Classification Management

JOURNAL OF THE NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY

VOLUME III No. 2 - 1967

CONTENTS

Proceedings of Third Annual Seminar

Published semiannually. Annual subscription, $10. Editorial address: 201 Eye St., SW, Washington, D.C. 20024. Edward H. Calvert, Editor. Views expressed by individuals in the *Journal* do not necessarily represent views or official positions of NCMS.

PROCEEDINGS OF THIRD ANNUAL SEMINAR
Washington, D. C.
July 19-21, 1967

WELCOMING ADDRESS

by

Donald B. Woodbridge

Good morning, ladies and gentlemen. We have a few ladies, I am glad to see. It is my privilege to bring you once again greetings from the National Classification Management Society Board. Lest some of you begin to wonder if I am a fixture at the national seminar, I hasten to add that this is my swan song. Next year Dick Durham will occupy this spot. As you know, the bylaws provide that the retiring President succeed to the position of Chairman of the Board — and the opportunity to greet the seminar. Incidentally, the bylaws provide nothing for the retiring Chairman.

Last night two newly elected board members were installed: Dick Boberg and Gene Suto. Neither of them needs an introduction to NCMS. Dick made a lasting mark last summer in Los Angeles as chairman of the 1966 seminar. Dick is Manager of the Classified Document Security Section at Aerospace Corporation, and that includes the classification management office. This past year he has been chairman of the Southern California Chapter of NCMS.

Gene Suto is Director of the Security and Documents Department, including classification management, at Research Analysis Corporation, McLean, Virginia. He was secretary-treasurer of the first seminar and for this, our third seminar, he is chairman of the Budget & Finance Committee. Obviously, Gene is a good man with a dollar for they have also kept him on all three years as secretary-treasurer of the Washington Chapter. Last night we gave him the ultimate accolade by electing him national Secretary-Treasurer. He is a man you are sure to hear from.

Our new Vice President elected last night is Don Garrett, whose title always throws me: Deputy Director for Classification Management in the Office of the Deputy Assistant Secretary of Defense (Security Policy).

And our new President is Lorry McConnell, who has served us as national Secretary-Treasurer and Vice President in the past. He is head of

---

Because of space limitations, introductions, complimentary opening and closing remarks and similar material, and business reports of local chapters have been omitted from this issue. Omitted material remains a part of the official records of the Society, however, and is available if needed.

the Corporate Office of Classification Management and Editorial Liaison in the System Development Corporation, Santa Monica.

And now a brief report on the state of the Society: Our assets — this doesn't give bank balance — but our assets at the moment are $1971.40, which will take care of our *Journal* for a while. You will undoubtedly be hearing from our Secretary-Treasurer to reinforce that balance.

Our total active membership roll— which, unfortunately, doesn't mean total paid up — is 154. We lost one member by death.

Plans are being laid, as you know, for a seminar next year in San Francisco, as a joint effort between the two California chapters.

I regret that I can't announce additional chapters. We still have only the three: Washington, Southern California, and Northern California. But there are good prospects, I think, in Albuquerque, where we made Jim Marsh chairman by fiat, and in the Boston area where Ken Wilson is being very active.

The *Journal,* as most of you are aware, has now appeared in a fourth issue. The *Journal* makes good reading; sometimes entertaining, always instructive. If it reveals a certain persistent preoccupation with something called DD-254, it also lets us know that things are being done about that famous form. The men behind the walls of the Pentagon are not faceless bureaucrats; they turn out be remarkably patient and perceptive human beings, working with skill against truly formidable odds, with our interests and the country's interests uppermost.

The Society has performed a great service to its members and to posterity in recording not only its own deliberations but the words of our distinguished guest speakers. To be sure, one sometimes wonders just what posterity will make of it all.

One of the things we learn by perusal of our proceedings is that our tasks will never be done — they are always just beginning. The perfect DD-254 remains an ideal. Among the self-effacing responsible scientists who understand the perils we face, on whom we can count for support, instructions, and enlightenment, there will always be the slightly petulant genius whom we must learn to understand, like today's petulant younger generation. Our mastery of cybernetics can never keep pace with the movements we are trying to guide. The themes of our seminars can bear repetition for many a year.

We have been in business now long enough to experience growing pains. Mavericks have appeared on the scene. Members have sent in resignations. In spite of widespread rumors to the contrary it seems that classificationists are humans, too.

Dr. Welmers certainly started something at last year's seminar when he invented C/S Land — *Classification-Security Land* — as a paraphrase of Lewis Carroll's *Wonderland;* and the Roving Reporter from *Security World* was quick to seize the opportunity. But it's too easy. We are sitting ducks and he couldn't miss.

Alice's looking glass has reflected

foibles and follies for a century and yet we are tempted to say it was written for us, though similiar claims have been put forth by many others, ere now, I am sure.

Alice makes good reading too. Renewing my acquaintance with her, I have no trouble at all in finding passages to illustrate our kinship.

You remember the caterpillar's instruction to eat one side to grow tall and the other side to grow short.

"One side of *what?* The other side of *what?*" thought Alice . . . (Does that sound like the search for AEC/DoD interface?)

"It's really dreadful the way the creatures argue. It's enough to drive one crazy."

"Oh, there's no use in talking to him," said Alice desperately: "he's perfectly idiotic!"

"But I don't want to go among mad people," Alice remarked. "Oh, you can't help that," said the Cat; "we're all mad here. I'm mad. You're mad." "How do you know I'm mad?" said Alice. "You must be," said the Cat, "or you wouldn't have come here."

"Then you should say what you mean," the March Hare went on. "I do," Alice hastily replied: "at least — at least I mean what I say — that's the same thing, you know." "Not the same thing a bit!" said the Hatter. "Why, you might just as well say that 'I see what I eat' is the same thing as 'I eat what I see'!"

"She felt she had never been so much contradicted in her life before and she felt she was losing her temper."

But of course our favorite quotation is bound to be the famous remark of the Red Queen:

"A slow sort of country," she said. "Now *here,* you see, it takes all the running you can do to keep in the same place. If you want to get somewhere else you must run at least twice as fast as that."

Whenever we see common sense confronting a world where perfection of logic takes precedence over the validity of premises, *Alice* is our companion. Now I am not for a moment implying that that is our world, the world of classification. Yet when we can quote *Alice* like scripture it makes you stop and wonder just a little.

Sometimes in exasperation and frustration I have been tempted to refer to this world of classification as a never-never land, but not for long. We are always face to face with the seriousness of our business. This past year has roused, I think, as never before, the sense of crisis imminent and all-encompassing. The word "revolution" no longer seems adequate to describe what is happening. It is an exploding world. We face a population explosion, a pollution explosion, a technological explosion, an information explosion, a cybernetic explosion, to say nothing of the final, ultimate explosion of the world's nuclear arsenal. Unfortunately, amid this crescendo there are no sounds of an explosion of brotherly love.

Survival in the midst of explosion is today's challenge. How vulnerable

are we? Will the structure of our civilization shatter, spall, fragment, vaporize, or can we harden it? Can we devise the shields and safeguards for survival?

Among the shields and safeguards are those that we in classification management must devise and uphold. But today the devising of them demands far more knowledge, sophistication, experience, and wisdom than we needed even yesterday. The upholding of them demands more from each of us, and demands that there be more of us. Our numbers are too few and the professional qualifications become steadily more exacting. It is no exaggeration and no anticlimax to say the NCMS was founded none too soon.

Keynote Address

by the Honorable John E. Moss, Member of Congress

Mr. Chairman, let me first express pleasure for the opportunity of meeting with so many with whom I have had somewhat of an adversary relationship for the past thirteen years. It has been an interesting thirteen years.

Looking back, I recall when you could not get a bit of interest over the question of news management. There was no credibility gap. Really, there was very little public dialogue on the availability of information. I feel that if the subcommittee has achieved anything worthy of note, it is that it has created in the intervening years an increasing awareness of significance of information in our society.

You handle it. You know the nature of the content, the degree of sensitivity, the impact of that which is not available. You have a very serious responsibility each time you make a judgment, advocate a policy, or determine a classification, because at each point you have determined that a small portion of the totality of information is not going to be available finally to those that have the greatest need for it. I hope that it's always a balanced judgment.

In a society where each and every one of us is part of Government, it is essential that each and every one of us has an absolute maximum of information available in making the very important decisions we must make as our own governors.

Next year is election year. We are going to have injected into the campaign, inevitably, questions that touch upon the security of this nation: the adequacy of the performance of the Government of the United States in meeting the threats to the security of this nation, the progress that we have made in relationship to any combination of forces which might be committed in opposition to us. You all recall the so-called missile gap issue of the 1960 campaign. You also recall that that was a very close campaign in which a fraction of a percent changed or could have changed — materially perhaps — the character, the direction of the Government of the United States. And, that is true not only in the years when we have a presidential election but it is true each two years when my contract and the contract of my colleagues go up for renewal.

In each district we have to answer to an electorate or to a constituency that does not tolerate any plea or privilege or any classification over our actions as their representative. I mention this because I want to place in context the significance of information in our society. It is a vital ingredient, and yet, as you know far better than the average American, it is so sensitive in some aspects that it could also lead to a serious impairment of our strength if it were to be prematurely disclosed.

The committee has always recognized the delicate nature of the balance that must be maintained between a public need to know and a national need to protect information.

In an effort to define more precisely some of the basic guidelines for information disclosure — after twelve years of study and with the assistance of Senator Long of Missouri — we sponsored legislation which was signed into law on July 4 last year and is known as Section 552 of Title 5 of the U. S. Code. Now a lot of people thought that immediately upon the adoption of that bill a tremendous mass of information could or would suddenly become available. Well, of course, you know it did not. It will not. The areas of concern to the subcommittee about information have always been very limited. I have repeatedly told publishers' groups, editorial groups, journalism students, and other interested organizations and individuals that the instances of withholding or nonavailability of information are rarely dramatic, that if there is any drama in the work in which my committee has been engaged, it is the totality of impact not the individual instances.

But along with the need for protection of security material we have had an intermixing of another factor — and this is one that has caused me great concern. It is where an individual's security becomes commingled with the nation's or where material becomes nonavailable because it might prove controversial or embarrassing. Such situations do not involve the security of the United States and cannot be valid grounds for classification as they are not encompassed in any sense in Executive Order 10501 or in any of the statutory exemptions which are granted by law.

The statutory exemptions are continued, in the main, in the information legislation passed a year ago and now effective under guidelines issued by the Attorney General and which are implemented by rules and regulations adopted by the departments and agencies, rules and regulations which in the months ahead will be given very careful attention by my subcommittee. We have a very clear intent in drafting the Public Records law: an intent to maximize the flow of information; an intent to have clear and meaningful guidelines. And we are going to have them. We are going to have them if we have to call before the committee each department and agency whose rules and regulations tend to frustrate the intent of the Congress.

The report we wrote when we sent the legislation to the floor reflected a very careful, a very deliberate consideration. The guidelines issued by the Attorney General after almost a year of close cooperation and consultation with the staff of my subcommittee and the staff of Senator Long's committee in the Senate also reflect very deliberate consideration.

There was a commitment there to the public that the confusion of issues would be eliminated, and we are going to concentrate on that type of elimination. Bona fide security, of course, is not involved.

Those of you from industry know that excessive classification can impede progress as well as add to progress. You know that needless barriers slow down utilization of information. You know that the strength of this

nation is not derived from any policy negative in character. Frequently the most important developments occur by the accidental discussions, the cross-fertilization of ideas; a cross-fertilization which is minimized as classification is needlessly maximized.

Back in 1956, the subcommittee sat through eight weeks of hearings at which we had four Nobel laureates on a panel of very distinguished scientists representing most of the disciplines that have contributed so much to the strength of this nation. There was a clear consensus then, and nothing in the intervening years has tended to obscure that consensus, that there was far too much classification in industry and in Government, and in the industries that operate under contracts from the Government.

If we could have better guidelines we could have more progress. If we could have better guidelines we would have more efficiency and more effectiveness; we would secure more for our dollar with far iess duplication of effort.

Now I want to go to the law we passed. Actually it is two laws. One is the Public Records law, requiring countless numbers of Government agencies to explain how they operate, and to publish orders, opinions, policy statements, manuals and instructions, that are the end product of their operations. That is under Sections A and B.

The other is a Freedom of Information law — Section C — requiring public records to be made available upon request and permitting a court test of Government secrecy.

Section E applies to both the Public Records and the Freedom of Information parts of the law, spelling out those categories of Government records that are not necessarily public property.

Sections D and F are special sections, one requiring votes of multi-headed regulatory agencies to be put on the record and the other protecting the Congressional right of access to Executive branch information.

The Public Records section requires each Government agency — and that includes the boards and the bureaus and the divisions of all departments, to publish in the Federal Register a description of how it operates, and to publish an explanation of how it does business, and how the public can find out about the routine activities of such agencies, boards, commissions, bureaus or whatever they might be.

These requirements, we hope, will go a long way toward helping the public cut through a long existing paper jungle of confusion.

The Freedom of Information part of the law requires public records to be made available rather than merely requiring them to be published as provided in the first two sections. It is at this point that the law becomes particularly significant — both to those who seek out the records of Government and to those that are charged with the guardianship of those records.

In my opinion, the keystone of this section, perhaps the most important feature of the entire act, is the proviso that any person denied access to a public record, based on a top

level administrative decision, has the right to ask a Federal district court to rule on the propriety of the refusal, with the burden of proof for refusal resting solely upon the agency. If an agency official is unable to furnish proof and still refuses to give up the record, that official can be punished for contempt. Remember, there has never before been a right of court enforcement in this country of public access to the records of public business.

I suspect that the provision for judicial review will have a most salutary effect on those who, in the past, have exercised arbitrary or capricious denial of Government information for such outlandish reasons as "in the public interest" — this is a very unprecise definition—or for a "good cause found." You know I have never met a person who wanted to withhold information who couldn't find a "good cause" for the withholding.

The new law contains nine exemptions from disclosure:

The first relates to matters specifically required by Executive Order to be kept secret in the interest of national defense or foreign policy. I will come back to this first one a little later on.

Exemption number two applies to the operating manuals and handbooks used by Government employees in their inspection and audit duties. This exemption also applies to Government negotiations in purchasing transactions.

The third exemption covers all documents that are specifically protected by other statutes, and it might interest you to know that there are more than eighty other statutes.

The fourth exemption concerns trade secrets and commercial and financial information obtained from any person and privileged and confidential.

Exemption number five covers staff memos and letters to federal agencies. This exemption is based on the contention of the Executive branch that Government staff assistants will be completely frank in their opinions only if they are protected. An argument can be made on this point, but it is an improvement over the old law which permitted secrecy about all matters of internal management.

The sixth exemption protects Executive branch files that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy. Such details have previously been withheld under the "good cause found" provision of the old law.

Exemption seven restricts access to the investigatory files compiled for law enforcement purposes. So far, such files, those of the FBI and Secret Service, for example, have been protected in the public interest.

The eighth exemption protects financial or commercial information gathered by the Government from private institutions.

And finally, the ninth exemption protects information oil company geologists must file with Government by law.

It seems quite apparent the new law can help bring order out of the administrative chaos that Government classification procedures have become,

for it affects both the classification of documents withheld to protect the national security and the classification of routine records which fill Government filing cabinets.

Of the nine categories of exemptions I have just listed, one category gives statutory authority for the first time to the system of protecting security material.

Exemption number one, which I indicated I would return to, grants the President statutory power to protect secrets in the interest of national defense or foreign policy.

It may surprise many to learn that until now there has been no specific statutory authority for Executive Order 10501 and for all the classification procedures it sets up. Both this order issued by President Eisenhower and an earlier order on the same subject issued by President Truman rely only on the President's broad constitutional powers.

I do not know whether an act of Congress, granting statutory authority for the security classification system, will make possible more orderly management of the system. I do know that the new law will require the top officials of every agency to take a careful look at the classification system. There have been attempts in the past to cut down on the huge volume of classified material generated in hundreds of Government and private contractor offices. And there have been attempts to improve the methods for handling classified material. But these attempts have not been notable for their success.

There have been other attempts to extend security controls to documents that fail to qualify for classification under the security system. Sometimes these attempts have been successful, at least for a short while. My subcommittee was responsible for the failure of one such attempt when the Department of Commerce set up the Office of Strategic Information a few years ago. When we proved in public hearings that the Office of Strategic Information was trying to force scientists and contractors to place classification on routine information which might have some future value to some potential enemy, Congress cut off the appropriation and the Office of Strategic Information was abolished.

I hope a like fate will befall similar attempts. It will not be necessary to await congressional action, for the new Freedom of Information law will force top level attention on classification problems before they get too big to solve.

There is hope that such top level attention also will be given to the problems of managing the tons of routine Government documents restricted under a lower grade system than that provided in Executive Order 10501. A current survey of Government agencies by the subcommittee shows that fourteen different terms are used to accomplish the same job —identify routine material which does not qualify for restrictions under Executive Order 10501 but which the agencies want to keep to themselves.

I suppose that things could be worse. There could be even more confusion. And there was, four years

ago, when my subcommittee first looked into the problem. Then, we found the Government agencies and departments using thirty-seven different terms to designate non-security material they wanted to restrict.

The most popular term today is "official use only," with "limited official use" running a close second. The other terms range from the mouth-filling "for department use only — not for release," which is used by the Interior Department, to "eyes only," which is used by the Peace Corps to send personnel records to staff members.

This proliferation of security stamps is not only confusing but is nonessential. Nonsecurity records should either be open to the public or they should be restricted to use within the Government. And there should be one common term to identify those administrative documents that must be restricted.

Under the new Freedom of Information law, such uniformity is possible. In fact, it is anticipated that it may even be necessary. Government records will either be publicly available or they will be exempt from disclosure under one of the nine clear categories; and a single term, "exempt" or some similar label, should be used to designate such documents.

There are many problems with the management of information classified as "top secret," "secret," or "confidential" under Executive Order 10501. Parenthetically, a subcommittee survey shows that in 1966 approximately 30,000 Government employees were authorized to classify security information under the Executive Order, at an estimated administrative cost of $1,900,000. But those problems are small compared to management of routine documents identified by fourteen diverse terms. The new law—with the intelligent help of classification experts—points the way to a solution of many of these problems.

There have been references to the apparent favorable attitude of the Executive Branch officials toward implementing the basic intent of the act. This attitude is reflected in the tone of Attorney General Ramsey Clark's foreword to the Department of Justice guidelines, which departments and agencies hopefully followed in setting up their regulations to implement the law. He said, in part, and I quote:

"If Government is to be truly of, by and for the people, the people must know in detail the activities of the Government. Nothing so diminishes democracy as secrecy. Self-government, the maximum participation of the citizenry in affairs of state, is meaningful only with an informed public. How can we govern ourselves if we know not how we govern? Never was it more important than in our times of mass society, when Government affects each individual in so many ways, that the right of the people to know the actions of their Government be secure."

Gentlemen and ladies, I could talk for a long time about the problems encountered over a span of thirteen years as Chairman of the Information Subcommittee of the

House of Representatives. All of it might not be interesting, but before I open the program for questions, I want to assure you that it is interesting to me. You would think after thirteen years with one subject that it would become very boring; but each day I can be almost certain to encounter some new and novel approach to information withholding that will keep my staff occupied. I am ever amazed at the initiative, the unbelievable initiative, at the resiliency in some agencies and departments, the bounce-back they have on creating information problems. The only thing I can say is that in thirteen years we have moved from the old pattern of extended public hearings as the means to solving the controversies to the point where today most of them are solved by a telephone call at the staff level. And now, may I have your questions?

LESLIE AYRES: I would like to lead off with one leading question. Having read the bill and having looked at the implementation, I find that we are still addressing the flow of information in the Executive branch of the Government. I would like to ask, Mr. Moss, what does your bill do to the Legislative and Juidicial branches of Government and the public-at-large who are also citizens of the country?

