, JR., CPP

Mr. Bouchard is Deputy Director, Corporate Security, with responsibilities for Special Programs at Grumman Corporation. He also currently serves as the Chairman of the Contractor SAP/SAR Security Working Group (CSSWG) and is the Co-Chair of the National Industrial Security Program (NISP) SAP Working Group.

Prior to joining Grumman Corporation six years ago, Mr. Bouchard was employed by Eastman Kodak Company for twenty-four years, in various security positions, including FSO and Security Manager for Special Programs.

Mr. Bouchard holds memberships in the American Society for Industrial Security, the National Classification Management Society, the Industrial Security Working Group (ISWG) and the Contractor SAP/SAR Security Working Group (CSSWG). He is a former member of the ISWG Board of Directors and has served on the CSSWG Board of Directors for three years.

He has been designated a Certified Protection Professional (CPP) by the Professional Certification Board of the American Society for Industrial Security.

Mr. Bouchard holds a B.S. Degree from the Rochester Institute of Technology and has attended numerous Government and private sector management and professional courses.

DEBORAH CARROLL

Ms. Carroll is currently assigned in the International Security Directorate in the Office of the Deputy Under Secretary of Defense for Security Policy. She is an employee of the Defense Investigative Service

Ms. Carroll is a working member of the U.S. delegation to the Multinational Industrial Security Working Group consisting of all NATO nations less Iceland and participates in the U.S/Canada Security Committee and the Defense Trade Policy Working Group. She is deeply involved in the development of the International chapter of the NISPOM and related changes to the new Defense Trade Regulation. Mrs. Carroll also is involved in the development and negotiation of various international security agreements. She is a member of the Society for International Affairs and is involved in its activities on classified exports, re-exports and its Licensing Advisory Board. She recently completed an article with an industry counterpart on how the ITAR, the ISM and the SAMM interrelate.

While at the Defense Investigative Service Ms. Carroll specialized in international transfers, the role of freight forwarders in commercial and foreign military sales, and establishing better communication between industry, Customs and the State Department. She received the Capital Region Industrial Security Representative Award of the the year for 1990.

Prior to joining the Defense Investigative Service, Ms. Carroll served as the Administrative and Security Officer for the White House Liaison Office, National Park Service. In this role Ms. Carroll was responsible for establishing and managing the security program to support White House Construction Activities.

Ms. Carroll is a graduate of the University of Michigan with a specialty in Southeast Asian Studies. She had credits toward a Masters from American University.

WAYNE R. COFFRON

Mr. Coffron, Senior Security Supervisor, joined AAI Corporation in 1987 after serving ten years as an officer in the United States Military Police Corps. He is a graduate of the University of San Jose, San Jose, CA and Jacksonville State University where he received his Master of Arts degree. Mr. Coffron is FSO qualified.

Mr. Coffron's responsibilities at AAI include Supervision of the AIS element in Corporate Security, SPP development and implementation, AIS user Training, Programmer/Analyst and System Administrator courses for Evolving Technologies, Inc., San Diego, CA.

Mr. Coffron is an active member in the Information System Security Association.

JOSEPH R. DEGREGORIO
"JOE D."

Joseph R. DeGregorio is the Director of Industrial Security, Defense Investigative Service, Southwestern Region. A native of St. Louis, Missouri, he received his undergraduate degree in Radio-Television Journalism from the University of Missouri, Columbia, Missouri, in 1970. In 1979, he received a Master's degree in Public Administration from Long Beach State University, Long Beach, California.

Joe served as an Industrial Security Representative from 1975 to 1979 in Los Angeles, before becoming the facilities Division Chief at the St. Louis Cognizant Security Office in 1980. He stayed in that position until 1983. In 1983, he and Greg Gwash, now Deputy Director for Industrial Security at DIS HQ, established the first DIS office in West Germany. Upon his return from Europe to St. Louis in 1986, he started his current position as Director of Industrial Security, Southwestern Region. The Region is now located in Irving, TX.

Joe is a member of the National Classification Management Society. Disabled American Veterans, American Legion and National Journalism Society. His hobbies include tennis, entering contests and helping the community/parish.

WILLIAM J. DESMOND

Mr. Desmond currently serves as the Chief, Physical Security Branch in the Policy Standards and Analysis Division of the Office of Safeguards and Security, Department of Energy Headquarters. He has twenty-five years of experience in government security programs at both the Headquarters and field element levels.

Mr. Desmond was graduated from the College of the Holy Cross, Worcester, Massachusetts with a Bachelor of Arts Degree. He holds a Master of Science degree from Florida State University, Tallahassee, Florida.

Mr. Desmond is married to Sheila Coughlin Desmond. They have five children and reside in Frederick, MD.