MOSS: Not a single thing, and let me tell you why. It is not because I don't think that the Legislative or the Judicial branches couldn't stand the same careful scrutiny that I have been privileged to subject the Executive to. It is a simple matter that my committee does not have the jurisdiction over the Legislative or the Judicial branches of the Government. There are at least two committees in the House that do have jurisdiction over the Legislative branch — the Committee on House Administration, and the Committee on Rules. And there is one committee that has jurisdiction over the Judicial branch — the Committee on Judiciary. Had my committee the jurisdiction, we would have included the two branches in a comprehensive study.

I would like to point out one very interesting difference between the Legislative and the Executive branches. If you will read the Constitution with great care you will find that "secrecy" or "secret" is mentioned in it just once: when it says that the Congress shall keep a journal of its proceedings and from time to time shall publish the same excepting those portions which in its judgment are required to be kept secret. That is the only constitutional sanction for secrecy. But it does not excuse the proliferation of Executive sessions which daily occur on the Hill and which conceal from the public the important actions of their representatives. I hope that before many more sessions have passed we will tackle, through the Reorganization Act, the problem of too many secret meetings on the Hill.

Do we have any more questions?

LORRY McCONNELL: I have heard some people comment, although I am a representative from industry, but I heard some Government people comment to the effect

that there is much concern about practicalities of making information available. There has been somewhat of an information explosion, and I wonder if you would care to comment on this? Is it the intent of the law, for example, to encourage agencies to make provisions for making information more available through additional funding and things of this type?

MOSS: No. The only thing that the Committee has been concerned with—and I have repeatedly over the years in my public appearances attempted to emphasize and underscore this—we have been concerned with the removal of barriers to access on the part of those who have an interest in information. I don't think the Government has responsibility to start just an affirmative program of putting out masses of information. In the first place, it would be overwhelming. I think if we really wanted to create absolute confusion all we would have to do is to start putting out everything in Government and we would have it. But to those who seek it, there should be an orderly method for obtaining it and unnecessary barriers should not exist.

Now, part of the pattern of evolving this orderly procedure is going to develop through the case law as the courts start reviewing the instances of refusal. And while we grant specific categories of exemption the decision as to whether or not they are properly categorized is reviewable by the courts. So that in addition to the legislative history and the Attorney General's guidelines and the rules and regulations of the departments and agencies and the bureaus and the commissions, we are going to have some case law.

Throughout the long months of negotiation — there is a lot of give and take represented in this bill in its final form — the one provision I insisted remain unchanged was that of judicial review, because I think it the most important and that ultimately it will prove the most constructive provision in determining what should and should not be made available to the American people.

JAMES LANGFORD: Mr. Moss, there seems to be some divergence of opinion as to whether technical data, unclassified, relating to weapons systems and space systems is clearly excluded from public disclosure under the law. I wonder if you could comment on that?

MOSS: In my opinion it would be contemplated in the law that unclassified technical data would be made available. Now, we have had the first draft of the DoD's guidelines sent to us about three months ago. They were totally unsatisfactory and were rejected by the Committee. I have not seen the final regulations, but they will be reviewed with great care. I don't know whether it will be necessary finally to have hearings on them or whether they will conform with the guidelines issued by the Attorney General. This may be one of those instances where a little case law will have to develop before we have the final answer. The intent would be that if data are not classified they should be made available under

orderly procedure governed by the rules and regulations.

FRED BOONE: I believe the law exempts from disclosure trade secrets obtained from another person. Is it possible that we might develop within Government plants and laboratories certain procedures and techniques which would be in the nature of trade secrets, developed and owned by the Government? Is it conceivable, under the law, that this type of information could be restricted to our own industry, let's say, and not disclosed to our foreign competitors? In other words, trade secrets developed and owned by the Government, would they be affected?

MOSS: The trade secrets owned by the Government? If they were classified, they would be exempt. If they were not classified, they would not be exempted. In other words, the Government's technology is usually available throughout industry, unless the Government determines for reasons of security that it should not be.

BOONE: No, I have in mind techniques that we should watch, that relate directly to national security and defense but could not be classified on the basis of national defense but rather in a category of a technique we would like to restrict for our own interests, and, therefore, we would like to get a limited distribution. By what means might we do that?

MOSS: Well, why would you want to give it limited distribution? Distribution at all would usually expose it sufficiently so that the reasonably alert intelligence on the part of any other Government could gain access to the information. If it is essential to the security or the well being of the national interest of this nation that it be very limited then I think that the regulations of NASA should attempt to justify a category that restricted it. And, again, we might get into the area of a court test. I don't know who would have standing in that instance to go into court. I think that we have here a hypothetical question. Without something more substantive and illustrative of it, it would be very difficult to answer.

EUGENE SUTO: Mr. Moss, I have a question about basic research that is conducted by scientists from purely unclassified sources, and a scientist comes up with a breakthrough in a particular area. This is work being done for the Defense Department and the classification is then placed on the material. Usually the scientists' views are that the information should be disseminated to all scientists. May I have your views on this, please?

MOSS: I agree with the scientists one hundred percent. This is one of the things I mentioned about the 1956 hearings. When you get into basic science, science is very, very nonpartisan. It has no national loyalties. The secrets of nature are open to the universe and any nation with a scientific community is going to be adding to the bank of basic knowledge. I think that we as a nation have been frequently far more the over-drafter on the bank of basic scientific knowledge than we have

been contributors to it, the pure research.

SUTO: Even though this would involve national security?

MOSS: If it is clearly national security — now, you are talking about a breakthrough that is clearly identified. Then I am told that — and let me say that it was the consensus of the very distinguished panel that we had — that you might successfully classify that for about two years, but to hope to protect it longer is vain. And here again I think realism should be applied. We also should weigh against the classification the advantages that might be gained by a wider dissemination. I recall the president of Bell Laboratories discussing in that series of hearings the case of the transistor, expressing his conviction that had it been classified, as had been strongly urged, the progress made in many areas of electronics would have been far less. Because of its availability, it was utilized in manners undreamed of when it was first developed. And where would we have gained greater security—through the classification, the limited availability, the limited opportunity to adapt it to new and broader uses, or through the protection of it at the moment? This is a difficult question. Sometimes the judgment is not made by the informed scientist, but is made by someone who has little more understanding, perhaps, of the scientific significance of it than I myself would have. And this is unfortunate when it occurs because it tends to departmentalize knowledge, and to prevent a cross-fertilization which is so very much a part of the pattern of scientific progress.

ROBERT BECKNER: In the past, there have been a number of security violations in periodicals. Is there any provision for the downgrading of the material that has been released through periodicals?

MOSS: There is no provision for the downgrading, except rule of reason. I think there should always be a rule of reason in classification and in the imposition and maintenance of the classification system. You can classify and protect information to a certain point, and when it is evident that it can no longer be protected, classification should be removed. One of the great failures of classification is that we fail to remove the classification labels when it is obvious that the material can no longer be protected. I could cite many, many instances that have come to the attention of the committee over the years where security labels remain on information widely known to the public, not only the American public but the public around the world, in the most sophisticated nations.

M. D. AITKEN: Should this group or should the Executive branch of the Government in general, be apprehensive about any review by your subcommittee at the three levels of classification as specified in Executive Order 10501?

MOSS: I would hope that they would have no reason to be apprehensive. I can assure you that my interest in protecting the security of this nation is as great as anyone else's, although I must confess that I have

been charged on occasion with trying to make all information available. They would only have reason to be apprehensive if they are abusing the proper use of it. I might add that I am firmly convinced that abuse, the excesses which are practiced, weaken rather than strengthen the effectiveness of classification. When you routinely see documents with a high classification stamped on them and they are really trivia, that doesn't strengthen your respect for the system. So I think a little more narrowing would be very helpful.

JAMES LANGFORD: A question regarding the definition of the general public or public: With due respect, if it is determined that the technology is not exempted from this bill, where we must release it to foreign nationals, or more particularly Sino-Soviet bloc representatives, would this not violate the intent of the Munitions Control Act? Even though Government agencies are not subject to the letter of the act, it would seem they would be subject to its intent.

MOSS: Well, now, I would have to, I think, give you a written response after a little careful reflection on that. The law says, "Any person may go into a Federal District Court . . ." You are talking of information you say is protected under the Munitions Control Act. We recognize a number of categories of information are protected by statute, and if it is clearly in the area of information protected by statute, then the statute would apply; the protective statute would apply. Remember, one of the categories of the nine exemptions that I mentioned, was where the information is clearly protected by law. I pointed out that there are more than eighty statutory exemptions on the books. If you could give me a specific example and get it to the subcommittee, I would be very happy to prepare a written opinion for you.

ROBERT CALVERT: A procedural question. Anyone can request information. Is it a sufficient answer to tell these people this information is available, or is it incumbent upon us to give an answer to them directly?

MOSS: The statute provides, and it gave a grace period of a year for the departments and agencies to, in effect, make an index of information and to determine orderly procedures for public access to the information. If it is information that is normally within your jurisdiction then I think you have the obligation to make it available.

WOODBRIDGE: We thank you very much for this brilliant and forceful illumination of what you might call "the other side of the classification coin." It is a matter of great concern and interest to our Society.

MOSS: Mr. Woodbridge, I want to thank you and each of you. You have been most patient with me.

LUNCHEON ADDRESS

by

Joseph J. Liebling, Director for Security Policy, OASD(Administration)

Department of Defense

Now that my "hundred days" in this new job are on record, I guess I ought to be ready to deliver a bundle of break-through suggestions on how we can solve the security review and classification management questions to everybody's satisfaction for all time. But frankly, the more I dig into the information problem from the OSD vantage point, the more I begin to understand what Voltaire once said about contemporary historians: "The man brave enough to try it will be criticized for what he puts out; then condemned for suppressing that which he failed to mention."

In a very real way, all of us here who share a common interest in the objectives of the Society are custodians of contemporary history. In that capacity, we are caught in the middle. Our duty as regulators or monitors is to safeguard material that does or could affect the national security. At the same time to be all inclusive, there is our equal devotion to the truth and to the facts we make available to cover all sides of controversial public issues. The root tenets of this democracy are watered only by the free flow of information to the American people who collectively and through their chosen representatives give essential meaning to our endeavors.

You and I—all of us in this room—bear a heavy responsibility. In large measure through our efforts, the United States must continue its way to reconcile the need to maintain free access to information with the requirements of the national security on a practical basis. Some years ago, I recall that a Washington newspaper editor told a Senate subcommittee flat out that "secrecy is alien to freedom and incompatible with freedom." "Secrecy's price," he concluded, "is too high" to risk our free institutions. Perhaps this is so, but if opening the Government's state and military files *in toto* is the price we must pay, then the American people ought to be told that in all candor, and they might just as well get used to it.

There are a few axioms concerning security. One is: Where security is found to be excessive, it can always be cured by relaxing it. There is no cure, however, for inadequate security. Information once compromised cannot be recovered. It is obvious, however, that the swinging of a pendulum indiscriminately between indifference and hysteria in either direction is not the answer.

The issue goes beyond that drawn by impatient editors or a few heavy-handed officials who assume a proprietary interest in information that has been entrusted to them only by virtue of their jobs in Government or defense industry.

One issue the angry editor refused to acknowledge has been rightly referred to as "intelligence on a silver platter." Despite the most vigilant efforts by the FBI and our military counter-intelligence, they are simply helpless to cope with a perfectly legal transaction that takes place daily on any corner newsstand.

Through careful screening of our news media and periodicals, the Soviet Union and Red China have been able to acquire a great deal of valuable data, anything from the specifications and performance characteristics of military weapons systems to the highest level of Government planning in some instances—simply by reading about them in technological documents obtained through Government agencies commercial sales. It is no secret that the Soviets made tremendous strides in the field of electronics after World War II through direct purchases from the United States Government. On the other hand, this same information provided the U.S. scientific and technical communities with the greatest base for technological advancement any government has ever experienced. Even today it is referred to as the "technological gap" between U.S. superiority and European capability.

I would not wish my remarks at all to be interpreted as a general critique upon the American press. This is our way of life! In fact, I would go so far as to subscribe to the views expressed in a recent speech by Dr. Edward M. Glick, Director of the American Institute of Political Communication. He said: "Today's press is a far more decent and honorable institution than its predecessors of one hundred or even fifty years ago. The media generally—and the larger newspapers and television stations in particular—are doing a much more effective job of disseminating and interpreting the news than was the case at the turn of the century."

Dr. Glick also said that "The Federal Government has substantially increased both the scope and quality of its informational output in the past generation." As one who has been associated with that undertaking for the past twenty-five years, I must endorse these sentiments.

This brings me to talk a little about this job as Director for Security Policy. I acknowledge the functions of the Directorate for Security Policy as a balance wheel that encounters the varied and sometimes conflicting pressures of our national policy and converts them to a measured flow of sound, common sense determinations.

The responsibility we have and which many of you share has been referred to as a thankless job in the defense structure. I don't agree with that reference because each passing day brings with it new interests on the part of the Congress, the press, the public and by Government officials toward a better exchange of ideas on the subject, as will be experienced here in the next few days.

It has been said that there is another long-range debit in the security ledger: that unnecessary classification fences built around knowledge slow technical progress, add administrative

burdens, and run up costs for the whole program. This point of view has been a most controversial one and on occasion has received some support from the technical and scientific communities. The stature of U. S. technological superiority world-wide is an unequivocal fact. Surely security has not hampered such progress, in spite of lamentation to the contrary.

In dealing with excessive cost factors, due to security classification, I would like to document some examples involving the Air Force, where I formerly participated. We had the requisite authority and knowledge of available national security policies and by exercising common sense judgment born of experience we saved about $2,000,000 in the downgrading of technical orders on the Thor missile we were sending to Britain. In another case, a field trip was taken, which cost Uncle Sam about $20 to $30 plus travel, where a declassification of J-85 jet engine parts was undertaken. That alone saved $100,000 just in security costs. An estimated $635,000 was saved in phase-down of overseas supply bases which by themselves would have meant nothing to an enemy agent anyway. These actions were accomplished in a single Air Staff classification management office.

I'm sure there are many other examples of security officers using good judgment and common sense that many of you can recall from your own experience.

In a more general sense, consider the case of a classified item developed with the aid of Government funds and produced by American industry. The manufacturer is now interested in exporting these items to certain friendly foreign countries. Furthermore, the Commerce and Treasury departments are anxious to promote exports. To improve these foreign purchases would not only help our balance of trade, but the increased production would be expected to reduce the cost of future purchases by the Department of Defense.

Here again the Department of Defense security review and classification management responsibility comes into play. Among the more important factors to be taken into consideration in providing a position to the Department of State, which administers the munitions export program under the International Traffic in Arms Regulation, are (1) security aspects, security policy interests and/or implications, including current security classification, if any, of the item involved, and (2) significance of the specific item proposed for export in relation to the latest state of the art or advanced technology in that particular category of item. It is also necessary to relate the proposed export to technological developments or programs in the country of destination. Maximum use of available technical intelligence is all important to security and classification managers in addition to project and engineering people.

In one way, it has been said that the veritable tide of information we must release, in contrast to the trickle that comes out of the communist countries, is a blessing in dis-

guise. A major complication for Moscow and Peking is that they must worry that the volume of unevaluated data they find in print must be authenticated. Don't get the wrong impression—they're not *too* embarrassed. I'm sure our intelligence gathering agencies would be glad to exchange acquisition headaches with them. There is nc immediate prospect that the considerable "handicap" we now afford foreign intelligence agencies through our liberal disclosure policy will be narrowed in the future. It is a price we willingly pay to retain the democratic rights we have and which they must envy.

All possible resources are being exploited to provide us with better designs to produce sound national security policies. Views of leading industrial representatives and of news media are being marshaled. The divergence of views is quite challenging. Again, permit me to use a concrete example. In attempting to institute what we thought was a constructive program last year for better classification management, a requirement was set up for paragraph marking both in Government and in industry. As recent as this past April many of the national corporations which were members of a national trade association reflecting their views at a regional meeting reacted in an almost unanimous voice in the negative—"Too costly. It takes too much time for engineers to figure out the classification since they have no experience in fixing classification or evaluating information. Government security classification managers and analysts are not available for consultation, etc." This was the case presented both orally and subsequently documented with detailed facts and figures prepared primarily by industrial security people and company technical personnel for submission to my office. Rather than mandating the enforcement of this program within industry as required by previous directive with a July 1, 1967, deadline, we are deferring mandatory application until January of 1968, to give us more time to study the overall subject.

When viewing the program in the overall national interest and after discussing the matter with many of the top level executives of the major corporations, it seems to me that greater benefit can be accrued to both the Government and the American industry in many vital areas. Effective security classification management, which incidentally is the key factor bringing about the requirement for safeguarding of information in the hands of industry, including paragraph marking, in addition to the cost saving factor, will (1) facilitate international export and trade by American industry, (2) provide us a greater flow of information to news media and the public regarding current defense posture, (3) increase our industrial base because of greater availability of such information to small business, (4) permit a wider exchange of know-how among the scientific and technical communities including colleges and universities, domestic and international, and (5) provide for a fall-out state-of-art and

technology available for commercial purposes.

This is what an effectively managed classsification and declassification program holds for us collectively.

Freedom of information is a pillar of our society, while the requirements of national security are at a paramount premium. The line between these two concepts is a changing one. We in Government and you in industry in concert must be flexible enough to accommodate each objective. Each of us in the Department of Defense regards this as a priority responsibility in the implementation of DoD Directive 5400.7 issued just three weeks ago on the "Availability to the Public of DoD Information" consistent with the Public Information Act of 1966. In the words of Secretary McNamara, spoken on June 30, the Department "has an obligation to guarantee that full and prompt information is made available to the American people as a basis for their understanding of the national defense and the operations of the department."

PANEL–EXECUTIVE ORDERS AND LAWS AFFECTING CLASSIFICATION IN THE GOVERNMENT

Clifford J. Nelson, Department of Justice, Moderator

I am here as moderator because Mr. Rubenstein asked if I would take this job, and apparently it is related to the fact that I have been the chairman, as shown in the biographical data you have, of the Subcommittee on the Protection of Classified Government Data.

I might give you a little background on that. This is a subcommittee to a committee that is commonly referred to as the ICIS, which is the Inter-Departmental Committee on Internal Security. This is a committee that was set up by the National Security Council in 1948 and assigned all responsibilities in the internal security field except those relating to intelligence, investigations and so forth, that are assigned to another committee set up by the National Security Council called the Inter-Departmental Intelligence Conference. Now the ICIS has about five subcommittees of which one is this subcommittee four of which I am the chairman, the Subcommittee on Protection of Classified Government Data.

If you look at Executive Order 10501, Section 17 contains a provision that says: ". . . that the National Security Council shall conduct a continuing review of the implementation of the order to make sure that classified information is properly safeguarded . . ."

This responsibility the National Security Council assigned to its ICIS Committee and in turn was passed on to the subcommittee four, of which I am chairman.

I might tell you a little how the

subcommittee carries out its responsibilities. It is made up of representatives from the Department of Defense, Department of State, the Atomic Energy Commission, the Department of Commerce, and the Justice Department.

We don't have any staff or anything like that. The ICIS has a secretariat to perform certain services for us. But through the years we draw up a questionnaire on the Executive Order and send it out to all of the departments and agencies and get their responses back and review them and see any shortcomings. Over the years we have found certain shortcomings. Most are corrected by a letter from the ICIS to the agency. Some have resulted in amendments to the Executive Order.

It was felt that since Executive Order 10501 had been in effect about since 1953, it was time to make a comprehensive review of it. So the ICIS sent out letters to all of the principal departments and agencies asking for any views, suggestions for changes, and so forth, of the order, in light of the experience in all those years. We have gotten back most of the replies and we have several suggestions for amending the order.

I might say this about amending the order. We have always taken the position in the subcommittee that every time you amend Executive Order 10501 it's like throwing a rock in the lake—it sets off a lot of ripples. Everybody starts rewriting regulations. It all takes time and costs a lot of money. So unless the proposed amendment or suggestion really resulted in some significant saving or substantially enhanced security, or really made some worthwhile advancement, we have been loath to make amendments.

I might indicate to you some of the suggestions for amendment of the order that we now have under consideration.

For example, there is the ever-recurring suggestion that definitions for top secret, secret, and confidential be revised—be made more precise. We will consider this again.

Another suggestion: as you know, the word "defense" appears in the order many times, and the words "information" and "material." Sometimes they are used interchangeably, sometimes in opposition to each other. It's been suggested that the order be cleaned up to use these words a little more precisely.

Another suggestion: that some other term be adopted instead of "confidential" because this is a word that has so much public usage.

Another suggestion—and I think this has been given impetus by the Freedom of Information Act that Mr. Moss talked about this morning—and that is that there be another classification system to cover nondefense information. I think Mr. Moss touched on that a bit this morning.

Another problem—and it has come up before and it appears to be more and more of a problem because several agencies have raised it—has to do with classifying automated material—all these tapes and things from computers. I know so little about it I can hardly explain what the problem

is. But as far as the subcommittee is concerned, we will probably have to get some people in. We are now so uninformed in this field we will have to get some real computer people in to see if there is a problem, and if there is how to solve it. This is one of the things that we will be going into.

Another suggestion, and this was touched on by Mr. Liebling, is that in documents there be more identification of the particular information that is classified.

Another suggestion that has come from agencies having overseas installations, mostly defense and intelligence agencies, is that the requirements for the storage of classified material overseas be raised—that the confidential material be treated just about like the top secret material.

These are examples of some of the suggestions that we have and they are under consideration. From any agency particularly affected, we will bring in representatives so that the Committee can get their views.

We are obstensibly the experts in this field so we are not bound by any department position. We recommend and adopt what we think is best. Then our recommendation goes up to ICIS itself. And then it's staffed in the agencies and the agencies all take a position on it. Once that is done, and it is adopted or passed on to the Attorney General, it starts going through the course of the Bureau of the Budget for further staffing, and ultimate adoption, if it gets that far. Basically that's the function the ICIS performs in this classification field.

This Freedom of Information Act that Mr. Moss talked about—that one exemption, E-1, about matters specifically required by Executive Order to be withheld in the interest of National Defense or foreign policy—this also raises some questions about the order that cut pretty widely across the board. While considered in our committee, such matters are also considered in the Office of Legal Counsel Department. On that subject we have—on the Freedom of Information Act—Mr. Anthony Mondello.

ANTHONY L. MONDELLO
Office of Legal Counsel
Department of Justice

Thank you, Mr. Nelson. Fellow panelists, ladies and gentlemen: First, I am flattered beyond words to have been invited to address a group of experts about a topic that I am not at all expert in, the topic of classification. I am a little better informed about this Public Information Act and I have been asked to talk about that. I am not too sure that the act has very much to do with classification, however, but you can decide that on the basis of what we get out in this period today.

I think the most important thing I could say about the act itself is that it either establishes or it recognizes a new mood in the handling of information in Government. It takes a startling new approach to what must be made available. It represents, I think, a basic change in the philosophy of the Government's handling of information.

Under the law as it existed before July 4, the burden was always on the person who requested the document from the Government official to show a number of things. One was that he was properly and directly concerned, for example, under Section Three of the Administrative Procedure Act, and he had to justify why he should be given the document he sought. And even if he was properly and directly concerned with it, it could be withheld from him on the basis that good cause required its confidentiality even from him or that secrecy was required in the public interest. The act, the passage of it, its ultimate enactment, represents great dissatisfaction, certainly in Congress and even elsewhere—notably among the press—about these vague standards like "public interest," "confidential for good cause found," and even the test of being properly and directly concerned, although that's a much more specific affair. There is another thing about the previous law that existed with respect to information. If you didn't like what a Government official did to you, and he denied giving you a document, there wasn't very much you could do about it. If you happened to be a litigant in litigation and you knew that there were documents available in Government files that might help you in your litigation, you could try to get them and you might get a judge to order them to be subpoenaed. But these were relatively rare cases. We have handled just a fair number of them in the Department of Justice, and it didn't answer the question of getting out of the Government files a lot of information many members, either of the public or of the press, were interested in. Now, the changes that have been brought by the Public Information Act are basically three of these rather large scale, overall changes.

First, any person has standing to seek a document regardless of his concern. He can be a curiosity seeker; he could be a crackpot; he can be a self-designated Attorney General who is inquiring into the affair of whether Government is being properly handled. He can be literally anybody. He can be an alien. He can be a Chinese communist who goes to the Defense Department and says, "I want these three tons of documents." There is nothing in the statute that will permit you to ignore a request merely because you didn't like the nationality or alienage of the person who made the request.

The second major change is that the burden is now on the Government, not on the requester, to justify the withholding of a document, and that burden the Government can usually support only by showing that the document that's requested fits within one of the nine exemptions of the act.

And the third matter of importance is the fact that now a person who is denied a document can run off to the district court, where he can challenge the denial and where the burden of proof is on the Government to justify the withholding.

I think these are major changes indeed!

The provision for judicial review

put teeth in the act, which we will shortly find out all about. There have been already some cases brought. Of course there are as yet no decisions.

The Office of Legal Counsel that I work in is a very small office in the Department of Justice. It spends most of its time grinding out opinions, giving legal advice to the White House, and to the heads of departments and agencies. And you might wonder how come we get involved with this Public Information Act.

We were very reluctant about it, but once the law was enacted we found we were getting a great many phone calls from general counsels all over the Government who wanted to know what the act meant, what particular provisions of it meant. We soon learned that a general counsel here would put one interpretation on language, and some other general counsel had a different area to protect and would put quite a different interpretation on the identical language. The language itself, we found, wasn't so clear that you could answer questions—answer all questions—straight from the text of the act. We found some of the language to be ambiguous, and we found we had to go to the legislative history of the act in order to discover what some of the language was designed to mean. After a while it became obvious that something was going to have to be done if there was to be a uniform construction of the act throughout the entire Federal establishment. And so we reluctantly agreed that rather than have to write a series of what are very difficult to write, formal legal opinions of the Attorney General, it would be well to prepare a pamphlet that indicated what we thought the act meant both in the overall and as to its specific language. And so we agreed to prepare what is now published. If you hadn't heard about it, it's called "The Attorney General's Memorandum on the Public Information Section of the Administrative Procedure Act." It runs only about fifty pages. It's available at the Government Printing Office for a quarter. It contains an appendix which has in it two versions of the law that was enacted, and I would like to explain why that's necessary:

Back on July 4, 1966, Public Law 89-487 was enacted. But that enactment fitted into the Administrative Procedure Act. During the course of 1966, the Administrative Procedure Act, along with the rest of Title Five of the United States Code, was codified and reenacted as positive law. But they did not insert P.L. 89-487 into this new codification because it did not become effective until a year later, July 4, 1967. In the process of its codification, there were well over a hundred changes made in the language and in the format of this section which deals with Public Information. So the Attorney General's Memorandum on which we worked for more months than I would like to remember deals with Public Law 89-487 because right up to the last minute we didn't know what the text of the codification would be like; and the pressure of time made it impossible to get it rewritten around

the new codified text and still out to the printer on time to get it to the agencies on time, so that the regulations that each agency had to publish would have whatever benefit there is in having this to refer to.

This is not too harmful a matter because in the course of codifying this Public Information Act the codifiers have indicated—both House and Senate committees have—that all of these many changes—essentially changes of style and changes in order to permit the codified version to fit well within the rubric of the entire codification of Title Five—specifically, the changes were made without substantive change, and both committee reports say so.

So for briefing purposes, Government lawyers, if they use this memorandum at all to indicate an interpretation of the act they wish to be followed, are going to have to show how the interpretation fits the old language and the pre-codification enactment and then indicate that without any change, there have been changes in language. It makes a relatively difficult two-step approach but it should not be serious.

In this memorandum, what we tried to do is weave togther the text of the act with all of its legislative history, and to the extent that we have done our job well there will be a relatively uniform response of the entire Executive branch toward the provision for making information available.

Now, I would like to get to a few specifics about the statute itself. I understand, although I was not present this morning when Congressman Moss talked about this, that he apparently regarded the so-called Freedom of Information aspect of the act, the availability to the public of Government information, as essentially stemming from the public's right now to request a document from a Government official. And for this purpose he apparently ignored the two earlier major provisions of the statute, the first of which has to do with the publication in the Federal Register of a good deal about Government agencies, which is designed to permit members of the public to deal with the agencies. This section is relatively unchanged over what it used to be in Section Three of the Administrative Procedure Act. It includes, for example, things like publication of matters having to do with an agency, agency-organization, the places of business, the offices and methods that the public must use to deal with the agency, the general course and methods of agency functions and procedures that are available to the public, rules of procedure, the availability of forms, special instructions to the public, and general rules and policies adopted by the agencies. So the public can be guided in how it deals with agencies.

The second major subsection of the act is one that has to do with making certain kinds of documents available to the public for inspection and copying. We concocted the idea, in this memorandum, of having each agency maintain a reading room or some similar facility where documents of the sort required by the statute

will be available to the public, so that they can just come in and pick this material off the shelves if need be.

Now the material itself: final opinions and orders made in the adjudication of cases and with much of that, those of you who are defense-oriented will have almost nothing to do; statements of policy and interpretations adopted by the agency that are not published in the Federal Register; administrative staff manuals and instructions that affect the public, unless the matters are published and offered for sale, and unless they are maintained in current index of such matters.

Now, those two main provisions of the act: publication in the Federal Register, and availability in a public reading room.

Each, gentlemen, carry their own sanctions. If there is something that you should publish in a Federal Register because the act requires it, and you do not publish it in the Federal Register, the act very specifically states that you "cannot adversely affect any person by such a matter which is required to be published and is not published." But, of course, if you don't handle the adjudication of cases, here that is not going to bear very hard against you.

The sanction for failing to keep a reading room, or otherwise make available to the public, final opinions, orders, or staff instructions, is that you may not rely upon them, use them, or cite them as precedent against a party, unless you have indexed them and made them available or unless you gave the party actual notice.

There, again, most of the heft of that sanction runs against the kind of agency that adjudicates cases and has parties who appear before it, against whom they might want to cite something as precedent. Whether that fits your functions, you will have to decide.

The statute has a provision—the major one that Congressman Moss did talk about—concerning requests for identifiable records, which request can be made by any person, and denials of which are subject to judicial review.

It then has a few other provisions not too important to us here. One of them is the requirement that the record of the final votes of each member of a multi-headed agency shall be made available for public inspection.

Then there is the subsection that sets forth nine exemptions. The most important thing about these exemptions—that is, the two most important things—are that the nine exemptions apply across the board on every requirement of this section of the Public Information Act, so that if something is exempt by one of these exemptions it need not be published in the Federal Register, it need not be made available in a public reading room or a similar facility, and it need not be given to anybody who requests it; the second thing is that the authorization to withhold documents that's created by these nine exemptions is permissive—not mandatory.

I think you will find, if you read

casually through some of the agency regulations that appeared in such a body on July 3 and 4, the last two days of the deadline, that most of them indicate what is exempted from the act by using these exemptions. Some of them proliferate a little and indicate particular kinds of records of that agency that do fit particular exemptions, although that's not uniformly the case. But having said that matters of that kind that the statute provides for can be exempted, they have also indicated that they will consider a request for materials that fit the exemption, and decide whether some overriding public interest will permit them to be disclosed.

Now in talking about the general approach of the act the Attorney General included just a few statements in a foreword, some of which I would just like to read to you. They are relatively very brief. He says:

> "This law was initiated by Congress and signed by the President with several key concerns: that disclosure be the general rule not the exception; that all individuals have equal rights of access; that the burden be on the Government to justify the withholding of a document not on the person who requests it; that individuals improperly denied access to documents have a right to seek injunctive relief in the courts; and that there be a change in Government policy and attitude."

Now, we have tried, in the course of getting this memo out, to satisfy that requirement of the Attorney General. It used to be that you could balance the need of an individual against the need of the Government with respect to a particular document. If you were fortunate, you would get into a lower court to do that.

Now what you do is you balance the need of the Government, but in different terms, against the general need of the public, which is spoken of in this statute. The terms are rather more broad and they are embraced in all of these exemptions. What I would like to do is go through the nine exemptions very briefly.

The first is the one that Mr. Nelson mentioned to you. It is now introduced with this language: "This section does not apply to matters that are . . ." and then it lists nine different categories of matters. When it says "this section" it means the entire section that I have been talking about including its publication and making-available requirements.

The first exemption applies to information specifically required by Executive Order to be kept secret in the interest of the national defense or foreign policy. One of the ambiguities that we faced immediately with that one was what the word "secret" means in that context. I will leave it to you for the moment to decide whether it means the description of secret as you find it in 10501 or merely something to be protected, deserving of protection, or something that should be withheld.

The second exemption covers matters that are related solely to the internal personnel rules and practices of an agency. In its context, from the background of its legislative history,

that should not be read as though it read "internal personnel rules and internal personnel practices." The practices are somewhat broader than those that could be qualified by the word "personnel." Generally, it will cover such things, for example, as the advice you have put in the manuals of audit instructions that you give to your inspectors in the Department of Defense.

The third exemption is: matters specifically exempted from disclosure by statute. You heard Congressman Moss mention the more than eighty statutes that exist that do provide one way or another for the withholding of information.

The fourth is the one that we spent more time on than any other in the course of putting this pamphlet out: matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential. You will have great difficulty if you take only that language and try to discover whether a matter that is privileged or confidential but is nc commercial or financial information can be withheld. You will also have the same reverse difficulty. We thought it was pretty obvious that the statute was not trying to hide all commercial and financial information but merely that financial and commercial information that was privileged or confidential. In the light of its legislative history, we give it that meaning, and, of course, that treatment in the memorandum.

The fifth exemption is for inter-agency or intra-agency memorandums or letters that would not be available by law to a party other than an agency in litigation with the agency (and this means any other private party). With respect to that one, we have been asked to write a rather tremendous law review article and keep it up to date. We have many requests from the agencies to incorporate in the rather brief confines of this memo the kind of article that would indicate every case in which a document had been withheld and had been passed on by a court as "proper withholding." So that you could pinpoint types and kinds of documents that you would be free to withhold. The task isn't that simple, and what you get to ultimately is a treatise on the discovery rules that are used in the Federal district courts. There are treatises on that subject and one of them runs about four volumes. The discovery rules themselves cover ten pages in the U. S. Code, and it would not be an easy thing to describe except in the rather broad terms that we have used in this memorandum: basically, if a document is routinely available in litigation, so that at the mere asking for it by counsel everybody would agree, and the Judge would say, "Yes, produce it . . ." if it ever got to the Judge—that is being routinely available. If it is that routinely available in litigation and you are asked for it by a requester, then you have to give it to him. So what is routinely available in litigation, will be available to the public. If in the course of operating under the discovery rules in litigation, however, you would get into a very gutty fight

about whether a particular litigant should have a particular document either because of his position or standing or need, that document would not be routinely available in litigation; and, therefore, would not be available to the public.

As with all these other exemptions, if you have any difficulty in understanding what is covered and what isn't, what you ought to do is go to your nearest counsel at whatever stage you are in your agency—ultimately to your general counsel—and seek his advice as to whether documents should go out or shouldn't, under this exemption.

The sixth one is for personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Now, to some people, I guess to Louis Brandeis, the former justice in the Supreme Court, any invasion of privacy was a clearly unwarranted invasion of privacy. But we have heard from the subcommittee staff that those words that are used, "clearly unwarranted invasion," are meant to be a significant test. I suppose because there are three words, you could break it down and discriminate between "unwarranted invasion" and "clearly unwarranted invasion." And I suspect that can be done. No one has any idea what a district court is going to do with that, or an appellate court, for that matter, when the case hits them and they have got to make discriminating decisions of this sort. But basically that exemption covers personnel and medical files, and it says, "and similar files." I think what the latter may cover is information that, though not from medical or personnel files, would disclose things about a person that the person would consider private, or that might generally be considered private; so that the protection would extend as well to these other files even though they were not denominated "personnel files" or "medical files."

The seventh exemption covers investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than an agency. Now, here again you have a reference to litigation in connection with one of these exemptions; but this reference is quite unlike the one that I read to you in Exemption Five. There we discovered that if something were routinely available to a litigant, everybody could get it. But here, all investigatory files compiled for law enforcement purposes are put beyond the pale; nobody can get those. The exception in this case says, ". . . except to the extent available by law to a party other than an agency." We think that what that means is: well, maybe you are familiar with the Jencks Act, where if a witness is put on the stand and somebody thinks he is lying or thinks he is deviating from previous testimony he gave, there is a way of getting from the judge an order to get a copy of what he gave to the FBI or some other investigating agency before, to compare the two to see if he is lying. Under the Jencks Act, you have certain burdens before you can get that far. Also under the

Jencks Act the judge has to be satisfied of certain things before he will make the disclosure. What we think, in light of the legislative history of this act, seven means that Congress did not wish to disturb the area of the Jencks Act, or any similar areas where they exist. So that it's not a case of the entire public, something that every litigant can get. Here investigatory files are protected except in those instances where litigants who can use the Jencks Act have a right to get into investigatory files in order to get a copy of a document. So it permits district court judges to still operate under the Jencks Act—a far narrower exception to the exemption than you had in the fifth exemption.

The last two everybody seems to discount very much because they are so particularized.

Eight reads: contained in or related to examination, operating or condition reports prepared by, on behalf of, or for the use of, an agency responsible for the regulation or supervision of financial institutions. It clearly is pointed to banks and banking regulatory agencies.

The ninth is also very special: geological and geophysical information and data, including maps, concerning wells. That means only what it says and in a very narrow coverage.

We raised the question in the course of the memorandum whether you need eight and nine since you have Number Four, the one having to do with trade secrets and commercial or financial information obtained from a person and privileged or confidential. As you can see, if you talk about commercial or financial information, most banking information would seem to fit. Although I dare say most banking information is not—or much banking information—is not either privileged or confidential. But you can see that there is overlap between four and eight and four and nine. But I think the banking agencies will be happy that eight is there rather than have to rely on four alone, because we found our greatest ambiguities in number four.

Now, that is pretty much what the statute says, and I guess that any classification problem that might come up for you will come up under Exemption One only. And we, in the course of the memo, indicated that when agencies determine that matters within their responsibility must be kept secret in the interest of national defense or foreign policy, but the matters are not specifically required to be withheld by Executive Order or other authority, they should seek appropriate exemption by Executive Order, to come within the language of Subsection E(1), (That's the first exemption.)

Some agencies are making that attempt, and we actually have at the moment under consideration whether an Executive Order could be drawn to cover a specific area or areas that might be uncovered, or about which there might be some doubt. I am afraid that is about all I can say about that. I haven't any idea where it will ever go, or if it will, but the matter is being considered. I suppose if you know of particular, discrete areas that

are unprotected but deserve protection, you ought to let your superiors know about it so that they could consider whether they should make that kind of request. Thank you.

JOHN H. PENDER
General Counsel's Office, Atomic Energy Commission

It will probably take me a minute or so to get up the speed here, because despite Tony's protestations of modesty amongst experts I think we all ought to feel grateful for having Tony here, because at least on the Executive agency side he is today, I think, *the* expert at least in Washington, and it certainly gives you a nice opportunity for balance, having heard the expert on the Congressional side this morning, and now Tony this afternoon.

My own personal view is that this area that Tony has been talking about will, within the next year or two, be one of the most interesting and challenging, for even folks like us, who are largely concerned with classified matters.