EUGENE G. DUNSMORE

Eugene G. Dunsmore is currently the Chief, Classification Management and Contracting Officer for Security Matters, Lockheed Missiles and Space Company headquartered in Sunnyvale, California. He has over thirty-six years experience in government/Industry Security. He has previous experience as a Navy Midshipman, Air force Aviation Cadet and Provost Marshall. He attended Oklahoma University and Syracuse University, and holds a B.S. degree in Business Administration from Notre Dame College. He was employed by General Electric for eight years in Security Management working with NASA, Army and Air force. Mr. Dunsmore has twenty four years experience with Lockheed in Program Office Management and Classification Management. Eugene has served the National Classification Management Society as a member since 1981, as a speaker at the 1982, 1987, 1988, and 1992 national Seminars; 1983 Program Chairman and the 1984 and 1992 Chapter Chairman and Seminar Chairman for the 1983 Mini-Seminar, of the Northern California Chapter; and as a speaker at numerous Chapter meetings including Dallas/Fort Worth and Northern California.

STEVEN GARFINKEL

Steven (Steve) 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 reports annually to the President on the status of the information security system. He began his federal service in 1970 in the Office of General Counsel of the General Services Administration. His positions in that office included Chief Counsel for the National Archives and Records Service, Chief Counsel for Information and Privacy, and Chief Counsel for Civil Rights.

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). He is a member of the District of Columbia Bar and has received numerous Presidential and Federal Service citations and commendations, including the Presidential Rank Award of Meritorious Federal Executive. In June 1989, the American Defense Preparedness Association presented him with the *"Security Man of the Year Award"* and in October 1990, the National Classification Management Society named him an *"Honorary Member"*.

JOHN B GASTON

Mr. Gaston is the Director of Security and Facility Security Officer, for McDonnell Douglas Technologies, Inc. (MDTI), San Diego, California. Before joining MDTI he was the MCAIR YF-23 ATF Security Manager in St. Louis. He joined MCAIR after completing a career in managing scientific and technical intelligence, operational intelligence, command and control, and special security activities for the USAF. His military career included two tours at the Foreign Technology Division, as Chief of Security and Chief of Advanced Research; two assignments at the Aerospace Medical Division, as Director of Intelligence; a tour to Det 3, 619 Tactical Control Squadron, Palgon Son, Korea, as Operations Officer and Senior Battle Director; and assignment to the 18 TFW, Okinawa, Japan, as chief of Operational Intelligence; and a tour to Paddy Control, Can Tho, Vietnam as a Weapon's Controller during the 1968 Tet Offensive.

Mr, Gaston has also represented the USAF on multiple Intelligence Community working groups involving Biomedical Research, Chemical Warfare, and Man-in-Space. He is a member of several professional associations and working groups (NCMS, OPS, AFA, ISAC, CSSWG and AFIO) and has given various presentations including one to the Third National Operations Security Conference. Under his leadership at MDTI, his Security Awareness team received the Secretary of the Air force *"Security Education Activity of the Year"* for 1991.

TRACY GULLEDGE

Tracy Gulledge, Technical Publications and Staff Writer, Department of Defense Security Institute, graduated from Park College with a B.A. in English. She holds an M.Ed. In Educational Leadership from the University of West Florida. Prior to coming to the Defense Security Institute in March 1985, Tracy was a special agent with the Defense Investigative Service, assigned to the Southeastern Region. In her initial position at the Institute was as a course developer in the Correspondence Course Division. She is currently a technical publications writer in the Educational Programs Department, and staff writer for the *Security Awareness Bulletin.*

GREGORY A. GWASH

Greg Gwash, Deputy Director (Industrial Security), Defense Investigative Service, a native of Minnesota, 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. He is also the Government Co-Chair of the Regulation Working Group of the National Industrial Security Program Task Force, responsible for drafting and assembling the NISP Operating Manual. Prior to his appointment as Deputy Director (Industrial Security), DIS, in October 1990, he was chief of DIS's Office of Industrial Security for the DIS Pacific Region, headquartered in Long Beach, California. From 1983 to 1987, he was chief of DIS's 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. Prior to his Federal civil service, Greg served in the United States Army's Special Forces, including duty in Vietnam from 1965 to 1967. He is also an inactive member of the California Bar Association.

RICHARD L. HARPER

Richard L. "Rick" Harper is currently the Security Manager for LTV Aircraft's efforts on the B-2 "Stealth" Bomber. He began his security career 14 years ago as an officer in the Army Counterintelligence, and still participates as a Major in the reserves. Rick also served as a special agent with the Central Intelligence Agency prior to entering the industrial security field. He worked as a security representative at several contractors before accepting his current position. Rick has been an active participant in NCMS, holding the positions of chapter chairman, chapter vice chairman (2 terms), chapter recruitment chair, and publicity chair for the 1992 National Seminar. Rick and his wife, Susan, have one daughter Kelly. He received a BS. from Midwestern State University, and an MBA from Dallas Baptist University.