I know in the case of the Commission's operations I think we can look forward to some interesting questions with our industrial contractors in the area, in particular with those who have a substantial interest with the Government, as a prime or substantial contractor. When you get into such questions as, "When are you in the position of a purely private firm or citizen, and when are you standing in the shoes of the Government?" I think we will have some very interesting times over the next couple of years. This is particularly true when you keep in mind that over the years we have been operating to some extent with not only classified information but information you might call pseudo- or semi-classified, which while not bearing the formal stamp usually associated with classified information, carries with it the characteristics—the characteristic consequences—that are associated with classified information.

I think, again, despite Tony's protestations, this is an area of something for you experts in classification management to be thinking about.

Now, one of the areas that Mr. Mondello mentioned is specifically exempted from the operation of this new law, and that is information the disclosure of which is exempt by some other statute. I propose to spend a few minutes exchanging perspectives with you folks on the perhaps most well known area, at least in the industrial technology area of information, that is not only specifically exempted from disclosure but which we are under a mandate not to disclose at least generally to the public. That is the area of Restricted Data, which is covered and controlled by the Atomic Energy Act. I am particularly glad to have the opportunity to exchange views and perspectives from our respective vantage points because of the tremendous and rather awesome responsibilities I feel that individuals with classification authority have.

As your fine luncheon speaker, Joe

Liebling, pointed out, what you do or don't do in this area has tremendous significance from the standpoint of the Government's national security effort. It also has tremendous significance, as many of you are well aware, from the standpoint of its immediate impact on industrial activities, the way you do business, what you can or can't do.

It has an impact even on our private lives because in your hands you have the trigger that if used brings to bear all sorts of resources and requirements to protect the national security.

And, of course, one that immediately comes to mind is the security clearance requirement. We all know the impact that this would have on individuals not only in their business and professional lives but in their private lives. So I think it is well to bear in mind, as we confront these problems, the authority as well as the responsibility resting in our hands.

Now those of you that have been associated with the Atomic Energy program well know the concept of Restricted Data. Its content, its definition, its statutory definition, have remained for most practical purposes virtually unchanged since first incorporated in the law in the 1946 Atomic Energy Act, the so-called McMahon Act. There was a slight change when the act was given a general overhaul in 1954, but I think that for most of us it didn't have too much significance. For those of you who are not too familiar with it, let me just repeat that what we are talking about is what the statute refers to, and that is:

All data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy . . .

Now the Atomic Energy Act is unique in many ways and certainly right at the outset it is unique in that it provides what I think can fairly be called rather technical guidelines as to what is to be classified and controlled and put under the mandate against general dissemination and release to the public. You have technical guidelines that I would contrast with, you might say, subjective guidelines. Although when you come to the declassification aspect you revert to what I would call somewhat objective-subjective political guidelines, in that the declassification of what falls automatically into the category of Restricted Data once the technical judgment is made, rests upon a decision that its declassification can be effected without undue risk to the common defense or security.

This special category was established in 1946, as most of you well know, but it is well to keep in mind, I think, that it was done with the consensus, at least in Government, of all those who were interested in and who had differences on other points as to how our Atomic Energy program was to be controlled and how it was to progress in the ensuing years.

The President, the various committees, the one headed by Mr. McMahon, Mr. May's committee, those

who spoke for the civilian control approach, those who spoke for the services of the War Department—all felt that in this area some special statutory control was necessary, and they all agreed on the approach we have been living with for the last some twenty years.

Once the technical judgment is made that information does fall within the purview of the statute, the statute then invokes other controls. While not fundamentally different from those we are normally familiar with in our overall defense information and classification program, they are invoked in some special ways. In many a case, some special sort of clearance is required to follow different regulations, and so on down the line.

Now another significant result of the statutory scheme that we have had to work with is that—and this point has been repeatedly emphasized by the Congress in the committee reports—once information is determined to be within this particular category there is only one way to get it out. That is through declassification. Sort of a choice of extremes. Although in '54 the Congress did relax that choice between extremes somewhat, at the behest of the military departments, by establishing Formerly Restricted Data. Actually, that's a rather narrow category, in that it concerns only information about the utilization of atomic weapons, and in large measure this is of interest to the military services in their operations although it can have some washback effect for those who are in the Atomic Energy production program.

There has often been a lot of confusion about what this concept of Formerly Restricted Data means, what its consequences are. In the simplest way, I, from my own standpoint, felt it was, assuming you understand where Restricted Data fits into the picture, this: Formerly Restricted Data is simply Defense Information for all domestic purposes, but for international purposes it is subject to the full extent of controls that the act imposes on international transactions that might involve Restricted Data. This, of course, involves such things as some cases of transactions with foreign governments, and generally these would have to be pursuant to a special agreement by the President himself, which would lie before the Congress, and which the Congress could—at least the way the law reads—veto.

The fact that we do have this statutory scheme, and the way it is structured is really a two-edged sword, in that once your technical judgment is made that you do have information that fits within this special statutory category you not only are under a mandate to classify it, but the Atomic Energy Commission in turn is under a mandate to take hard, current, and recurring looks at that information, so that it can be declassified as expeditiously as possible in order to carry out one of the chief objectives of the Atomic Energy Act, which is to assure early, expeditious, and free flow of this information amongst the industrial and scientific community. Because as has been recognized from

the outset, and as has already been said today, to a large extent our industrial and scientific achievement is due to the free society that we have, the risks that we have run in releasing and disseminating and ushering information out into the public community at a much earlier stage than other kind of society would tolerate.

I think the Commission, from what I have seen, has attempted to carry out this mandate of a vigorous declassification policy. Of course, there is always room for disagreement. It is impossible to satisfy everyone or even large segments at times. But those of you that have been in the Atomic Energy program or around the fringe of it I am sure are well aware of what a vigorous and zealous committee is always at the Commission's heels as far as carrying out the purpose of the Atomic Energy Act and the commission's responsibilities are concerned. And this is one area I can assure you the Joint Committee on Atomic Energy is most zealous about. As a consequence, today, at the risk of over-simplifying things, but for our general purposes at the moment, I think it is fair to say that despite the breadth of the definition in the statute as to what constitutes Restricted Data, we at the moment really have, you might say, three major scientific and technological areas that we think remain classified. They are the weapons program, obviously, the area of naval reactor information (Admiral Rickover's program) and the production technology, principally in the area of our so-called diffusion plants and possible substitutes for those—the various potential centrifuge fields. And, of course, the related production of the information that is of tremendous significance to the military national security posture as far as potential enemies are concerned. On the other side of the coin, I think you will find that for all practical purposes the information in the power reactor field, the information of great concern to utilities and manufacturing industries, is declassified.

As far as the future goes, "Where do we go from here?" it is hard to say, although it is interesting to speculate, particularly in the light of the negotiations that the Administration has been pursuing very zealously here during the last few years in trying to bring about a so-called nonproliferation dream. Once again, after the efforts of the late '40s and early '50s, there seems to be considerable promise and hope that we might get at least some measure of international control over weapon production. If the right kind of treaty did come out of this current effort, one could hark back to the purposes for which the Atomic Energy Act establishes controls, that is, that the controls were necessary at least until the time you had international control of weapons and weapon production. One might speculate that if we did have such a treaty, perhaps one of the offsprings might be an eradication or change in the statute so far as the total Restricted Data is concerned. I myself would think that with the mood of the time, if such a treaty did come about the situation would be such that the gov-

ernments would be expected, on a world-wide basis, to implement the treaty within their own country by imposing controls on their own citizens, their own domestic firms, because as technology advances we find that the potential for small segments of our society to frustrate the purposes of these kinds of controls advances. Again you have the two-edged sword. As technology advances to bring you social benefits, it also brings hazards where small groups can raise havoc with society as a whole. But these are some thoughts on the perspectives I bring to bear, and I look forward to hearing what perspectives you may have from your respective vantage points.

ROBERT L. GILLIAT

General Counsel's Office, Department of Defense

I don't believe that I am going to make a speech. In fact, I am not going to have to make very lengthy remarks in view of Mr. Mondello's lucid explanation of the Freedom of Information law. Yes, we are back to that topic because the only possible justification for having me on this panel is the work that I have done recently in connection with the Department of Defense's implementation of the Freedom of Information law.

In view of the presence today of Mr. Liebling and Mr. MacClain and Mr. Garrett, it would be presumptuous of me to speak on other areas of general concern with respect to classification, and if you have questions on these during the question session I will ask each of these gentlemen to heat up his microphone and answer them.

But back to freedom of information. The title of this panel is interesting, because it is entitled "Panel on Executive Orders and Laws Affecting Classification in the Government." I think my first observation with respect to the Freedom of Information law is that it neither effects nor affects classification in the Government. I think that ought to be the one message that should be emphasized. I say this because since the Department of Defense directive—which, incidentally, is Number 5400.7 and is dated June 23, 1967—since it hit the streets one of the common frequent questions or comments I have received is "Can't we avoid all the problems under the new law just by classifying more generously?" Well, I think you know what my answer is, and if you don't know what my answer is, you know that Mr. Liebling's answer would be to those comments: "Definitely not."

Classification is not affected by the Freedom of Information law. The same standards, the same criteria, are applicable. I think we can say the same thing with regard to declassification, the vigor with which you are pursuing the laudable goal of declassification should not in any way be lessened by reason of the passage of this act.

I think Mr. Moss's comments to you this morning indicated what the Congressional view on any effort to begin overclassification as a solution to the problem of the Freedom of In-

formation bill will be. The reasons for this I think are too apparent to most of you experts for me to mention. The matter of cost in protecting classified information, which Mr. Liebling highlighted to some extent in his remarks at lunch today, is definitely a factor. Another factor I might mention is that an individual who is denied a record he requests under the Freedom of Information bill has a right to appeal that denial. He has a right to appeal it ultimately to the head of the component. Now in the event that the basis for the denial of the record is its classification, I believe that the individual who has classified it should be prepared to defend his classification to the head of the agency or his designee for that purpose.

Whether the courts ultimately, in their *de novo* review of refusals, will feel empowered or required to challenge classification is a question that no one can answer. I would hope not. But in the event that they should interpret their authority as requiring this, I think we should all be prepared to defend our classifications. Indeed I think we should always be prepared to defend our classifications from all challenges.

Now the second point that I think I want to make—and my orientation is necessarily a Defense orientation today—is that the Public Information law has no effect on requests to Defense industry. All my points seem to be "negative," but I think I am really responding to questions I have had.

The law is applicable only to the Executive branch, and this does not give an individual the right to request the Government document from Defense industry and obtain it from them. I would suggest that such a requester be referred to the Government agency that is the constructive custodian of the record involved.

Thirdly, you will note in DoD Directive 5400.7 that we have indicated that the designation "For Official Use Only" may be used where appropriate to identify material that comes within the statutory exemptions of the Freedom of Information law. Now, Representative Moss today slipped a little in his language at one point, as most of us do from time to time, by calling F.O.U.O. a classification. It is not a classification. There are only three classifications under Executive Order 10501. You all know what those are. The use of F.O.U.O. is solely for the purpose of designating a document that we in Defense feel comes within the exemption from the Freedom of Information law, when we feel another individual receiving that document might not be aware of its qualification—for example, for exemption. It is for internal convenience only.

The press was rather unhappy about the continued use of F.O.U.O. in the Department of Defense directive. They thought it something new. As many of you know, it is not anything new. We can trace its history back at least thirteen or fourteen years and probably beyond that. I asked Don Garrett and he quickly gave that kind of figure, and Don always knows what he is talking about so I'll not challenge it.

The F.O.U.O. marking I must emphasize does not mean an automatic withholding of a document. It means that the originator of the document, or someone empowered to mark it F.O.U.O., had thought that it comes within that exemption. The person who is given the authority under DoD Directive 5400.7 for implementing regulation of a component will have to make the ultimate decision whether that document actually comes within an exemption or not. And this I would say applies—primarily when I am being precautionary—when a document has such a mark we are concerned that there be an independent evaluation. Conversely, the absence of F.O.U.O. does not mean that a docum '1 necessarily be released.

The last thing I want to say about "For Official Use Only" is that the directive, on page 17, paragraph 9(d) encourages paragraph marking of F.O.U.O. material. I can say in reference to this, as well as to the classification area where this seems to be controversial, that such paragraph marking will greatly facilitate the evaluation of the validity of that particular designation.

And as to the details with respect to the handling of F.O.U.O. and other aspects of this designation I think that you can anticipate in the not too distant future an instruction or amplification.

Lastly (I would say I don't think it's necessary to put much emphasis on this because Tony has gone through these exemptions rather clearly) some of the things that you seem to be concerned about—I take this in part from your questions to Representative Moss today—do fall within exemption areas, and I urge you to consider these exemption areas carefully. This is true particularly with technological data of various kinds. It may very well fall within Exemption Four. This is B(4) 5 U.S.C. 552, and as it is written currently in the Department of Defense Directive, this exemption is interpreted as follows, referring to records:

> "Those containing information which a component receives from anyone, including an individual, a foreign nation, an international organization, a state or local government, corporation or any other organization, with the understanding that it will be retained on a privileged or confidential basis, or similar commercial or financial records which the component develops internally, if they are in fact the kinds of records which are normally considered privileged or confidential. Such records include . . ."

And they give a list of examples, which I will not take the time to read right now. But I think that the kinds of documents with which you are concerned will frequently come within this particular area of exemption.

Another area of exemption that will be of great interest to those of you concerned with personnel security review is the one that Mr. Mondello mentioned for personnel, medical and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Now, I think that that exemption, by any reasonable construction, will protect the kinds of security records most of us are intent on protecting. In fact, in the Department of Defense Directive 5400.7, on page 15, we have listed this kind of record as an example of the kind that is protected. We describe them thus: "Those compiled to evaluate or adjudicate the suitability of candidates for civilian employment and the eligibility of individuals, civilian, military, or industrial, for security clearances."

Now, there are some others that may be of interest to you. The one for investigatory files may be pertinent to you on some occasions. And the exemption for documents that involve internal practices would be of some interest to some of you. I would hasten to add, in connection with that one, and I think Tony tried to make this point and maybe he did make it, but let me remake it: an exemption that may be suitable for use with regard to one aspect of this statute may not be suitable for use otherwise. Let me illustrate. The internal document exemption, the internal practices exemption, may mean that we need not publish in a federal register or make available in our reading room, a maintenance manual for a truck, because it is solely internal. There isn't any interest in it. Nobody probably wants it except a guy who comes along every ten years and writes in and asks for it. I would think it entirely inappropriate for us to deny his request under Section A (it used be be C).

Now, lastly, there has been some concern about the Export Control Act and the Mutual Assistance Act. At one time these were listed as examples of statutes which authorized exemptions under the Freedom of Information law. We removed those as examples for the reason that they seem to be confusing to many people. This doesn't mean that the Export Control Act or the Mutual Assistance Act, or whatever it is, has somehow been appealed. Obviously, they have not. They are still as effective as they ever were. People in the international security business felt that there might be some confusion in considering these a basis for domestic withholding of information. For that reason they were removed as examples. Those of you perhaps that saw the directive in a draft form, as Mr. Moss did, would wonder about the elimination. That is the explanation for it. I might say that with reference to Mr. Moss's comments this morning that they illustrate how much more adept the Justice Department is in drafting its documents then the Defense Department is. Justice by my count received, at least on two occasions, plaudits, and we received one condemnation. So, I am taking lessons from Tony. Every Thursday from three to four I am learning how to write regulations that please members of Congress.

KEVIN T. MARONEY
Chief, Appellate Division, Department of Justice

Fellow panelists, ladies and gentlemen: I am going to try to cover this

subject as briefly as I can to permit you sufficient opportunity for questions of the panel.

There are four basic statutes that could roughly be termed espionage statutes, one of which you already heard mentioned—the Atomic Energy Act. And, of course, the primary purposes of that, at least the espionage provisions of it, are to protect Restricted Data from improper transmittal to unauthorized persons. To my knowledge or recollection, there have only been two espionage prosecutions under the Atomic Energy Act: the Rosenberg case, back in '49 or '50; and more recently the case involving an Air Force sergeant, in Kansas City, the case which was eventually lost in the court of appeals because of the confession problem that was present.

The espionage statutes we more often deal with and utilize in connection with the typical espionage prosecutions are 18 United States Code 793 and 794. They are part of the Espionage Act of 1917. They have been on the books, with modifications, since that time. The first section, 793, relates to obtaining information with intent or reason to believe that the information will be used to the detriment of the United States or the advantage of a foreign power. The 794 provision relates to transmitting information, again with the intent or reason to believe that the information will be used to the injury of the United States or to the advantage of a foreign nation. Both of those "horns" of the intent do not have to be present. In other words, we do not have to prove that a person in transmitting information improperly intended to injure the United States. It is sufficient if he transmitted it to a foreign power or with intent that it would end up with a foreign nation, knowing that it could be of benefit to that foreign nation. And, of course, the foreign nation doesn't have to be a hostile nation or an unfriendly nation. An improper transmittal to a representative of any foreign nation is sufficient to bring the act within the statute.

The fourth statute, which has only been used once, is in Title 50, and it relates solely to employees of the United States who transmit information that has been classified to an agent of a foreign government. So that statute has a very limited application, applying only to employees of the United States. The only case in which it has been used was against a former State Department foreign service officer, Irvin Scarbeck.

Now, in any prosecution under 793 and 794, the Government cannot rely on the fact that a document which had been classified was transmitted to a representative of a foreign government. It must prove, additionally, that the information in fact relates to the national defense. The fact of classification is evidence of that but it does not establish it. The principle was established by the court of appeals for the Second Circuit in a World War II Nazi espionage case, the United States v. Heine. That case involved, as I recall, the collection by individuals on behalf of Nazi Ger-

many of technical information relating to aircraft production but which was of a nature that was publicly available. In other wards, any person in the aircraft field could easily have secured it, and many did secure it and had this kind of information. The court in the Heine case held that even though it might be said that this information relating to aircraft production would be helpful—unquestionably it would have been helpful and was helpful to the German government at that time—the statute contemplates not only that it does in fact relate to the national defense but that the Government has made a conscious determination to withhold it from the public domain for reasons of protecting the security.

So in any prosecution we bring for violation of 793 and 794, we have to prove these two elements. And sometimes establishing, by testimony, why a particular classified document does in fact relate to the national defense requires the production of additional facts to prove that point. So sometimes an evaluation must be made in a circumstance such as that as to whether the proof required to meet that test would be more detrimental to the Government's security program than if we didn't prosecute at all. Under Title 50, Section 783 which relates to a Government employee turning information over to a representative of a foreign government, the fact of classification itself is sufficient to establish the offense. And in connection with First Amendment arguments that have been raised under this, we have argued at least, and argued successfully in the Scarbeck case, that in view of the limited application of this statute applying only to Federal employees and proscribing only transmital to representatives of a foreign government, that you don't have a First Amendment problem, at least not a First Amendment problem that would be present under the general statute.

Now, of course, the espionage statutes, as all of you I am sure well know, cover more than the classical spy situation. They, of course, provide penalties for losing or causing to be compromised classified information through gross negligence. For example if someone on business has his brief case with classified information and is at the airport waiting for a plane and he has a couple of martinis and rushes to catch the plane or something and leaves his brief case, that might well come within the gross negligence provision of the statute and would be punishable under it. Obviously, most situations such as that don't result in criminal prosecutions but are handled administratively by the particular agency that would be concerned. But the point is, the statute does cover that kind of problem. It also covers or proscribes—makes it a criminal offense—for anyone who has knowledge that classified information has been improperly removed, unlawfully removed or turned over to someone, to fail to make a proper report.

I think that it is pretty clear, and it certainly has been well publicized, that in the past decade or so there has been a substantial step-up in espio-

nage activities of the Soviet-bloc countries. And, of course, if the number of prosecutions brought in this area is any kind of a barometer, a comparison of the number of cases brought in the past ten years with the decade after World War I indicates that of course the step-up is three to four times what it was at that time. In the decade following World War II in 1956, there were only three or four cases brought involving Soviet espionage. In the past decade, from '57 to '67, there have been nineteen espionage cases brought, sixteen of which involved Soviet espionage activities.

J. Edgar Hoover, in an article appearing in the *Industrial Security* magazine about a year ago, pointed out that not only had there been an increase in the past ten years or so in Soviet espionage activities, but their method of operation has become more sophisticated. Unlike the years under the Stalin regime when Soviet representatives in the United States were rather clannish, and somewhat seedy in appearance, and unwilling to mingle, the Soviet representatives in the United States today are, of course, much more polished and all too willing to mingle with American society.

I might digress just a minute here to point out again what all of you probably realize pretty well, that in the area of espionage activities the Soviet utilize two types or two kinds of agents. One is called a "legal agent" —that is, an individual who is legally in the United States under some legal cover, such as a connection with an embassy or connection with a mission at the United Nations or international group. The other type of agent is called a "illegal agent." He is a person who is in the United States illegally, and, of course, the ideal situation for them is the United States doesn't even know he is here. The case involving Rudolph Abel is a pretty classical example of an illegal agent in this country. And while a legal agent, a chauffeur at the embassy or a second secretary, or someone of that kind, of course is free to contact Americans, people in the Government, people in industry, an illegal agent, sometimes, of course, must keep his real identity unknown and would not or should not communicate directly and in person with a legal agent of the Soviets'. In other words, Abel, for example, would not have a personal meeting, would not have lunch with the second secretary of the Soviet embassy or consulor office. As a consequence, of course, the method of communication for an illegal agent, as was shown by the evidence in that case, is to use what they call "dead drops." If the legal agent is going to communicate with an illegal agent with the Soviet Government he would leave a message in a previously arranged drop point. And, of course, all kinds of devices such as hollowed out coins are utilized in that regard.

Today, of course, much of the activity, much of the espionage activity is carried on directly by the so-called legal agents making direct contact, personal contacts with American citizens here in the United States. Of course many of these have the hidden purpose of attempting to cultivate a hidden friendship and to utilize that

friendship as a wedge in securing cooperation from the American who might be in a position to furnish valuable information—classified, if possible. And again, as Mr. Hoover points out in that article that I referred to, once this personal relationship is established, either through meeting somebody at a cocktail party, living in the same neighborhood, or such a thing as that, then, of course, a Soviet agent who has an espionage mission is supposed to look for some lever by which he can persuade the American to cooperate. Hoover points out that there are these following levers that are utilized commonly and are shown by some of the espionage cases that have been brought in the past ten years. Of course the first is the ideological appeal. If he can find someone in the position to furnish information who is also ideologically atuned to communism or is pro-Soviet, this of course is an ideal kind of lever. The second might be determining that an employee of some industry or Government is disgruntled, has an ax to grind, and encouraging him to take it out on his employer or the Government. Another is an appeal to the ethnic origins of the individual American, who may be Russian-born or whose parents may be Russian-born, or be from some Soviet-bloc nation. A hostage situation, of course, is well known in circumstances where a person here in the United States has relatives in an iron-curtain country. Coercion and blackmail are quite commonly used as a Soviet espionage technique. Another is an appeal to a free exchange of information—that this idea of classification is only harmful to the progress of mankind and that science and so forth would be better served if information were freely exchanged between countries. And the last, perhaps the most base, I suppose, is the appeal of money.

It is your job, it seems to us, and our job as well, to be familiar with the techniques of Soviet espionage and do everything that we can to make the job of Soviet agents tougher. I think it is the job of all of us to ensure that all employees who have access to classified information are familiar with the techniques that are being utilized by Soviet agents, who in making these personal contacts, building up these personal relationships, lead up to something. If our people are contacted they should be prepared, and they should not become duped into some unwilling cooperation. Thank you.

DONALD GARRETT: Mr. Maroney, under many circumstances industry will develop technical data and technology on their own, privately financed and not related to any Government contract utilizing any classified information. And yet many times this technology has a terrific impact on national defense. How do you suspect the Heine case would affect the application of the espionage laws to the prosecution, or to deter the release of this private technology which could be used to the injury of the United States or to the detriment of the United States or to the assistance of a foreign nation?

MARONEY: Well, first of all, let me ask another question: Does the Government know of the existence of this information, of this data?

GARRETT: In both instances. Sometimes they do know; sometimes they do not.

MARONEY: I may be wrong, but it was my understanding that the Government was in a position—had some procedures for classifying information of that kind which does in fact relate to the national defense, and for that reason it should be protected. For example, patents. Doesn't the Patents Secrecy Act cover things of that kind?

GARRETT: As I understand it, the Patents Secrecy Act applies only if the individual filed a patent application. Let's assume that he has not filed a patent application. There is some question in our minds, at least in our General Counsel's Office. Our esteemed General Counsel has advised us that this purely private information may be too far for us to reach for classification under Executive Order 10501, which may indicate that we are not in a position to classify even though if it were involved in a military application, or if it were developed for the Department of Defense, we would classify it. Let us assume here that we are not in a position to reach it for classification under 10501. Would, in your opinion—and I believe I am correct in referring to 793(d), which refers to the mere release of information to unauthorized persons when it is known or reasonably expected that it could be used to the injury of the United States or the advantage of a foreign nation—would 793(d) apply?

MARONEY: 793 requires that the information has been classified under the authority of the President.

GARRETT: 793 (d)?

MARONEY: It must be information that has been classified under the authority of the President. The present authority for classification is 10501; so that 793 would not be applicable, today, anyway, unless it has been classified under 10501. And I think that under the decision in the Heine case and the rationale of subsequent cases that followed, is that if the Government has not made a determination that the information should be kept secret, must be kept secret in the interest of national defense, it doesn't come within the purview of the espionage statutes. Now, as I understand it—and I am not really an expert in this, I just have some peripheral information—there are, for example, controls over the export of technical data. I think the Treasury Department, and the Defense Department, I suppose, regulate that. But that, of course, would only concern the export from the United States of that data.

GARRETT: That would, of course, come under or cover the technical data that fall within the International Traffic and Arms Regulation, I believe.

MARONEY: Maybe one of these gentlemen from the Department of Defense could further enlighten us.

NELSON: Well, Mr. Garrett, any Government agency that had knowledge of this type of information with-

in some corporation or manufacturer, it certainly would be incumbent upon them, I would think, to make every reasonable effort to arrange with the manufacturer to see that that information was classified. Now, you might run into a situation, I agree, where you might not be able to force the originator or the possessor of the information to classify it. I don't know what you do in that circumstance. But I think that's more hypothetical than practical. I think any corporation or any manufacturer, anybody that had that kind of information, would be cooperative with the Government.

MARONEY: I am sure you are right, Mr. Nelson. As a matter of fact, we have had a number of occasions in which this purely private information has been noted for classification, let me put it that way, by Defense, and the contractor, recognizing its value to national defense, has acceded to our request to treat it as classified. In that respect, I would suppose that that kind of determination by the Government would satisfy the Heine case.

NELSON: I think so. Mr. MacClain?

GEORGE MacCLAIN: I would like to express a sort of point of view which is perhaps a little different. I think it's possible to treat the act of classification as merely a matter of form or as a matter of substance. I would take the point of view that if the Government has no power over the information in the hands of the private party it would be a matter of form and not substance to treat that information as classified even as a matter of agreement. If that is right, then I suppose the test of whether it is classified would come up in the court action. Were I asked to rule on it, I would consider it as not classified, because the Government really has nothing but the relationship of a consensus with the owner of the information. I don't know that this is right but it might be possible, through purchase, payment of a price, for the Government to acquire enough ownership interest in it to make it a perfectly legal thing. This would be the approach that I would follow.

KENNETH WILSON: I have a question of Mr. Gilliat. If I understood you correctly, you said that you envisioned the possibility under the Freedom of Information Act that it might be necessary to defend the classification of the information in a document if someone took court action to force the Government to release it. This classification is normally assigned through the famous DD-254 by the originator in industry by what we call "marking." Would you also envision, then, that the person who originally marked this, the company or its representative, might have to defend in such an action his proper interpretation, his proper application of guidelines in marking?

GILLIAT: You are suggesting that the origination of the classification comes from industry?

WILSON: No, no. The Government normally tells us what it feels should be classified about a particular contract through a form—of various degrees of adequacy. The scien-

tist who writes the information, or the company representative, is actually marking the document—and, of course, the marking is what places it within the pale, if you will, and is what we are contesting in this case. Would you envision that the company or its representative, then, must defend its application of guidance, its proper interpretation of that guidance?

GILLIAT: No, no. I think it would be up to the agency head or the component head as we have described them in the Department of Defense directive to defend it, if in fact that is essential. I think Mr. Mondello might want to speak to this point—whether this is likely or not. Perhaps he would prefer not to. But I would think that you might be, or someone at a subordinate level might be, in a position where he should have to explain the basis for the classification marking to the component head, or to his designee for purposes of making a final determination for the component as to whether they would release it or not, because the requester is not going to be able to go to court, we assume, until he's exhausted his administrative remedy. Now, I don't know whether, if we were forced in court to defend the classification, it would or would not be appropriate at some point to seek the technical expert witness kind of thing that might come from industry. I just can't envision the law that far. We haven't got an interpretation. I don't know. Tony, do you want to speak to this at all, or would you rather not?

MONDELLO: Well, it is difficult to say what is going to happen. The only approach we have had to it recently is a case that happily we won, where Mr. Katzenbach, then the Attorney General, personally reviewed the files and personally wrote part of the "assertion of privilege," a statement running about 10 or 12 pages. And he tried very hard in describing the documents that we had withheld —some forty-nine documents, I think, out of about a grand total of 4500, which we managed successfully to retain—he tried to give the judge an appreciation of what the general content of those documents was without tipping our hand as to what was in them. He told both negatively and affirmatively the kinds of things we wrote in documents of that sort, and even more closely the kind of thing covered in these documents. Now, I dare say, if the system breaks down, if you have to go to court and show the document to anybody to justify it—but I can't imagine that we will ever have to go that far. Wigmore, in his treatise on evidence, talks about this and thinks it is terrible that a mere clerk in the War Department can be privy to these secrets and they won't show them to a Federal district judge. But the fact of the matter is, we don't control judges. We cannot control what they do with the information once they have it. We can control the clerk, and if we fail, Mr. Maroney will take care of you. So, it is a real problem. The only approach we know to it so far is to bring the court as close as we can to what is in these things. I think most of the problem that Mr. Gilliat was talking about

before, about the justification of classification, is going to wash out before you ever get to court. Because if you have once decided that classification is wrong, you will probably give up the document, and that is the end of that.

FRED DAIGLE: Mr. Gilliat, I hope you will appreciate the interest that you generated when you mentioned the anticipated paragraph marking of "for official use only" documents. The basic question I have is in this particular application. I got the indication from you that this marking would possibly be used to indicate an exception under two through nine of the various exceptions of the Freedom of Information Act, and that classification marking of the three basic markings would be used for exemption under Exemption One. In other words, all DoD material would be exempted under Exemption One, and if the Department of Defense gets into any of these other businesses they would use something like "official use only" or other such marking. However, I got the impression from Mr. Mondello that the Department of Defense would not necessarily be concerned with any exemption except Exemption One.

GILLIAT: No, we have several pages of explanation of things we are very much concerned with in addition to Exemption One. I don't think that you could begin to suggest that we would make all of the material—medical files, personnel files—available to any person who asks, for whatever reason. Obviously, we are concerned with those, and prefer to mark documents containing such information, records containing such information, "for official use only." I think that's a bad example, because usually personnel records are kept segregated as personnel files. There is no need to mark them because the only people handling them will know that they are for official use only and there will be no obligation, perhaps, to mark them. But in the document where there might be some question on the part of the persons handling it, they should know that there has been a determination by someone that this is considered to fall within the exemptions.

DAIGLE: I got the impression from the speaker this morning, Mr. Moss, he was taking this "official use only" as an example of something that would no longer be permitted. There seems to be a little difference.

GILLIAT: I think he had a legitimate objection here when he says that —how many did he say there were— fourteen?

DAIGLE: I think there were originally twenty eight and they have got it down to fourteen.

GILLIAT: Yes, now it's down to fourteen. And I think there may be something to be said in favor of getting agencies to agree to have one designation for such material, if possible. However, in the Department of Defense I can think of one very good reason for not changing "for official use only," which is the thing we have traditionally used for this kind of information, and that's the expense of buying all those new stamps. I have

heard the arguments, saying that there are many more descriptive terms than that and more effective terms than that. I think a lot of them make sense, but, you know, we are sort of stuck with this one and it doesn't really make that much difference.

WILLIAM FLORENCE: I have a question that relates to the one that was asked first—Mr. Garrett's question—relating to privately owned information. Perhaps I might ask Mr. Mondello to answer the question of whether the first exemption of the Information statute may be applied to information other than information of the Government. In other words, let's see if it may be applied to private inventions or other privately developed processes.

MONDELLO: That's a hard one. First of all, the first exemption again is preceded by the words: "This section does not apply to matters that are specifically required by Executive Order to be kept secret in the interest of the national defense or foreign policy." The entire statute has to do with the Executive branch. I don't know what the powers of the President would be, to reach out to private property and declare that it has got to be blocked off for national defense or foreign policy purposes. Conceivably, it might be done. And Congress, for example, can ban the use of narcotics, the possession of narcotics, this kind of thing. It's conceivable to me that a way could be found to permit the President or the Congress to reach ideas and information of that character. But I should tell you there would be very serious constitutional implications in such a reaching out, if I understand what the Supreme Court was involved with in the Steele case some years ago. So, it's not a matter you can rush willy-nilly into, but it is a possibility that somebody ought to consider.

PANEL – RESEARCH IN AUTOMATED CLASSIFICATION MANAGEMENT

Gilbert C. Jacobus, Office of the Comptroller, Department of the Army, Moderator

JACOBUS: The type of material that will be presented this afternoon will take us into the wondrous world of the computer. This is something that we all face. Sometimes it seems a little bit like Lewis Carroll's *Alice*, actually. You remember "The Walrus and the Carpenter:"

"The time has come, "the Walrus said,
"To talk of many things:
"Of shoes and ships and sealing wax,
"Of cabbage and kings,
"And why the sea is boiling hot,
"And whether pigs have wings."

Well, automation experts in recent years tended mainly to expound upon wonderous accomplishments just over the horizon. There's a new philosophy abroad these days—an old philos-

ophy, really—which makes more sense both to business managers and to scientists. It causes us to examine what computers are doing and what they can do within resources that can be allocated to computers considering the economies of a given situation.

Computer technology, if it teaches anything, emphasizes precision in thought and clarity in communication. Aside from computers, for years now there has been a tendency in many instances to be highly vague, often ambiguous, in relation to security classification activities. In other instances, we have been overly specific.

In a sense, then, there is a built-in conflict in this automated environment, an environment that is so rapidly engulfing our managers, our scientists, and our office workers. Perhaps we should remind ourselves that security classification encompasses personnel of various skills and levels of operation, hardware of various kinds, documents of endless variety, communication facilities—especially electronic—and most decidedly, ideas in any form.

This afternoon your panel intends to provide food for thought in relation to basic problems that call for solutions that are sound economically, organizationally, and sociologically, if you will. This new world of ours is still an old world without any doubt whatsoever, a world in which we encounter new manifestations of old problems as well as some different problems.

Our speakers come to you with a wealth of knowledge, stemming from wide experience in the area under discussion.

CHESTER L. GUTHRIE
General Services Administration

Over that fine coffee out there and those homemade brownies, our fearless leader, the censor for General Eisenhower, said that my purpose here was to first bring black despair, and then hope. I can assure you the first I am up to; but I don't know if I am up to the second. At least I can try.

This is a very interesting subject, really. I hate to reveal my age, but I think I am in the same period as our fearless leader, because I remember running into the problem of classification in terms of security during the war. The security officer was assigned to me, and I can imagine no more fantastic experience than to have that happen to one who never had to work in this field. I can assure you, I have both compassion and a great deal of confidence, not to say a very high regard, for your entire profession. I never did solve it. I don't think the security officer did either, but we came through pretty well. No courts-martial. Actually, the subject so intrigued me that I did look a little bit into some of the thinking. I am not trying to preempt one of our speakers here, who has or is going to go more into history, I assume.

But the search for security of data has gone back as early as man—as we know man. We all know the way in which the heralds of ancient Greece were made secure. If you were to

take the herald from the opposite side when he came to give you the word and put him over the coals until he talked, you could be assured they would fry yours when you sent him over with your message. So the heralds of ancient days were relatively safe. Information wasn't.

You remember the story of the time of the Chinese emperors and Ghengis Khan, when they would tattoo a message on a man's head, let the hair grow out, let him carry the message, then he disappeared from the face of the earth.

Another interesting type of security, against fraud, was the use of the ancient clay tablets—probably the only secure concept that has yet been worked out. If you remember, you put the document—let's say a will or some other important document—on a clay tablet. Then you'd cover it with a clay envelope. It all shrank together and you hardened it and you could never change this thing because whatever you did to the outside envelope wouldn't show up inside, and if you tried to change envelopes they never shrank together again. So that it was an ideal thing. I think that's where we got the double envelope concept that I remember so vividly. We went through a lot of codes and methods of one sort or another, all of which are very difficult to succeed with, as you may know. I think the only successful thing we had was when we used American Indians of some of the lesser-known tribes with languages that no one else knew. Those codes were never broken, to my knowledge. Too bad they weren't. We would understand how to handle the moon visitors or the outer space visitors that we keep thinking about.

Actually, more seriously, the compromise of security, be it administrative, industrial, national or what not, has its rules, depending upon the situation and what we are trying to accomplish. We can say that certain data have been compromised and certain data have not. Our problem—and this is where we began to enter this area of black despair that I threatened you with—lies with the computer.

The computer has brought problems to us that are dimensional rather than fundamental. I would like to emphasize that. If we can keep that thought in mind I think the rest of it becomes a lot simpler. Dimensional? Well, for example, we are used to alphabetic language. Suddenly we have it in digital form. We are used to it in visual form, and we have it in impulse form. We are used to it for human brain manipulation, and suddenly we must have circuitry manipulation. This hasn't changed anything but the dimension, but that it has changed. It frightens one a little bit when you think of the possibilities of these circuitries. I don't know if any of you were acquainted with one of the techniques used in World War II, when they were using halfwave transmission, placed up tightly against the transmission wave of the Japanese radio. Are you? Anyhow, to the Japanese this seemed a little bit like static, but it was readable with the right kind of circuitry.

So, for a long time, very important messages simply rode right on the back of the Japanese transmission. It gives you something to think about.

For example, almost any type of circuitry will transmit a bit. We know that we are grounding our computers in ways to stop transmission now, but there are many ways in which they may be transmitting. It may not be worth trying to read them, but on the other hand we do know here that they are transmitting, and this gives us something to think about.

The linkage involved is a lot different when you are linking electronically from when you are linking by spoken word or written message. It's almost like reading minds. You see, you've changed the dimension again.

I remember one story—I think it is apocryphal, but it may be true—where one of the large universities in Boston—I will not mention its name—put some examination information into the data bank that was—I have forgotten where the computer was—probably at Penn—and it didn't take long for the senior students or the graduate students in Boston to figure out a way to dial into that computer. It took a little bit of logic, and they could do it. This was one of our first worries about "linkage".

We get into the problem of satellites. I mean satellites that are small computers to big computers, not the kind flying overhead, although they, too, may be trouble. The satellite has linkage, of course. This has both possibilities and problems.

Probably one of the weakest points is the programmer and the program. I just left hearings over at the Brooks Committee where they were worrying about what happens to old programs when the programmer is promoted or finds a GS-11 in another agency or leaves you for the telephone company. The chances are that you can't find the program he wrote, and the first time you update you are in serious trouble. On the other hand, this program is just kicking around. Nobody ever thought of it as a basic document the way it is. And yet if there is anything that could compromise the administrative, industrial, or security function in general of a computer, it is that programmer and his programs. So here is a whole area that needs some logic. I don't think we can do what one would be tempted to do: let the programmer do his job and then revert to the concepts of the ancient Chinese emperors and let him disappear from the face of the earth. I don't believe that is acceptable. But we have the problem.