MARILEE HOOD

Marilee Hood, a native of Oklahoma, obtained her bachelor's degree in Business Education from Northwestern Oklahoma State University. In her current position, she is one of two Computer Security Specialists for the Southwestern Region of the Defense Investigative Service, with primary responsibility for the states of Texas, Oklahoma and the lower one-third of New Mexico. Prior to her appointment to the Defense Investigative Service in February 1991, she was the ADP Facility Security Representative for the Defense Contract Management District - South. From 1980 to 1987, she worked for the Environmental Protection Agency as their hazardous waste program Data Administrator. She has also held positions with the National Bureau of Standards and the General Services Administration. Prior to starting her federal civil service career, she was a high school teacher.

Ms. Hood is active in assisting the local National Classification Management Society in establishing an AIS special interest working group.

ROBERT HUBBARD

Robert Hubbard was appointed to his present position as Deputy Chief, Headquarters Personnel Security Branch, office of Security Affairs, U.S. Department of Energy on September 7, 1991, after serving as a Senior Personnel Security Specialist at the Department of Energy (DOE) for six years. He transferred to DOE in December 1985, after employment as a Program Analyst at the U.S. Office of Personnel Management's Office of Federal Investigations (OFI) from March 1974 to December 1985. Prior to employment with OFI, Bob was an officer in the United States Navy, and Principle of a private school in Atlanta, Georgia. He received a BA degree from the University of North Alabama and a MA degree from Auburn University.

While at OFI, Bob was responsible for interacting with the government's personnel security community on many issues affecting security clearance processing and Federal employment suitability determinations. He served as OFI's representative on numerous interagency study groups addressing problems in the security community, and proposing ways in which to improve the system for processing clearances. He is the author of several task force reports and was involved in preparing legislation, regulations and policy documents on personnel security matters with government-wide scope and application.

In his current position, Bob supervises an office responsible for processing DOE security clearances for contractor personnel supporting DOE under Headquarters contracts; DOE Federal applicants and employees; and employees of other government agencies and offices, including also the White House and Executive Office of the President as well as the U.S. Congress. Since arriving at DOE, he has served on several interagency study groups evaluating government-wide personnel security operations. The latest such group is the ongoing National Industrial Security Program (NISP) effort to develop uniform procedures among government agencies for processing contractor personnel for security clearances.

SHIRLEY A. HUMPHREY

Shirley Humphrey is Chief of the Personnel Clearance Division, Defense Industrial Security Clearance Office and is primarily responsible for all security clearance processing actions which include: Initial clearance processing, revalidations/reinstatements/conversions, International and OODEP clearances, special access programs, periodic reinvestigations, representative of foreign cases and adverse information reports.

Previous experiences have included: Industrial Security Representative, Cleveland, OH, and Alexandria, VA; other DISCO positions have been Adjudicator, International Clearance Administrator, Special Access Program Coordinator and management/supervisory positions since 1983.

ROBERT H. IWAI

Robert H. "Bob" Iwai, Director of Security, Central Intelligence Agency, was born in Hawaii on 28 April 1936. While attending the University of Hawaii, he actively participated in the Army ROTC program, becoming Commander of the Corps. He received a BS degree in General Engineering and a commission into the U.S. Army in 1958. His wife, Janie Higgins, is employed by a local contractor.

While serving in the Army, Mr. Iwai was assigned to Germany during the start of the Berlin crisis, 1961-1964. He had the opportunity to complete his graduate studies in electrical engineering at Stanford University under Army sponsorship, receiving his MSEE in 1966. Mr. Iwai then became an instructor at the U.S. Military Academy for a three year period. He was responsible for teaching the one year basic course in electrical engineering to junior cadets. In addition to other assignments, Mr. Iwai served two tours in Vietnam.

Mr. Iwai retired from active duty in December 1978, with the rank of Lt. Colonel. He entered on duty with the Agency in January 1979, as physical scientist at Area 58. He became Chief, Engineering Division (CPG) at Area 58 in 1982, and was promoted into the Senior Intelligence Service in January 1984. Mr. Awai served as Chief, RS Division (DCG) from July 1984, until his promotion to Deputy Director for System Operations in February 1986. Mr. Iwai assumed the duties of Director of Security on 6 April 1992.

DAVID B. KENDRICK

Dave Kendrick is the Supervisor of Security Services for DISP programs at the E-Systems, Inc., Garland Division as well as a member of the E-Systems, Inc., Corporate Security Staff. He has been with E-Systems for six years. He started his E-Systems employment as a Senior Security Specialist, and was promoted to his present position in November 1988.