There is another side to this I want to bring to your attention, too, while I am building the problem. The computer, with its ability to bring many data together and new relationships of time and space and data itself, has a way of giving meaning that otherwise might not exist, or might not be available. This is one of the problems of ethics and procedure that concern the recent hearings. There was a hearing, if you remember, before the Gallagher Committee in the House last July, on the subject of privacy. Then there was another one before Senator Long

in the Subcommittee on Administrative Practice and Procedure, a judiciary committee, in which this subject was rather thoroughly explored. There was a lot of worry by a lot of people because nobody quite understood each other. There is an ethics problem involved. There is a fear involved.

It is true that if you can bring many data together in new relationships you begin to get information. I will give two examples. One is a simple one. I will fuzz this one over because I can see that it is a little on the dangerous side. I had to know what size, how many people were involved in one agency because we were doing some long range planning. The agency was unwilling to tell us, but there was some knowledge of how much space it had been occupying and how many records it could produce. Well, with these two data together, we were plus or minus 3 percent on the thing as it finally turned out. So here were perfectly innocent bits of data that, brought together in a new space, time and information continuum, are meaningful. Now this we all know; this is an old thing.

I hestitate to tell one other story to illustrate it, but I shall because I understand all of you are security classified and this is the one place that I could probably tell the story. This is the only place and time I ever told it. During the war, there was a number of apparently unrelated innocent bits of data that came across my desk. One was that the Admiral (this was the Surgeon General) needed an extra office. His office was down in Main Navy instead of over here across the street where the Bureau is. And yet the next bit of data was that there was only one person that had been added to the staff down there. In those days of tight space this didn't make much sense. The Admiral was a very cooperative person, so that worried me a little bit. Then there was a request for a safe. Well, there was a safe down there. But, safe they got. Safes were under tight control. But that's fairly innocent. I mean that's a place you'd expect a safe. Then in the log came a little entry, some days later, of an important biological specimen and it wasn't received anywhere except taken to this room number. Well, at that point the Security Officer called me, and he said, "Do you think that might be what we are worrying about, biological warfare? If so, we'd better watch this thing." So I said, "I will tell you what we will do. We will announce a routine check of all safe numbers and you go down and get the safe checked on that, and at least we have done what we could. And don't even alert the Admiral on this one." So, sure enough, it wasn't a random number that was down there. In any case, this turned out all right.

The only point I am attempting to make is that relatively innocent bits of data coming together can suddenly have a lot of meaning. I am using the very simple things. But it is in that frame of reference that some of these large data banks are beginning to frighten people. They know just where you were any time of the day, and, roughly, what you were doing.

And I don't know what the implications could be. Things like this are what worry people. So that's another side of it. Despite all this discussion of the computer and its problems, let me urge you to rely on your old principles. These are established and understood. The computer did not abolish the principles. They are still valid. They are in a new dimension. Your problem is to discover what they mean in the new dimension. "Need to know"—what is the "need to know" in the new dimension? That in this case happened to include the programmer, you see. What is "need to know?" What about clearances? Where is the new double envelope? But everything that has been found to be appropriate is probably, in principle, just as true with the computer as without. What can cause trouble, I believe, is not really realizing there is a new dimension applying and so the old principles must be rethought in terms of the new dimension. For example, I think some of the obvious things might be screened, which means the inquiry and source of inquiries. I don't know whether we'd go back to the old "hang up and I'll call you back" technique, but that is one technique. There are degrees of security that probably have to be reestablished in terms of the computer. I mean there is quite a difference the way you handle very, very top security from something that is of minor administrative confidentiality. But that all becomes important, because on top security you are involved with the proper person, inquiry, so forth and so on. And don't forget, there's at least one new thing that has been added, and I think one of the other panel members will go into it: the voice print is just as much your own as your fingerprint, and we may have reason to use this. Obviously, anything of security value should have some kind of code thrown on to it just to keep it from accidental disclosure. We probably should get some security training for our programmers, if we haven't already done so, and give them a special type of training so that they, too, can serve their proper responsibility. And I dare say that some more thought will have to be given to what has already been talked about—use of random numbers as identification techniques. There are a number of programs that have been worked out along this line, but I dare say there is a little more thought to be given. I think the whole point is, I don't believe this thought has been given to it by security officers who'd know whether or not it was accomplishing its purpose. There have been a lot of other people worrying about these subjects. There is always the use of people.

Remember we file stuff separately, too, when it's confidential. Well, there is such a thing as a satellite computer, and maybe there's something there, to be given some consideration. It's such an intriguing subject that it would be fun to continue this, but I would be preempting the time of the panel that I think have more of the answers.

All I was supposed to do was to bring you black despair and offer just a little ray of light, so I leave you

with this one message: Do not—do *not*—abandon your principles. They are still valid. Simply review them in terms of dimension, and don't be overwhelmed by the engineers who are giving you an engineer's answer. It is possible that the engineer's answer needs the professional classification person's concept to really be valid. I thank you.

JACOBUS: Thank you, Dr. Guthrie. You will note in the discussion Dr. Guthrie gave you, he covered personnel, hardware, documents, ideas in terms of relationships—the very thing I talked about in the introduction. He mentioned that new relationships create information. Well, this is an old story to information men and security people. He made the statement that basic principles are still valid. I question this. This is something that you and security need to do some thinking about. In so many instances, in running a war, we discovered the fact that security is an obstacle more than an asset. You know, I can well recall—since it was mentioned that I was chief military censor for General Eisenhower—at the beginning of Operation Overlord, in the planning stage we had thirty-two people who were cleared and knowledgeable in the development of the operation, the invasion of the continent. By the time we had reached two days before D-Day, we had something like five or six thousand people knowledgeable, in about everything except one—the exact destination. Our security problems were tremendous. The thrust of this is that if you are going to get things done, you cannot hold secrets. And the security officer will always be an obstacle in the way of a man who wants to get something done, if he holds security too tight. So you have a very real responsibility. Well, we are coming into the age of system interfaces, information system interfaces, if you will, and large scale data banks in this Federal Government, and particularly in Defense. We are in the throes of development of massive data banks. These pose real problems for security. Because of what value is a massive data bank if we can't tap it? Under what circumstances can we tap it, is the ruling that you as security people must come up with. And I question that the principles you have been applying in the manual age are adequate for what we face in the age of automation.

CARL HAMMER
Sperry Rand Corporation

Fellow panelists, ladies and gentlemen: The subject of security considerations for electronic systems is receiving increasing attention both in literature and in open forums such as this one. As the complexity of our systems grows, so does the complexity of their software management systems. While at the same time, the users of these multiprogrammed and multiprocessing machines make additional demands by introducing well known problems of an earlier era into the modern electronic environment.

Bernard Peters, in his well known presentation before the Spring Joint Computer Conference, made the point that:

"The attainment of security is largely a management problem. Management must first and foremost be aware of the real need for security safeguards and it must fully understand and support the development of objectives and criteria which it is willing to underwrite. Moreover, management must learn to understand that security cannot be attained in an absolute sense, but that every security system implies a probability of loss which can be made arbitrarily small in return for the value invested in the system."

The systems about which we are talking today are electronic systems in a new, generic sense. They combine hardware with software to achieve maximum utilization of such a capital investment and to provide maximum returns for their users. These electronic systems of today are self managing, in the sense that they have taken over numerous functions from human organizations and have translated them into their own little world of transistors and cores, drums and tapes, communications links and input-output devices. Consider the fact that the executive systems that govern the operation of these machines carry on two of the most important functions of industrial management: monitoring and control. The monitoring function observes the state of the resources, records the job queues, logs equipment utilization, and does numerous accounting functions. The control part of the executive system is the decision-making function which allocates resources in an optimum manner, assigns core space, peripheral devices, even software segments for overlays in the real time mode, or deals with priorities and resolves conflicts. The decision-making functions of tomorrow's systems will include even error-correction in a noisy environment, diagnosis of hardware that is malfunctioning and that must be taken off-line for medical treatment by electronic technicians, and advice to human users who are communicating with the system through conversational languages. We have no difficulty in observing that all these functions have their counterparts in organizational management and thus it does not come as a surprise that we begin to place increasing emphasis on the security aspects that surround these complex and resource-sharing operations.

Permit me to single out a typical problem to illustrate the point and to prepare the stage for later discussions in this panel. Unlike the computer user in the middle fifties, today's user must share "his" machine with others. The executive system will allocate to him the resources he needs to do the job. Now suppose that he has written a program he wishes to debug and to test for possible errors. Even if it were not for the security problems, one would certainly want to prevent this test program from malfunctioning in such a way that it destroys data belonging to another program; or worse yet, that it destroys or alters another program, also in operational use at the time. In the age of time-sharing, this rather classical debugging problem has re-

ceived considerable attention by many manufacturers and many users. As a result, certain protective features have been incorporated into the hardware of newer machines and the software systems have many built-in functions designed to cope with the problem. However, we know that the effectiveness of any chosen solution can only be determined under operational conditions that allow us to measure the empirical quality of the system's security. In fact, it has been recommended that the executive system itself should contain certain test programs that routinely "attack" the system, attempting to break through the security barriers, and thus allow the user to monitor the confidence levels of what we might here call dynamic security. (It is interesting to note, parenthetically, that at least one agency has indicated an interest in developing pertinent hardware and software security criteria.) This approach might tend to reduce much of the work done now in a hit or miss manner by manufacturers, although it does reflect their earnest desire to cooperate and find the right kind of requirements ultimately acceptable within the market place. We hope very much that our discussions here will provide a stimulus for concerted action in that direction so as to enhance future system designs and to endow them with the features that will be needed.

In this search for good security design criteria, we must also take into consideration the fact that electronic systems of the not too distant future will operate largely in the utility mode, almost totally unattended by humans as far as the central processor and its associated data storage devices are concerned. Thus the security of such combined hardware-software systems is amenable to rather precise analysis, very much unlike its counterpart in human organizations where the frailty of human emotions and the instability of the characters involved play a key role. This seems to be the only point where the earlier noted similarity between human and machine systems does not exist. Nevertheless, while strictly analytical methods may ultimately point the way to the determination of criteria for the security of the central computer complex, human aspects must be considered where communications, data transmissions, and remotely operated devices are concerned. We hope that the identification and distinction of these two problem areas will provide us with the clues that we are looking for in the design and development of secure systems.

In summary, we feel that the development of criteria for hardware-software systems is not only a challenging proposition but it is a *sine qua non* for the design of future systems. Therefore, it is most urgent that we come to grips with this problem, that we develop a deeper understanding of it, especially within responsible management circles, and that we chart a course of action that will provide us with the necessary guidelines for the implementation of the required system features. The longer we delay the decision to take an active stand in this matter, the

costlier will be the equipment and software modifications we must make eventually. Thus it is especially fortunate that in meetings such as this one we can discuss these matters and bring them to the attention of the real principals, namely management. Only through their understanding and with their cooperation can we hope to achieve an equitable and acceptable solution to the security problem.

JACOBUS: Thank you, Dr. Hammer. That was a real fast survey. I hope you caught the depth of thinking that is involved in what Dr. Hammer presented to you. He is talking about the world of multiprocessing, multiprogramming, all of it machine-controlled, with executive systems. This gets you into a different kind of security arena than we have had to deal with in the past. It is a very difficult one, incidentally. We have faced some problems of this nature in the Army, to which we have been unable to find very good answers as of this date, particularly in a highly secret scientific activities.

Hardware and software security criteria, and the utility mode unattended by humans—how do we work security into these aspects of our activities and still retain a capability for adequate operations? Again, I come back to the point that must be emphasized: we cannot afford, in this practical world of ours, to permit security to become too great an obstacle. We do have to produce.

Note that Dr. Hammer stressed the fact that human considerations must be brought into the picture with remote input-output devices. So you see, we are constantly being forced back to the point that we must deal not just with ideas, we must deal with personnel security, we must deal with facility security, we must deal with hardware security. Our world is not as simple as it was when Henry Wheeler Shaw was talking in the format of Josh Billings, somewhere back in the 1880s. You remember, perhaps, he pointed out that in those days a secret ceases to be a secret if it is once confided. It's like a dollar bill—once broken it's never a dollar again. This is a basic principle, but what does it mean? What does it mean in this era of automation with massive data banks with remote input-output devices that, properly operated, can enter these data banks and pull information out?

Part of the problem and a major problem involved in the use of remote input-output devices lies in the communication field.

CHARLES P. BUCKLEY
Chesapeake and Potomac Telephone Company

Ladies and gentlemen, the problems NCMS is facing are ageless, and to prove my point I will use an analogy Hank Boettinger of A.T. & T. often uses. What I am going to do is take you back to about 6000 B.C.

Don't worry, I'm going to make this very short. My thesis here is that what management has wanted from its EDP people, or its data processing people, is the same throughout the ages. There's been no change whatsoever. Maybe if you can just get this

particular thing in your mind, we might at least lay the predicate, as the lawyers say, for some of the more serious discussions to follow.

Back in Sumeria, you can imagine a man who set up some sort of a business, and was very successful. He was selling goats, wheat, grain, olive oil and all those things. One day he got more business than he really could remember, so he had a helper come in. His name was Abul. And he said, "Abul, my mind is getting burdened with all these orders, and I'm really having difficulty. Write these things down, would you? Figure something out for me." It's a source of provincial pride for me to think that the first systematic writing on this planet came from this type of operation. (In fact, Eric Hoffer, the old longshoreman authority, has said that the literary class started when unemployment hit the scribes—those accountants.)

In this particular situation, Abul came back the next day and said, "Chief, I think I have got what you want. There's a fellow down the street that's been putting together little bricks. They're made out of clay. I think I can take a few sticks here and some of these clays, and I'll get a few clay-punch operators, and we'll start writing these orders down." In fact, they started to write so many orders down that today I understand it's an embarrassment of archaeologists that so many of these things are available that they're taking up a lot of storage space.

The cuneiform approach was fine, and Abul became a very big man with his boss. His boss took more and more orders, and he had all sorts of expansion in olive oil, wheat and grain. Soon he achieved the tycoon status. He started to circulate at the local chamber of commerce out there and let Abul handle all of his business. He came back in a few weeks, and he said, "Abul, how's business?" And Abul says, "Boss, don't talk to me; I am too busy right now. If you want to know how business is, look at all those clay tablets." (There's been a parallel on this in our own era today.) Meanwhile, the boss says, "Look, all I want to know is what's going on around here. Don't tell me about the clay punches. All I want to know is what's going on." And his DP man says, "It's all there in the files, Chief. All you have to do is look it up." (You can see the theme we're getting to here.)

We're going to take a quick jump up to Egypt, and we'll describe some of the more recent problems. We're up here at the Nile River Transportation Company, and it's during the reign of Ramses II. Meantime these clay tablets have been a little cumbersome, so up here today they've put together a new approach, a real new technique. The salesmen have sold everybody on scrolls. A fellow comes in and he says, "How're you're doing?" Well, by this time all you have to do is grab your scroll and you can look at the whole operation depending on how fast you are at the scroll, and the boss says, "Look, we've got a wonderful situation here. We can look at an entire account. We have recorded here the seven lean years, the seven

fat years, made all of the comparisons. We've got projections, and we can even afford a priestly caste to take care of this sort of thing now." But certain problems developed. The boss says, "Well, how's business?" The clerk says, "Well, it's all here on the scrolls, Chief, all you have to do is just zip through and look for yourself." The boss says, "I see you're having some trouble with our Greek branch." "Yes sir," the clerk says, "those fellows up there are becoming troublesome. You know, we've taken a couple thousand years to develop this coding system we've got here, this beautiful hieroglyphics deal. Those fellows up there have the temerity to invent a new coding system that they are calling 'alphabet.' They've been sending people down here telling us that we ought to change to their system. That's no good. We've got to have transferability. We can't have all of this change. Those fellows up there don't know one glyph from another, and we're not going to change our beautiful coding system." Then the boss says, "Fine, make sure they toe the line." (There's another parallel here.)

I think we'll take another few thousand years' jump, and go to the Hanseatic League. By this time, we have got the problem of multibranches. At this point, we're getting closer to some of your classifications problems. A crowd down in London, in Lubeck, in Hanover are selling herring, beer, silver, and other things.

One of the men, the boss, says, "I just came back from a tour of the branches. You know, they have got all different kinds of forms, they're spelling items differently, they're spelling "casterling" as "sterling." We've got to have a little more order around here. Our operations need discipline." His technical man says, "Chief, I've got the answer." He says, "You know, there's a bird over in Mainz named Gutenberg who just invented a high-speed printer, and I think this is going to be the answer to our problem." So the boss says, "Great, we need him. Go over and get him. Tell him we can't do without him." So they get Gutenberg on the job, and everything is on the same forms now, the same terminology and so on, all over the world.

But the boss comes back later and says, "What are these posting errors? Everybody's got a different posting." The fellow comes back with beautiful, bound ledgers. The boss says, "All I want to know is, what's going on." The fellow says, "It's all in these ledgers, Chief."

If you ask what is management expecting of EDP today, you can expect the same question for a long time: "What's going on?" We are now a people that have converted things to cards and cards have a direct lineal relationship to the old cuneiform. But we got upset about the filing problems with cards, so we went to tape, which is a counterpart of the Egyptian scrolls—which were pretty good except when you needed something down near the rod. We are coming to the point now where real time and instant access are probably going to give us the best of all worlds. But I think we still have something of

the mentality we've just discussed—the new scheme to solve old problems. What we've learned in 8,000 years of data processing is that the human problems are still the same. The hardware really never solves our on-going problems; it solves the past ones. But the interface of humans with the use of this hardware is the real path of advance. You know, everything that you propose that does not relate to the past is, by definition, unreasonable. Reasonable men say, "How does this square with our past activities?" The *advant-garde* type says, "This problem is too big to use the old solution." The other man, the conservative, says, "This problem is too big to try things new." And the tension between the new and the old is really the rocky path of data processing in the future. Now let's talk about the future just for a moment.

Communications and the computation have much in common. The telephone system is itself a computer. Its components are dispersed across the continent but they work as one. Equipped with more than 90 million input-output stations, this enormous computer can be commanded to provide any one of three million billion answers (and that's a real mouthful) it takes to connect any one of its stations—telephones—with any other and do it in a matter of seconds. It is a "real time" operation by definition and design.

Because of the introduction of computers, our whole concept of what constitutes a telephone call has changed. Today a telephone connection can carry a stream of data, or an engineering drawing, or a TV program, or a copy of a newspaper column, or it might even carry a human voice. In short it can be set up to transmit information in almost any form, oral or graphic, transitory or permanent.

In the computer's short life span we have introduced many new developments and services to match the needs that it represents. New higher speed teletypewriter services are now widely used in providing data at speeds up to a 100 or 150 words a minute. At the other end of the scale, Telpac provides broadband channels that can be used for transmission at speeds up to 500,000 bits per second on a point-to-point basis. Data phone sets translate the language of your machine into the language of ours, permitting data transmissions wherever telephone lines run. And our new Touch-Tone telephone, in areas where this service is available, can not only connect you to a computer but it can also register information into the computer as well.

In short, we in our business are taking as a clear and present challenge what only a few years ago seemed a fantastic 21st century speculation—that is, the need to bring our switched network to the order of capability that will be required to give business and government, and the public at large, instant access to computer-stored information as conveniently as you can telephone today. Thank you.

HUGH S. DUNCAN
International Business Machines

I want to complement the discussions that have taken place. This afternoon Dr. Hammer has described modern computing systems capable of organizing and managing the demands of large numbers of users without human intervention. Mr. Buckley has pointed out that computing and communications have much in common, and that communications facilities have been and are being developed to match the capabilities of modern computers. To briefly complete the picture of equipment capabilities, I would like to point out that a wide range of terminal devices have already been developed to allow you, the user, to utilize the communications and computer facilities that have been described. These terminal devices range from simple typewriters to enter and to receive information, at one end of the spectrum, to sophisticated TV displays with keyboards and light pens for entry, alteration, and presentation of information. You, the user and manager, now have the means for almost instant access to large data files and computing capability even though the computing facilities themselves may be miles away.

As caboose of this panel, however, I want to emphasize that the train that we have just dragged by you is just the first section. The second section is going to have to be run by you. We, the panel, hope that we have convinced you, the user, that the tools for new and improved operations are here, available for your use. But this is the beginning, not the end. Let me illustrate with an apocryphal story concerning a man by the name of Pete, who is a data processing equipment maker, and a man by the name of Sam, the user.

Pete and Sam went on a safari in deepest Africa to hunt lion. They gathered a group of bearers together and started on their safari. They tramped all day without seeing a lion. That evening, they set up camp near a water hole. The next morning, bright and early, while Sam was still fast asleep in his tent, Pete, the equipment manufacturer, hopped out of bed, grabbed his rifle and went down to the water hole. Just as he was leaning down to get a drink of water, he looked across the water hole and there standing on the other side was a magnificent lion. Pete lifted his rifle and shot, but in his haste he only wounded and enraged the lion. The lion took after Pete. Pete, naturally, beat it. Pete ran as fast as he could back to the encampment, the lion gaining at every step. Just as the lion sprang at him, Pete tripped over a root and fell. The lion sailed into Sam's tent. At that point, Pete got up quickly, dusted himself, and said, "Sam, there's your lion, I'm going back for another."

The lion is yours gentlemen. However, lest you thing us as irresponsible as Pete, let me point out that Dr. Guthrie has outlined at least an initial approach for thinking through these new systems that we are dragging by you. There have been several cited examples of applications, and I am sure that more examples will be

brought out in the course of the discussion which follows. The initiative, however, must be yours. We will be responsive to your questions and your proposals. We will try to work with you. But new techniques, new procedures, and new thinking are required. The challenge and the rewards are yours.

JACOBUS: Thank you, Mr. Duncan. Let me emphasize that in the short time we have had this afternoon it has been possible to afford you only a bare glimpse into this new world of ours.

Mr. Duncan reemphasized the importance of the role of the security man and the manager. Literally, it is up to you people and your colleagues to reach a determination of how to approach these problems in their new manifestations. Samuel Butler once said, "Life is the art of drawing sufficient conclusions from insufficient premises." We know, on the panel, that we have been able to lay down insufficient premises this afternoon. We hope that we have stimulated you to do some research in depth to reach the point where you will have sufficient premises for the conclusions we know you must reach.

I would like to call your attention to two hearings of subcommittees on the Hill on the computer and the invasion of privacy: a hearing before the Subcommittee on Government Operations of the House, and hearings on computer privacy before the Subcommittee on Administrative Practice and Procedure, the Judiciary Committee, U. S. Senate. If anybody wants citations on these, Dr. Guthrie has copies here from which you can draw the citation.

At this point, let me throw the floor open for questions.

ROBERT CALVERT: What is the state of the art in using remote inquiry devices to safeguard classified information in the memory units? We have this problem ourselves. We have remote inquiry units. We have drums on which there is classified information. I would like to know what is the state of the art? Are there "lock-out" procedures, are there "code" procedures?

HAMMER: Since you answered your own question, sir, yes, there are. You see, there are lock-outs, there are lock-ins, there are coding procedures, there are crypto procedures. I have some friends here. I stacked the audience. I invited some people from some other agency here which has three letters I believe, and I won't tell you what they are, but they are not BCDs. I said in my presentation, that while these procedures and the hardware are available, they cannot offer you a hundred percent security. In fact, I side with Bernard Peters—you cannot have one hundred percent security. Unfortunately, this fact eludes most every one of my friends who come out and say, "I insist on 99.999." Now, the way it goes is, briefly, for every 9 that you ask, you have to put out a few more dollars. You have to make a management decision that says, "How much are you willing to pay for that next 9?" And I am afraid that this management decision is the one that is hardest to come by, because that is a judgment problem,

you see. There is Kenneth Arrow's theory that you cannot translate this into absolute values, that you cannot make this a straight mathematical problem. You cannot say that the next 9 is worth exactly one million dollars or fifty cents, or whatever the case may be. This is where your judgment comes in. I just came back from a five-day conference in a very pleasant place. I think it is called Oahu. I had lunch there exactly twenty-four hours ago on Waikiki Beach. A few others and myself got together there for the last three days, discussing that very same problem. And I draw to your attention the fact that this is a solvable thing, but it's only solvable within the realm that Bernard Peters laid down, within the realm of probability. But you can go to any hardware manufacturer. I have a friend here from IBM who is going to tell you the same kind of story, I am sure, or RCA, and I guess I will have to mention a few others or else I am going to get clobbered. Anyway, there is another one that is in the news very often—so I am sure all of us can give you the same answer, you know. Mine is not a sole answer I am sure. Would you like to add anything here?

DUNCAN: No, I think I agree with Dr. Hammer.

GEORGE MacCLAIN: Would you be willing to say the number of 9s that anybody so far has been willing to pay for? Up to what point of accuracy has anybody made a demand up to now?

HAMMER: If you can define the data basis on which you want me to express 9s, I will give you the 9s. I am facetious, really: you know it is a data basis problem. No, I cannot do that.

MacCLAIN: Well, I have been under the impression—well, I know nothing about ADP, I want to make that clear—but I have been under the impression that the security problem has been a completely baffling problem up to now, but if I understand what you are saying, it is solvable in terms of dollars and cents. This is a matter of great surprise to me. But I am glad to know it if—well, if I am correct in so understanding. Am I?

HAMMER: Yes, you are. I am sure my friends from the other agencies are willing to speak up wherever they might be and are willing to tell you that also.

JACOBUS: Would anyone like to speak up?

HAMMER: Would the real agency please stand up. Well, I lost all of my friends, you can see.

MacCLAIN: Well, for example, we can assume that we have a classified drum, located at a remote point. Four or five different members of a group can use that system independently and be completely identified, completely separated, and can completely bar one from the other—and up to a certain point we can approach perfection, can't we?

HAMMER: I wish you hadn't said "completely." I said I wouldn't allow you that, you see.

MacCLAIN: I tried to say—I tried to draw away from that by saying "approach perfection."

HAMMER: All right. May I say, .999, and you state the number of 9s, yes. The answer is yes, this can be done. But this may require some rather elaborate hardware and may be rather costly. And then you may just find out that you are not willing to spend that kind of money. You know, someone told me out in Oahu, yesterday, that what we ought to specify simply is that the probability of loss be less than the probability of defection. You know, this is a shocker; It's very simple.

JACOBUS: See how you mix hardware and personnel security? You just can't get away from it. Any other questions?

MacCLAIN: May I go a little further?

JACOBUS: Please do.

MacCLAIN: I am still so amazed by what I have heard. Merely because I am with the Defense Department means nothing in terms of how amazed I can be. What is today, in your opinion, if you are free to say, the most difficult security aspect of this business of ADP?

JACOBUS: While he is thinking this out, I would like to suggest that the Department of Defense come down to the operating level of the services, and you might find some answers. You'd be surprised! People have been working on these things. I don't mean that unkindly.

MacCLAIN: No, I know that. I didn't know I was that far behind.

JACOBUS: We have some operations in the Army security classified two or three levels above top secret and we do them on the electronic computer—completely security, and security bound.

MacCLAIN. I don't hesitate to assume that if you have a locked-type room, which is completely shielded all the way around, and you have completely reliable people, you can operate in and out in a completely secure situation. I think there must be one remaining most difficult problem—if you are operating at a remote point, let's say. Do you know what that is?

HAMMER: You are asking for an opinion in the matter?

MacCLAIN: Certainly.

HAMMER: If the system that you mention consists of a locked room, shielded, electronic devices, I will venture to say that people are the weakest link. I can make the electronics as safe as I want to by dollars and by 9s, but the people I just don't trust. Sorry to say so, you know. That's the weakest link. You see, none of my computers and none of my friends' computers have ever been bribed. Or have defected, for that matter. I am dead serious. That is the most difficult problem to solve. I can do a tremendous amount of mathematics, statistics, and probabilities regarding the security of these files. I can put all sorts of hardware in there, and this is a mathematical problem, as I said. But I fail to see where I can subject people to mathematical analysis. That's the weakness, and that is the reason why I feel that we have made great strides and we will make even greater ones. Within the next five or ten years we will develop more and more automatic and unattended sys-

tems. This may turn out to be just a partial answer to your question, but I really don't have a good answer for you in that sense. I cannot say what—I don't even know what is the weakest part, because it depends on how you define it.

LORRY McCONNELL: We are talking about security and what price security. How about classification, the problem of identifying bits of information according to the level of classification? And then, say—conceivably—a huge data bank with various bits of information, each flag with its bit of data—how expensive does this get and how feasible is it today?

HAMMER: That's a good question. The answer lies again in dollars and cents and the management function, because what you described there is really an overhead. You are saying that you are willing to pay for a certain amount of overhead with regard to the data classification that you are attempting inside of the hardware. Your overhead may be say, one hundred percent—that is, for every bit that you have in there they have one bit overhead. That's a hundred percent. But usually it ends up more than that, so your overhead cost in this case might be something like a thousand or ten thousand percent. And, of course, if you can't live with that then you just can't live with it. But this is again a management decision. I mentioned to the gentleman over there earlier that I can't make a decision for anyone. You have to make it yourself. I think Dr. Jacobus pointed this out earlier—there are some decisions you gentlemen have to make. How you can tell the industry—and I think Dr. Dunn brought this out—what your requirements are and we'll give you the answers to that one.

JACOBUS: Of course, in your organization it's not only a question of the bits of information, it's also a question of the manner in which these bits are manipulated, which means control of executive routine. This can be expensive, too, when it becomes complicated in a large multiprocessing, multiprogram operation.

LAWRENCE MYERS: I would like to suggest that perhaps next to the personnel question that you raise as being the most important one, the classification job itself is most important. To determine classification, you must decide what it is you want to get done. If your objective is to get 100,000 men ashore in Normandy in the first twelve hours, this is one objective. If the objective is to get them there in a position to fight and maintain themselves then you have a different measure of security—the importance of it. With the amount of information that goes into an automatic data system, you have all kinds of bits and combinations that can come out. They have varying degrees of sensitivity, but it is very, very difficult to relate these to real-life objectives, such as putting these men ashore in a position to maintain themselves and fight. When you can do that—if it can ever be done in classification—then you have a basis to decide how many 9s you want. You mentioned the system that the Army has that will maintain a very

high level of security. And yet I would hazard a guess that this is done on the basis of all information within that system being handled at the same level of security, and the sensitivity being so great that you have decided this is worthwhile, even through some of the information may be less in value. For a limited system, this is an ideal answer. But when you have a data bank that includes an immense amount of information, being used by many different people, it becomes more and more important to be able to put it out to reach specific operational objectives. It becomes more and more important to be able to put it out in lower and correct classifications, which often, for cost, have to be measured against something other than confidential, secret and top secret. The cost-worth of maintaining one piece of top secret information does not even approximate that of maintaining in secure form another piece of top secret information.

JACOBUS: Thank you. Your remarks are one hundred percent on target. We ran into precisely this problem in a recent study conducted in the Army with regard to possible consolidation of a number of our scientific research-oriented data processing installations. And one of the governing factors in truth was this very proposition of high security on a part of the activities of some of the community that vitally affect the manner in which other elements in the community would have to operate. So this can be a very practical consideration. We are running into this even now. And what you have said poses a number of the kinds of problems for the security classification manager and the operating manager, which, jointly, they must resolve before people in the ADP, hardware or software, or even ADP personnel side, can provide the kind of facilities that you need.

ROBERT BECKNER: Dr. Jacobus, I was wondering what help you may be able to be to us in the automated classification systems in paragraph marking?

JACOBUS: Well, of course, this is one of our standard approaches today. Suppose you do mark by paragraph. This is the same as marking by blocks of information in a data bank. The question is, as a security matter—as was just raised in the preceding discussion—does the one block within a data bank govern the use of the entire data bank? What rules will you follow? You see, the classification manager not only must decide how things will be classified, but doesn't he also help to decide how classified material may be used? I think we are finding that classification management is taking on somewhat a new context. It's becoming more important because it is becoming a factor that governs our capability to produce, particularly in this automated world. How can we help you? I think what you have to accept is the fact that there are technical problems in software and in hardware in the ADP field. As far as the Army is concerned, we have a group of people in our computers system directorate who are experts in this field. If you would consult them, they would be

happy to make their expertise available to you at any time. Mr. MacClain?

MacCLAIN: It seems to me that I remember that last year at the seminar a talk was made that indicated that the problem of security in ADP was a long way from being solved. Maybe the talk that was presented, and which was so complex, was done partly in a facetious way. But is it a fact that in the year that has just now passed you have made tremendous strides here?

JACOBUS: No. As a matter of fact, the electronic security has been making strides ever since and during World War II, and essentially ADP security is electronic security. The security of personnel is a problem, as you know, that we always have with us. This is why Dr. Hammer points out that the weak link in many systems lies in the persons not in the hardware or the software. What we have to make progress in are the decisions with regard to how security will be dealt with, how we will permit it to govern our approach to the use of information. Because when you come down to it, you are constantly being thrust back upon the proposition that when we talk security, particularly classification, we are really talking about ideas or some manifestation of ideas. When you are dealing with the proposition of governing ideas, this is a human proposition. Your decisions must be human decisions. We can implement whatever decisions you make in any way you want them implemented, through our hardware and software in the ADP field, as Dr. Hammer says, if you are willing to pay for those 9s.

PANEL—CLASSIFICATION IN THE DEPARTMENT OF DEFENSE TODAY

George MacClain, Director, Directorate for Classification Management, OASD (Adm.), Moderator

MacCLAIN: Good morning, ladies and gentlemen. In this panel this morning I am going to open by making a few remarks on some subjects, which will not necessarily be commented on farther by members of the panel. The most fun of any panel is in the question and answer period, and probably the greatest benefit is there, too, so please feel free, after all the speakers have been heard.

I guess it is a good thing we discovered or at least we took up the business of paragraph marking, because if we hadn't there wouldn't be any excitement in this classification management business. But we have excitement because of paragraph marking, certainly, and I am going to talk a little bit about that.

I haven't got all the answers, as you know, and neither have any of you. But I want you to know that work is really being done on it both

in the Government and in industry. Some facilities have already published and printed and distributed their internal procedures to meet this requirement. Their approach is one that we like to see. It's a "can do" approach, in which they are going to say, "Well, let's get on with it and let's do it as well as we can. Let's either do it or prove that we can't do it." This is very beneficial. We find, too, that the companies are not all doing or interpreting in the same manner. Their approach is really different, from company to company, and there is a considerable demand on the part of organizations for a layout of specific guidance from OSD. After looking at some of the things we have been getting from industry, I think that what we are getting is as good or better than anything we could lay out. Nevertheless, this doesn't obviate the need for trying to standardize an approach, and I am sure that we will try to standardize an approach on any questions there are.

You heard Joe Liebling yesterday mention some of the reasons why paragraph marking can really benefit industry even if it costs something. What benefits industry is going to benefit us, too; and vice versa.

You know, paragraph marking is really nothing but classification reduced to what may be a practical scope. You may think that you have been classifying by documents but how much specific detailed analysis have you ever given an entire document after you have decided it has something secret in it? How much additional time have you spent trying to figure out what parts are classified and what are not? I'll wager that once you determine that the document has something in it that's classified, that just about ends it for you. Or, you may say you think you can do it better by chapter, or better by page, than by paragraph. But essentially if you do a classification job you can carry it down as far as you go. The only question is, how far down is it really practicable and beneficial to go? You may think it's not true, but it is true, that one organization in the Department of Defense came to me and asked, "Have you any objections if we carry paragraph marking down to the subparagraph, and the sub-sub-subparagraph?" And I said, "No, of course we don't. It's entirely up to you." And they are doing it. Now, maybe their particular style of business is not like yours, and maybe they can do it easier than you can. But let me assure you of one thing: classification by paragraph accomplishes things that classification by document never will accomplish—it makes you decide what it is that's classified, and why, and then it identifies it for the next fellow along the line.

I know as well as you do that this is not to be done without some cost. Up to now, we've been informed in general terms, and in terms of estimates, how much the cost of this is. And then we have been informed these costs cannot be justified by what we get out of it all. Well, it's a very hard thing to prove that there's a justification afterward, and it's a very hard thing to prove that there is not.

But I ask you to consider this: if you get a document that is paragraph-marked you will immediately, will you not, be able to make the maximum unclassified use of the information in that document without any sweat? This is a great advantage for you. You don't have to treat every chapter, verse, and line as classified when you know what is classified is clearly marked for you. And consequently you in industry and you in Government who know what's not classified are in a much freer position to talk, to discuss, and to work with the information before you. You can't put a price on that, and you can't prove it's worth so many dollars and cents or it isn't. But it is a tremendous advantage. It is to me. It is to the people I work with. If we get a document that is not paragraph-marked, we feel deprived of something. I wish that all of you were getting documents that are paragraph-marked so that you, too, would have the opportunity to see that it is worth what it costs.

Any of you who have conducted studies of more than an estimation type who think you can prove what it costs to paragraph-mark as against any other system you can name, we will be glad to receive your information. But let me point out one thing: it is pretty hard to find a basis for comparing paragraph marking costs unless by now you are already following the procedure of marking every page according to specific content of that page. There is not much difference between a page and a paragraph. Nobody has ever really griped about the page-by-page requirement—and yet it's only a few lines more than a paragraph. It is just that when you were finally told that it was by the paragraph that the real problem became highlighted. It is certainly not fair to say that the cost of paragraph marking is prohibitive when you say first only that "this document is secret because we know that there is secret information in it somewhere," and compare that with specifying which paragraph contains classified information. That is a comparison of nothing with something. Any cost that you measure on that kind of a scale is likely to be characterized as excessive. I would like to say that as far as I am concerned, I do not believe that the quality of the software is improved, particularly, by paragraph marking. You'll do just as good a job for your customer whether you mark by paragraph or not, as far as the product he is buying is concerned. And so I am not trying to prove that paragraph marking makes a better or worse product. I don't think that it does. But on the other hand, I know this: if you will take the time, as you should when you are dealing with classified information, to identify what is classified and what is not, the payoff in terms of really avoiding unnecessary classification will help you, your company, and your people. And it will help everybody else who gets that document from that time on.

We want to give it a real fair shake. It has been used in Government long before we put it on the books—though hit or miss sometimes.

We want to give it a real fair shake now.

The announcement that was made in the Industrial Security letter not too long ago that Joe mentioned in his talk yesterday is, in general, that the requirement did become effective July 1, 1967. No doubt about that. But nobody is going to be cited for not observing the requirement between now and next January unless he is indeed doing absolutely nothing about it now. If he is sitting around hoping that on January 1, 1968, the whole thing will be forgotten, so he doesn't need to spend any time and effort in the meantime, this is really a mistake. Because the DCAS people are going to cite you in industry or in any other place that they can for not making an honest effort now to get ready to roll by January 1. Fortunately, some of you are ready to roll and you are rolling already.

Well, the panel is not going to discuss paragraph marking. After the panel has finished and the questions on their subject matter have been dealt with, if you want to discuss paragraph marking, we can.

I would like to mention something else to you that has come up from time to time, and that is the DD Form 254. It is now really finished. I don't mean by that it's dead. I always wonder when I write a note to somebody, "send it back when you are finished" whether they get the real message I intend. Form 254 has been staffed two or three times around the Department as well as exposed to industry organizations, and it is now in the form in which we recommend it be adopted by the Assistant Secretary for Administration. Along with the form are a large number of instructions which, if adopted by the Assistant Secretary, will be published through the Industrial Security system. You will get it through the ISM.