Dave is a retired senior noncommissioned officer from the United States Air Force. During his military career as an Air Force Security Policeman, he was associated with a variety of security projects that propelled him forward in the career field. During a thirteen year tenure at Andrews Air Force Base, Maryland, he worked distinguished visitor security and was liaison between the Air Force Security Police and the U.S. Secret Service for Presidential Support. He served with distinction during the terms of four Presidents and was the first enlisted person to receive the coveted Secret Service plaque of appreciation. Dave culminated his Air Force Special Security Officer, first with the Air Force Electronic Security Command, and then the Joint Chiefs of Staff, Joint Electronic Warfare Center in San Antonio, Texas. His military decorations include the Air Force Achievement Medal, the Air Force Commendation Medal (3 oak leaf clusters), the Air Force Meritorious Medal, the Joint Services Meritorious Medal and the Air Force Humanitarian Services Medal.

Dave has been very actively involved with the STU-III program at E-Systems since the company's initial CCI Control Agreement in 1987. He is the Alternate Corporate Command Authority for the STU-III program, and has diligently worked with DIS on STU-III issues to include the placement of STU-IIIs in contractor overseas facilities. He recently received a letter of appreciation from Headquarters DIS for his efforts with DIS Southwestern Region to provide a STU-III training seminar for other contractors in the Dallas/Fort Worth area. He is also recognized as being the sole contractor representative to contribute to a new STU-III handbook scheduled for release by the DoD Security Institute this summer.

TIMOTHY D. MAHONEY

Mr. Mahoney is the Industrial Security Program Manager, Headquarters, Air Force Security Police Agency, Kirtland AFB, NM, where he helps implement the Air Force industrial security program. He is a career industrial security processional with over eighteen years of field, staff and higher headquarters experience.

Mr. Mahoney began his industrial security career with the Defense Supply Agency, DCASR-New York in 1974. He was an industrial security representative in the New York and Springfield, NJ, field offices.

He relocated to Florida in July 1978, when he assumed responsibility for the one-man industrial security resident office in Fort Lauderdale, FL, DCASR-Atlanta. In October 1980, the industrial security mission was transferred from DCAS to the Defense Investigative Service (DIS)

Mr. Mahoney was promoted to the staff of the new DIS Northwestern Region Headquarters in San Francisco, CA in March 1981. He becamc Chief, Facilities Division, DIS.

CATHY MAUS

Mrs. Maus is an Information Security Specialist, Office of Classification, Office of Security Affairs, U.S. Department of Energy. She has been with the Department of Energy (DOE) and its predecessor agencies (Atomic Energy Commission and Energy Research and Development Administration) since 1961. Her association with the DoE classification program began in 1983 when she joined the Office of the Deputy Assistant Secretary for Security Affairs as a Program Analyst. She has been with the Office of Classification since 1987.

Ms. Maus' primary responsibilities include managing the DOE classification education and training program (including DOE wide policy development and DOE Headquarters program implementation) and the classification appraisal program.

Mrs. Maus is married and has two sons. She resides with her husband in Boonsboro, Maryland.

LEONARD S. PATAK

Mr. Patak, who has over twenty years of federal law enforcement experience, is the Special Agent in Charge of the Dallas Field Office, Office of Export Enforcement. His office has export enforcement responsibility for a five state area which includes Texas, Oklahoma, Arkansas, Louisiana and Kansas. Prior to assuming his present position in April 1987, Mr. Patak served as a Special Agent and Senior Special Agent with the Drug Enforcement Administration in Dallas and New York and as a U.S. Army Intelligence Officer in Frankfurt, Germany.

Mr. Patak graduated from the University of Dallas with a Bachelor of Arts degree in History and International Relations. He completed his graduate course work in Central European History and Philosophy at the University of North Texas.

PHILIP T. PEASE

Mr. Philip T. Pease, SCES, is the Director of the Office of Security in the Administration Organization (DDA).

Prior to his current assignment as the NSA Director of Security, appointed January 1981, Mr. Pease was Deputy Director of Civilian Personnel from January 1979 - 1981. From September 1976 - January 1979, he served as the Executive to the Deputy Director for Administration. He has also held several management positions within the Office of Security and the NSA Directorate for Administration. He served as Chief of Management Services at Bad Aibling Station from 1971 to 1974.

Mr. Pease graduated from the Hillyer college in 1953. Beginning in August 1970 to January 1971, he attended the Armed Forces Staff College, Norfolk, Virginia. He has also participated in Senior programs with the Federal Executive Institute, Charlottesville, Virginia during March - April 1980, and the Brookings Institute, Washington, D.C., in April 1985.

In March 1981, Mr. Pease received the NSA Meritorious Civilian Service Award. In 1982, Mr. Pease became a charter member of the Senior Cryptologic Executive Services. On 30 June 1986, Mr. Pease received the NSA Exceptional Civilian Service Award. The President of the United States conferred the rank of Meritorious Executive in August 1984 and again in September 1991. On 6 April 1990, Mr. Pease was presented the National Intelligence Distinguished Service Medal by the Director of Central Intelligence.

Mr. Pease, a native of Hartford, Connecticut, currently resides in Ellicott City, Maryland, with his wife Ann. They have four children; two daughters and two sons. Mr. Pease enjoys skiing, reading and woodworking.

KERRY JAMES REDLIN

Kerry Redlin is the Information System Security Officer for General Dynamics, Fort Worth Division, where he is responsible for the research and documentation of automated information systems in accordance with the Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22M), DIAM 50-3, 50-4 and 50-5 and the National Security Agency "RainBow Series" to obtain government approval. Kerry began his security career as a Security Assistant with the Fort Worth Division in 1984. He transferred to the Data Systems Division of General Dynamics in 1985 as an Automated Information Systems Security Analyst. When the need became apparent for an AIS security professional within the Fort Worth Division, Kerry was selected for the position of Senior Security Specialist responsible for Automated Information Systems Security.

Kerry's interest in computers dates back to high school where he became adept using computer systems with and without authorization. He subsequently worked in the commercial oil industry as a computer operator and security specialist.

Kerry graduated from Tarleton State University, Stephenville, Texas in 1984 with a BS in Criminal Justice and an AS in Law Enforcement.

OLIVER B. REVELL

Mr. Revell, Special Agent in charge, Federal Bureau of Investigation, Dallas Division, was born on December 14, 1938, in Muskogee, Oklahoma. He attended the University of Georgia and East Tennessee University, receiving his Bachelor of Science degree in June 1960. In 1971, he received his Master's degree from Temple University. He has also completed executive programs at the Federal Executive Institute; Kennedy School of Government, Harvard University; and the National Executive Institute of the FBI Academy.

In June 1960, Mr. Revell received a Lieutenant's commission in the U.S. Marine Corps and served four and one-half years as an aviator. He left active duty in November 1964, as a Captain.

On November 16, 1964, Mr. Revell was appointed a Special Agent of the FBI. He served in Kansas City, Philadelphia, and Tampa Divisions and at FBI Headquarters (FBIHQ) in the Organized Crime Section, Inspection Division, and the Office of Planning and Evaluation. In January 1975, Mr. Revell was promoted to Assistant Special Agent in Charge of the Chicago Division.

In October 1976, Mr. Revell was promoted to Inspector-Executive Assistant to the Associate Director. In November 1977, he was designated Special Agent in charge of the Oklahoma Division. In August 1979, Mr. Revell was designated Deputy Assistant Director, Criminal Investigative Division, FBIHQ, where he directed the FBI's programs in Organized Crime, White Collar Crime, Official Corruption and Undercover Operations. In June 1980, he was promoted to Assistant Director and placed in charge of the Criminal Investigative Division, making him responsible for criminal programs and operations of the FBI.

In January 1981, Mr. Revell was placed in charge of the Administrative Services Division where he was responsible for Personnel, Budget, and Financial Operations of the FBI. In May 1982, Mr. Revell was again placed in charge of the Criminal Investigative Services Division. In July 1985, Mr. Revell was appointed Executive Assistant Director - Investigations. In this capacity he served as the Director's principal deputy for investigative, counterterrorist, and intelligence activities. He was also responsible for all international investigation and liaison activities of the Bureau, including its Legal Attache and Interpol operations. In July 1989, his title was changed to Associate Deputy Director - Investigations and was given additional responsibilities for oversight of the Training and Laboratory Divisions of the FBI.

As a member of the President's Council on Integrity and Efficiency, he was Chairman of the council's Committee on Integrity and Law Enforcement. He was a member of the Terrorist Crisis Management Committee of the National Foreign Intelligence Board and Vice Chairman of the Advisory Group/Counterintelligence. He also served as a member of the White House Oversight Working Group on Narcotics and the Senior Review Group for the Vice President's Task Force on terrorism.

In 1989, President Bush awarded Mr. Revell the Presidential Rank of "Distinguished Senior Executive" and in 1990 the President conferred upon Mr. Revell the "Meritorious Senior Executive" award. In May 1991, he was awarded "The FBI Medal for Meritorious Achievement" by Director William S. Sessions; and in June 1991, he was awarded the "National Intelligence Distinguished Medal" by Director of Central Intelligence, William H. Webster.

As of May 28, 1991, Mr. Revell was appointed to the position of Special Agent in Charge of the Dallas Division (covering the northern half of Texas).

Mr. Revell is a member of the International Association of Chiefs of Police (IACP) and serves on its Advisory Committee for International Policy and was Chairman of the Terrorism Committee (1986-1992), and a member of the IACP Executive Committee (1990-1991). He is a member of the American Society for Industrial Security, the Texas and North Texas Police Chief's Association, the Texas Police Association, the Greater Dallas Crime Commission, the Dallas World Affairs Council and the Dallas Rotary Club.

He serves as Chairman of the Law Enforcement Explorers Committee, Circle 10 Council, Boy Scouts of America; Chairman of the Anti-Crime Inventory and Assessment Subcommittee of the Public Safety Committee, Greater Dallas Chamber of Commerce; Co-Chairman of the Public Safety Committee, Plano Family Counseling Services. Mr. Revell is a member of the Advisory Board of the Southwestern Law Enforcement Institute, University of Texas-Dallas, and the Metroplex Marine Association, as well as the American Legion.

Mr. Revell is married to Sharon Ponder Revell, a registered nurse from Mars Hill, North Carolina. They have four children: Sergeant Russell Revell, U.S. Air Force, Fort Worth, Texas; Jeffrey and Christopher Revell of Fairfax, Virginia, both employed by the FBI in Washington, D.C.; and LeeAnne Revell, a student at the University of Oklahoma.

AUGUSTINA K. SCARDINA

Ms. Scardina is currently a Security Education Instructor at the Department of Defense Security Institute. "Gussie," a native of Baltimore, MD, received her B.A. from the University of Maryland Baltimore County campus. Shortly after graduation, she was hired by the Defense Investigative Service (DIS) as a case controller at the Personnel Investigations Center. After four years in Personnel Security, Gussie transferred to Industrial Security (IS) and gained IS Rep experience while assigned to the Washington, D.C. Field Office. From August 1986, until her relocation to Richmond, VA in November 1987, Gussie was the Education and Training Specialist for the Capital Region, IDS. During her initial assignment to the Industrial Security Department of the Defense Security Institute she provided instruction for the Industrial Security Basic, Management, and Specialist Courses and served as Course Coordinator for the User Agency Inspector Course. In August 1992, she joined the Educational Programs Department where she instructs the Security Briefers Course, assists with the instruction of the Security for Special Programs Course, and creates various security education publications. She authored the self-Inspection Handbook.

Gussie is an active member of the Northern Virginia based JIGSAG (Joint Industry-Government Awareness Group) and the Washington, D.C., Chapter of the NCMS.

E. NEIL SELF

Mr. Self has been President of Trine Incorporated, Huntsville, AL since July 1990. Trine is a small business which specializes in System Security Engineering (SSE), OPSEC, Program Protection, and Acquisition Security. Mr. Self managed and participated in two ongoing contracts for NASA for the definition of SSE requirements. He provided the SSE Management Plan and OPSEC Plan for the USASDC GBI-X program. Presently, Mr. Self participates in the SDIO System Security Working Group.

Mr. Self's prior experience includes Manager, System Security and Survivability with Teledyne Brown Engineering in Huntsville, AL, June 1987 to July 1990. His responsibilities included the System Security Engineering for the NASA/SDIO Starlab Program; Manager, Security and Safety, McDonnell Douglas Astronautics Company, Houston, TX, June 1982 to May 1987. He was responsible for all industrial and program security and safety for NASA and USAF programs.

Mr. Self has thirty years of experience in security, to include extensive work in system security engineering through a NASA muti-mission contract. He also has five years experience in the development and integration of system security engineering programs with multiple agencies to include: SDIO, AFSD, USASDC, NASA and DoE.

Mr. Self organized and managed the first multi-agency SSE program within SDIO while acting as a support contractor to NASA (this plan is still utilized as the model for SSE within SDIO). He analyzed security requirements and provided innovative countermeasures which resulted in a cost savings to SDIO of some $5M.

In 1988 Mr. Self received a Bachelor of Science degree from Athens State College.

MICHAEL SKURECKI

Michael Skurecki has been employed for 19 years by PRC Inc., located in Bala Cynwyd Pennsylvania, as Senior Administrator. In this capacity he is responsible for planning, organizing, coordinating and directing various facility/contract functions which include security, Government Furnished Equipment (GFE), management, QA and finalization of contract deliverables, office maintenance and other administrative functions.

In a dual role as a security consultant, he has traveled to PRC sites in various states to provide assistance to Facility Security Officers (FSOs) and complete security tasks assigned him by the Director of Corporate Security.

Prior to joining PRC, Mike was employed for 13 years, by the General Electric Company located in King of Prussia, Pennsylvania, as a Technical Promotions Specialist.

Mike is a 1965 graduate from Temple University with an Associate Degree in Mechanical Technology as well as a 1991 graduate from Villanova University with a Bachelors of Science Degree in Business Administration.

Relative to security, he has recently authored an article which is scheduled to appear in the August 1992 issue of American Society for Industrial Security - Security Management Magazine titled, "Value of a Sound Self Inspection Program - An Effective Preventive Maintenance Tool Leading to a Sound Security Program (SSP=SSP)." He also has authored and published several articles as well as a booklet pertaining to saving the environment titled, "Ten Most Wanted Improvements for Your Daily Environmental Living."

Mike is a certified FSO, and a member in good standing with NCMS and ASIS. In 1985, the PRC Bala Cynwyd office was the recipient of the Cogswell Award, highest award given to industry for excellence in

ROBIN A. SMITH

Robin is currently Supervisor, Security Administration for AAI Corporation, Corporate Security Office located in Hunt Valley, Maryland. She joined AAI in October 1986, as a Security Administrator.

Prior to joining AAI, Robin was employed as an Assistant Contract Special Security Officer for Martin Marietta Aero and Naval Systems located in Middle River, Maryland from February 1982 to October 1986.

Robin received her Associate of Arts degree in Business Management from ESSEX Community College and is currently pursuing a Bachelor of Science degree in Business Management from the University of Maryland. She has been a member of NCMS since 1986 and was instrumental in establishing the NCMS Chesapeake Bay Chapter and has served as its Chairperson during the past year.

NINA J. STEWART

Ms. Nina J. Stewart was named to the new position of Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures) in the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). She arrived in late September 1991 and is responsible for DoD policy in virtually all areas of interest to NCMS.

Ms. Stewart has spanned the spectrum of security, law enforcement, intelligence, counterintelligence, counterterrorism, counternarcotics and national security policy.

Ms. Stewart was a police detective in Texas, where she ran a narcotics unit. She has been a special agent with the State Department. Other career highlights include State Department Olympic Security Coordinator for the 1984 Olympics in Los Angeles; Staff assistant to the Secretary of State's Advisory Panel on Overseas Security which was chaired by Admiral Bobby Inman; Staff Assistant to the Moscow Assessment Review Panel, chaired

by the former Secretary of Defense Mel Laird; and Counterintelligence Officer.

Ms. Stewart worked at the White House for four years, where she was appointed by the President as Executive Director of the President's Foreign Intelligence Advisory Board. Her supervisors have included two U.S. Presidents, a former Secretary of State, three Secretaries of Defense, a National Security Advisor, a Director of Central Intelligence, a Chairman of the Joint Chiefs of Staff and four other four-star officers, a Congressman, two Senators, and two Directors of the National Security Agency.

Her current assignment includes the management of DoD counterintelligence programs, and information protection activities. She represents the Defense Department on the National Security Telecommunication and Information Systems Security Committee; she chairs the Intelligence Community's Advisory Group/Security Countermeasures; and she co-chairs the National Industrial Security Program.

WILLIAM D. TATE

Bill Tate is currently the Director of Security at Grumman Melbourne Systems Division, which is headquartered in Melbourne, Florida. He is responsible for all security matters relating to the Grumman's role in Joint Surveillance, Tracking, and Reconnaissance System (J-STARS). Until recently, Bill was the Security and Safety Manager for Grumman Technical Services, Inc. He joined Grumman in 1984 as the Computer System Security Officer for the Space Shuttle Launch Processing System at Kennedy Space Center and has been in Grumman security management since 1985. Bill was the Facility Security Officer at Grumman Technical Services, Inc., in 1989, when GTSI was selected as a recipient of the James S. Cogswell Award by the Defense Investigative Services.

Prior to joining Grumman, Bill was employed by TRW Defense Systems Group from 1979 to 1984, as a member of the Technical Staff on an Air Force system security engineering contract at Cape Canaveral and Kennedy Space Center. He also served in the U.S. Army Security Agency/Intelligence and Security Command from 1969 to 1978, as a signal Security Specialist. While in the Army, he served a year in Vietnam, three and one half years with the XVIII Airborne Corps at Ft. Bragg, NC, and three years as the ASA/INSCOM security advisor to the Army's European Communications Command headquartered in Worms, Germany.

Bill earned a Bachelor of Arts degree in Political Science/Pre-Law from the University of Central Florida in 1982. He has been a member of the National Classification Management Society (NCMS) since 1981 and is currently the Chairman of the NCMS Spacecoast Chapter on Florida's east coast, having served in the same position in 1989. Bill is a charter member of the Florida Spacecoast Industrial Security Awareness Committee. In addition to his security duties, Bill is certified as a Total Quality Management (TQM facilitator within Grumman and is an instructor in effective management techniques.

RONALD L. TAYLOR

Mr. Taylor is currently Manager, Secure Systems Engineering, the Aerospace Corporation, Los Angeles, CA. Ronald L. Taylor was first employed by the Aerospace Corporation, a Federally Funded Research and Development Center, as a project engineer with the Space Transportation System Security Engineering Office in August 1980, having served in the USAF from 1968-1980. He has subsequently been promoted and served as manager in the Aerospace Corporation Launch Base Security Engineering and Technology Division; and the Systems engineering Division. He majored in Electrical Engineering at the Virginia Military Institute, has a BA degree in Psychology from Louisiana Tech and an MS degree in Criminal Justice from the University of Alabama. Mr. Taylor was a panel member at the 1988 National Classification Management Society Training Seminar and the NCMS Fall 1988 Dallas/Fort Worth Regional Training Seminar, a featured speaker at the 1989 ASIS Fall Workshop on *"Facing Tomorrow's National Security Issues Today"* and has been a speaker at several Organization of Strategic Defense Contractors Security Conferences.

He has played significant roles in the integration of security into critical national space programs to include the Space Boosters Program, Defense Meteorological Satellite, SDIO Space Based Programs (Brilliant Pebbles, Follow-On Early Warning System, and Brilliant Eyes), the Advanced and National Launch Systems, the Space Transportation System, and the Consolidated Space Operations Center. He also participated in or guided development of classification guidance for those programs, and the current USAF Space Launch System Security Standard, SDIO Security Policy, and the DoD Acquisition Instruction 5000.2. Mr. Taylor has also been a key participant in the development and presentation of the Air Force Systems Command's Course *"Managing Security in Systems Acquisition"* and various industry orientations on the security impacts of new DoD Acquisition Directives.

HARRY A. VOLZ

Mr. Volz is the Director of Security and Transportation for Grumman Corporation. In this capacity he manages all aspects of corporate security, uniformed forces, transportation, special security activities, and interfaces with the national counterintelligence and security countermeasures community. Mr. Volz currently serves as the industry co-chair of the National Industrial Security Program (NISP) government/industry task force.

In over thirty-seven years with Grumman Corporation, Mr. Volz has been actively contributing to the development and improvement of Grumman Corporation's industrial security policies and programs. His leadership resulted in the recipient of the first James S. Cogswell Outstanding Industrial Security Achievement Award in 1966 and several subsequent awards.

In a prior assignment as Deputy to the Vice President of Security and Personnel Services, Mr. Volz addressed challenges involving labor relations disputes, equal opportunity issues, and investigations of active Soviet espionage operations. He has also served as the Deputy Director of Security and Corporate Services for Security and Transportation and as Deputy to the Vice President and Director of Security and Corporate Services.

In 1975, Mr. Volz developed and implemented an emergency evacuation plan which safely extracted over 2,000 Americans from Iran. He provided evacuation liaison to the Department of State, Department of Defense, the Central Intelligence Agency and other corporations. He also provided evacuation guidance to non-aligned corporations at the request of Grumman Corporation and the CIA.

Mr. Volz holds a Bachelor of Arts degree from Wagner College, a Master of Arts degree from New York University, a Master of Science degree from Hofstra University, and has done additional graduate work at the University of Indiana and at St. John's University. He is a member of several industrial security processional societies in industrial and government. He is the recipient of numerous professional and civic honors. Most recently he was recognized by Secretary Cheney and President Bush for his work on the NISP.

P.S. STEVE WHEELER

Steve Wheeler is the Chief of DoD Security for General Dynamics Fort Worth Division. Steve came to General Dynamics in March 1985, as a Security Analyst and has progressively advanced to his current position as Chief of DoD Security. He is responsible for administration of the Defense Industrial Security Program at General Dynamics. His responsibilities also include managing dedicated professional security staff assigned to or supporting a variety of international direct sales programs such as the Japan FS-X Program, the Taiwanese IDF Program and the Korean Fighter Program.

Steve served with the U.S. Army Intelligence and Security Command from September 1980, to January 1985. Steve was stationed in Italy from January 1982, through January 1985, as a Special Agent and Special Agent in Charge at Livorno Resident Office, Livorno, Italy. In these positions, Steve principally served as a liaison with Italian Intelligence and Counterterrorism officials.

Steve graduated from Armstrong State College, Savannah, Georgia in 1980 with a B.S in Criminal Justice (Concentration in Criminal Law) and an A.S. in Law Enforcement.

RICHARD F. WILLIAMS, CPP

Mr. Williams is currently the principle Assistant for Special Programs within the Office of the Deputy Under Secretary of Defense (Security Policy). He also serves as the chairman of several important policy groups and is a member of various intelligence and security advisory structures. His duties have often included providing testimony before congressional committees.

Mr. Williams prior experience includes Deputy Director for Information Security and Special Programs at OSD; Assistant Staff Director of the Commission to Review DoD Security Policies and Practices, i.e., "Stillwell Commission"; first Director of Industrial Security for the DIS Capital Region (he established it as an operational entity), and Senior Physical Security Manager for Protection of Government Property and Personnel with the Department of the Navy. He was the first Executive Secretary for the National Industrial Security Advisory Committee, Charter Navy member and interim Chairman of the DoD Physical Security Tri-Service Requirements Group, and Chairman of the DoD Special Access Program Working Group.

Mr. Williams has a Master of Business Administration with honors from Georgia State University, a Bachelor of Business Administration from Memphis State University, and has served as a Senior Executive fellow at Harvard.

Mr. Williams has received the DIS Distinguished and Exceptional Civilian Service Medal as well as other awards for his work in government and academia. He has been rated as a Certified Protection Professional by the American Society for Industrial Security (ASIS) and has served as a Board member and the President of the ASIS Professional Certification Board. Mr. Williams also is an adjunct facility member at several Washington, D.C. area colleges where he teaches business administration and security courses. He and his family reside in Stafford, Virginia.