We have made a few interesting changes. First of all, the new 254 is a two-sided document. And there is an additional document we call a 254c, which you may or may not need to use. The 254 and the 254c or any substitute for the 254c has to include a combination of a list of items by some kind of name or index, together with narrative topical guidance on each of those items. And the way the form is drawn up, if you don't have too much to say you can put it on the back side in Item 13—Item and Narrative Guidance. If that isn't enough room, you can use the 254c. There's a preprinted list of items. It is a list that serves many kinds of different cases. On the left side there is a place to list an item and on the right side there's a place for narrative guidance. And if you don't happen to like that, you can create any form of similar guidance you wish. The Air Force has a method of giving classification guidance in which they tell you what they are going to talk about, and they talk about it. That can be used in lieu of a 254c but it must be referred to in the 254c.

Another important change, and we think it's very important, has to do with the review by the user agency of the 254. The responsibility for review of the information in the 254 has

been separated, in substance, into two parts.

If you are doing business with, let us say, the Navy as the user agency, they provide the content of the 254. In the course of your performance of the contract you may obtain information from the Defense Documentation Center or some information analysis center, and you do this on the authority of the Navy, of course; but the information you get this way, the DDC information, may not be under the classification jurisdiction of the Navy, either now or at any other time. We call this material for which your user agency has no classification responsibility "reference material." Our pitch is that at no time, from the beginning or at any other time, is the user agency of a particular contract responsible as such for any of the classification of that reference material. Accordingly, if at the end of a contract, or if during the contract, there is a review of the 254, as there will be periodically, the user agency has the obligation to review the classification guidance for all of the information for which the user agency has classification responsibility. And I think you know what that means. But they have no responsibility to review, and indeed they will not review the classification of this reference material, even though you have it. Not only is this true during the course of the contract but it's true at the end of the contract as well. If this isn't clear, I want you to ask me about it later.

At the end of the contract, when you make your request, if you do, for retention of classified material, you will have to justify what you want to retain on a need-to-know basis. You are not unfamiliar with that. And at that time you have to demonstrate your need-to-know for the reference material as well as for the other material. Now, some time afterward when you still have reference material on your hands and it is still classified just the way it was when you got it, you may begin to think, "Well, what about this? I don't think this should be classified any longer." You cannot go back to the user agency directly and say, "Review it for me for classification." They are not supposed to have to do that from now on.

The rule is that the originator of that material is the one who still has the responsibility for it. Of course it may contain downgrading markings and you will take your guidance from that. And to the extent that it doesn't contain within itself the appropriate evaluation for downgrading and declassification, your job is to identify the originator. Now, I don't know how well you can do this. You look at the document; if you can't tell who the originator is, you are in trouble, of course. And the best that we can do, and what we are going to say is, if you need help in identifying the originator, in the following order you will ask for it. You go first of all to the place where you got it, the DDC, for example. The DDC will not evaluate it but they will say where it came from, thereby identifying the probable source of classification responsibility. If that doesn't work, then the

next person you go to is the last user agency with whom you did business. Maybe they can help you identify the originator. If they can't do it either, then you come to our office. And our job will be to help you identify the responsible classifying authority. If at this time nobody knows, I am sure that our office can find a way to do something about it. Now, that is a long way of saying that the review of classified material on a periodic basis will continue with the 254, but be limited to the user agency responsibility. And after the contract is over, there will be a review for need-to-know and this will come up periodically. During the need-to-know or retention period, the user agency will still review the material he has classification responsibility for.

There is something that we need to get from all of you within Government and not in Government, and that is some data on costs, particularly cost savings. There has been something in the paper recently that the Secretary of Defense has been claiming some cost reduction benefits that are really cost avoidance, and that some of them are a little more remote than that. I have heard two expressions of views on this. One is that cost avoidance savings could no longer be claimed in the cost reduction savings of or for the Department. I don't know if this is really true. Another way I have heard it said is that if the Department lays on a particular requirement, like paragraph marking, for example, which is new and is going to cost something, and then it suddenly changes its mind and says we are not going to do it, we then claim lots of savings. This isn't legitimate. The only thing that we can do to really claim cost avoidance savings is in a change in policy that's been established, that has been on the books, that we are going to get rid of now because we think the policy should be changed. And if that policy had incidental costs, we'll claim those savings. Of course we will. Make no mistake about this: to the extent that classification guidance and paragraph marking enable you to accomplish savings in the course of what you do, this is real hard stuff and we want it. And you know you can get it. You are going to hear from this panel that thousands and even millions of dollars have been saved because of classification management procedures that will enable you to do your contract work on the least cost basis, because you treat unclassified what you are entitled to treat unclassified, and you do not unnecessarily go out and buy an unclassified item classified simply because it's going into a classified end item. This kind of hard savings information we want, and I know that some of you have it. Some of you have been able to realize $75,000 on a particular effort and you know you have realized it, and if you are willing to put it on paper and send it to us, we want it. As a matter of fact, we will be coming out and asking for it some of these days, both within the Government and outside. So send it in without being asked if you have it.

We know that we have reached a

point also in classification management where we ought to go out and make certain that what we think is good classification management philosophy is being used effectively or ineffectively or is either wrong or right. What I am trying to say is, we had better look and see what we are doing now that we've said what ought to be done. So we are going to try to do two things as we look ahead. One is that we are going to try to get out and tell you more directly, more frequently, and at more places, what it is we want you to do, the kind of guidance we want you to get, the kind of things we expect. And then we are going to try to find out, too, by more field operations, what is going on. We know that from now on real classification management, that is sound fundamentally, is a question of communication and application, education, and indoctrination.

Some of you have already received your latest copy of the *Journal*. It contains an article by Art Van Cook. Art is in our office, and his field is Special Responsibilities—Downgrading and Declassification. Of course he is kept busy doing a lot of other things as well, but that is his primary responsibility. In the course of it, he has done a lot of thinking about whether the present downgrading and declassification system, especially the automatic one, is a good one or not, and he has reached certain conclusions that are laid out, at length, in the latest issue of the *Journal* and I encourage you very much to read this.

As a matter of fact, although it's an unofficial presentation and although it doesn't on its face carry the endorsement of our office, it certainly carried the endorsement of our thinking because we happen to believe that what he has come up with in the form of recommendations and conclusions has got to be exposed to others for comment. It seems to us that it's basically sound and right. And the automatic system, if he is right, will change its character in the future. Of course the automatic system was laid on the Government by Executive Order, and this means, of course, that we are going to have to staff it through the Executive departments to get some concurrence before it could ever be changed. Essentially, the changes would drop two of the four groups. It would change the phasing for automatic downgrading and declassification so that, at least as far as the automatic downgrading phase is concerned, it would work on a faster scale. Instead of being twelve year minimum it would be something short of that. For example, the top secret would last, I think it is, only two years and then go down to Secret. Secret would last two years, and then be Confidential—and so forth. Now, this is not DoD policy. This is not DoD-recommended policy outside our own immediate office. But we are ready to recommend it. And so I do encourage you to read it and get familiar with it because maybe you will like it. I think you might.

Well, I think that is about it, as far as what we are doing is concerned, in a general way. The panel has representatives from the Army, Navy,

and Air Force, and DCAS, and they are going to speak in that order.

M. D. AITKEN
Department of the Army

The Army presentation will be in three segments. First, I will discuss the Army organization for classification management and describe the materiel cycle in the Army. Next, I will discuss a case study of one method of achieving significant cost reductions and cost avoidance through intensive application of classification management and records management principles. And finally, I will present a brief appeal for innovation and imagination in seeking new and better management techniques and methods in handling and processing classified information.

The Department of the Army has established classification management as a function of command. Certain responsibilities for classification management have been assigned to Army commanders and implementation of DoD Directives and Executive Orders. These responsibilities, broadly stated, are oriented toward the continuing review requirements, preparation of classification guides, and the delegation of original classification authority. Within this guidance major Army commanders have developed classification management programs directed toward the missions of their particular commands. Consequently the scope and effort of this program in each command varies considerably.

As a principal Army procuring command, the Army Materiel Command places most of the classified contracts in the Army's multibillion dollar procurement program. Therefore, AMC is primarily concerned with most of the classification guidance issued to industry on these contracts. The classification program —the classification management program in this command—therefore, is perhaps the most comprehensive. So let's examine, briefly, the structure of AMC and see how classification management operates, Within the AMC unlike the Air Force Systems Command and the Air Force Logistics Command arrangement, which you will hear about shortly, the mission is all-encompassing for Army hardware—the so-called cradle to grave concept. That is, AMC is responsible for research, development, testing, evaluation, production, storage, maintenance and issue of Army materiel, from conception to obsolescence. This is not completely accurate, in that the Army Combat Development Command is responsible for Army doctrine and originates many of the Army requirements, and at the other end of the spectrum the Defense Supply Agency is primarily responsible for disposal. But for the most part, AMC is responsible for the life cycle of Army materiel.

Tracing the cycle through AMC, we start first with the several AMC central laboratories at which basic and applied research is conducted in various fields in support of Army requirements. Materiel development and developmental testing are conducted in one of the several AMC major subordinate commands, which are commodity-oriented, such as the Army

Missile Command, the Army Munitions Command, and so forth. Engineering and service testing for materiel reliability is conducted at the Army Test and Evaluation Command, another AMC subordinate command. Procurement and production of the materiel cycle is managed by the Commodity Commands of AMC and nearly 100 smaller procurement activities throughout the command.

As the item moves off the production line—and this production line may be in-house at one of the producing arsenals or it may be on contract--it moves into the AMC supply, maintenance and distribution system, which is controlled by AMC national inventory control points throughout the country. Finally, as the item approaches obsolescence or it is deployed, and ultimately becomes unserviceable, it is returned to the depot for disposal.

Classified material moving through this cycle passes through a pipeline which is insulated to a greater or lesser degree by the classification. The diameter of the pipeline varies inversely with the increasing classification; that is, the higher the classification the more constricted the pipeline becomes—the slower the item moves and the more it costs.

The job of the classification manager in AMC, then, is to keep the material moving through the cycle as rapidly and as economically as possible by reducing or eliminating classification requirements whenever possible and as soon as possible, thus expanding the diameter of the pipeline.

Every employee in AMC is personally charged with the task of seeking means to accomplish the AMC mission better, cheaper and faster. And the classification manager has the opportunity to contribute significantly to this objective. A point to note here is that throughout the life cycle of the Army classified hardware, with few exceptions, the classification through deployment or obsolenscence is controlled within a single Army command. While extensive coordination is usually required to change a classification within the Army, and sometimes with the other services, the classification management chain of responsibility is unbroken from cradle to grave. This permits closer surveillance of information classification, permits fixing of specific responsibilities for various functional aspects of the program, permits application of uniform policies and procedures, and provides the means for enforcing the requirements of the program through command channels.

Each of the nearly 200 subordinate commands, installations and activities within AMC is required to designate a classification management officer with specifically delineated responsibilities. These responsibilities include participation in development and review of in-house classification guidance, review of classification guidance issued in classified contracts, and the review of classified document holdings and other program functions.

Through the technique of decentralization it is possible to maintain simultaneous and continuous classi-

fication management surveillance of thousands of major classified item systems and components in the AMC inventory.

The effectivenes of the program is evaluated by annual Inspector General inquiries, security staff visits, and spot-check and sampling systems.

No discussion of the materiel cycle would be complete without a reference to the almost overwhelming accumulation of classified paper which is generated in support of classified hardware. Solutions to the problem created by the staggering load of scientific and technical information are being sought by many agencies and study groups. In this connection, we might borrow a classic understatement from the missile people to describe this problem. It is termed "an unscheduled pressure rise." Missile people use this phrase to describe the event when one of the birds blows up on the pad. We might use it to describe a fantastic paper explosion, which we heard quite a bit about yesterday.

About a year ago, recognizing that we had a problem in this area, we also recognized that strenuous efforts were required to cope with it. It was apparent from spot inquiries conducted to try to define the problem that normal administrative controls and continuous review requirements couldn't keep up with the birth rate and input. A massive all-out effort was needed to reduce the inventory of classified documents. So in August of last year a one-time review requirement was imposed on all echelons of the command, which directed commanders to physically review their inventories of classified documents with a view toward elimination of all material not essential to mission performance.

One hundred percent review of all top secret and secret documents was required, and a healthy sampling of confidential material, to determine what documents could and should be destroyed, retired, returned to the originator, downgraded or declassified. Reporting requirements were built into the one-time review to permit evaluation of results, analysis of trends, measurement of costs and the tabulation of other related data. Results of this comprehensive effort were more than gratifying in terms of accomplishment. But the reports received also confirmed our concern that we did indeed have a problem. Now, I will give you some of the accomplishments first and then I will define our continuing problem and how we propose to cope with it.

First, we were able to eliminate more than twenty-five percent of the top secret documents from our inventory by destruction, down-grading, or retirement. This was sort of a bonus because earlier in the year, six or eight months prior to this review, we went through a DoD-directed review of all our top secret material and eliminated a substantial number of our top secret documents during that review.

Twelve percent of all secret documents were eliminated, a total of 184,000 documents. About three percent of all confidential documents

were purged from the files, a total of 307,000.

Here is one way of looking at this accomplishment: the nearly 500,000 documents that were eliminated from the inventory represent more than 8,000 linear feet of classified container storage space, or about 1,000 classified containers, which cost about on the average somewhere in the neighborhood of $400 each. Therefore, in theory at least, AMC can reduce their capital equipment inventory by about $400,000. But as we all know, there are many other direct and indirect costs associated with the processing and storage of classified documents, which vary with the classification involved.

We considered the Lockheed study conducted several years ago on the cost of protecting classified information in one of their facilities and decided to run a parallel study to determine handling and storage costs for a typical AMC installation. The purpose of this study was partly to prove to ourselves and to AMC Commanders in the field that the one-time review requirement was worth the effort, rather than to demonstrate savings or cost avoidance. Further, it was hoped that we would be able to get a better fix on our problem and to identify classified document handling costs command-wide.

The management office at Picatinny Arsenal conducted such a study for us late in 1966, measuring all identifiable direct and indirect costs associated with the handling and storage of top secret, secret, and confidential documents above those attributed to handling and storage of unclassified documents. The study was conducted by qualified methods and time measurement practioners, and was based on an average flow of 60,000 documents per year and 500,000 documents on hand. A recap of the results of the study follow:

For top secret, direct annual cost per document: $5.16; indirect cost: $1.40; total cost for maintaining one top secret document for one year: $6.56.

For secret, direct annual cost per document: $4.69; indirect cost: $1.40; total cost for maintaining one secret document for one year. $6.09.

For confidential, direct annual cost per document: $2.11; indirect costs were determined to be insignificant and were not measured. Total cost for maintaining one confidential document for one year: $2.11.

Those familiar with the Lockheed study will note that these cost figures are quite compatible with that earlier report. In fact, one or two of them are identical.

Theoretical savings achieved by the AMC one-time review were—for top secret: $6,748; for secret: $1,121,589; for confidential: $648,012; total gross savings: $1,776,345.

The cost of conducting this review, based on the number of man hours expended, multiplied by the average salary of the reviewing officials, was $201,262.

Therefore, the theoretical net savings works out to $1,575,083.

Now, none of us is no naive as to claim actual savings in this amount. As far as I know, no one in AMC

lost his job because he no longer had classified documents to process or safeguard. There were no massive reductions in security controls because of the elimination of material to safeguard.

We *can* claim numerous intangible savings and benefits resulting from this comprehensive review program. First, we have eliminated the exposure of nearly a half million documents to loss or compromise. Next, the time spent each year on reviewing, inventorying, processing, and handling nearly a half million classified documents can be profitably diverted to requirements more closely related to our mission. The need for acquisition of about $400,000 worth of classified containers has been deferred, because we have about 8,000 feet of linear classified storage space we didn't have before.

But perhaps most important, we have been able to demonstrate to our field commanders that with very little effort much can be accomplished in this very narrow area of the total classification management program. In this connection, we recognize that we are treating a symptom of the problem rather than trying to find a cure for it. Nevertheless, if we can find a way to hold our own in this struggle while we are searching for the cure, we are not going to be buried in paper before we find it.

To insure that we don't fall behind, AMC has now established requirements for an annual comprehensive review similar to the one-time project, which will force elimination of unnecessary classified material and at the same time permit us to keep our handle on the problem and identify trouble areas.

To give you a brief idea of the problem we are still faced with, despite the comprehensive effort of last fall, here is what the AMC inventory looked like after the one-time review: 2,830 top secret, 1,355,684 secret, and 9,627,317 confidential documents—a total of 10,985,831 documents remaining in the inventory.

Before I leave this subject, I would like to throw out a couple of interesting figures produced during last fall's review: By an actual physical count in measurement of more than 60,000 documents, we came up with a figure for the number of classified documents per linear foot. The figure is sixty. The documents counted and measured were both secret and confidential and represented a broad variety of types of documents from bulky test reports studies to single sheets. We attach no accuracy guarantee to this figure, but it may be useful to you at some time when you are trying to determine the size of your inventory, particularly when you are talking about confidential documents.

Using the figure of sixty classified documents per linear foot, we came up with another interesting statistic. This is sort of a file-and-forget item. The newspapers have mentioned on a number of occasions that the Federal interstate highway program averages out at a million dollars a mile. Well, I am pleased to report that AMC can undercut that cost on an

annual basis. AMC has approximately 33 miles of classified documents in their inventory and it only costs us 28.5 million dollars a year to protect them! So when you hear your boss talking about getting more mileage out of your program, that's what he's talking about.

Earlier I said that I would close this presentation with a brief plea for innovation and imagination in seeking new and better classification management techniques. By this I mean that classification management, as an art, is in desperate need of new and imaginative approaches to our common problems and we need people who are not afraid to try new approaches and to keep trying despite an occasional failure.

We should try to find more effective ways to provide the original classifier with all available scientific and technical information and foreign intelligence so that he can make enlightened decisions, so that classification is assigned intelligently and not by intuition. We should try to find a means to reach top management, both in industry and Government, to educate and motivate officials at the highest levels in the principles and goals of classification management. A massive orientation and education program at that level is urgently needed in order to gain support for this program. We should try to broaden our base of professional talent. Establishment of a classification management career program in the Government would be one approach. And, with the utmost respect for middle-age membership, we should try to initiate and sponsor an intern or trainee program in classification management for recent college graduates. Above all, we need to keep trying, to keep moving to maintain the momentum we have gathered over the past several years. We can't let an occasional setback discourage us or even slow us down. Thank you.

DANIEL F. RANKIN
Department of the Navy

In June 1964 the Department of the Navy officially established its classification management program. This program in the Navy was implemented in Chapter IV of the Navy Security Manual.

At the present time, every command in the Navy is required to establish and maintain an active classification management program. I might say that at the outset it was apparent to me, and it was apparent to many people in the Navy, that the real problem in classification seemed to lie in the fact that there was no centralization of responsibility for classification, regrading, or declassification. I am not saying that you couldn't find someone in the Navy who would give you a classification decision. But, unfortunately, if you'd go into a command you'd have to get around and find the individual who classified the document if you wanted it declassified. So the real problem, then, was to try to set up some sort of centralization of classification responsibility. To resolve this problem we recommended that in the absence of any specified designee by the commanding officer, the classified material control officer

within the command would have this responsibility. He's called upon to establish and maintain a program for the commanding officer. So if anyone is dealing with a Navy command, he can go to the classified material control officer and get classification decisions.

I think it might be well to touch just briefly on some of the duties of the classified material control officer. First of all, he should coordinate the preparation of the classification guides. He should participate in any advance security planning. He has a big role in trying to educate everyone in the command in classification principles and problems. In general, he is going to be acting as a consultant in classification matters. So he should, then, direct and monitor a vigorous classification program. To this point, I have referred to the Navy in general. I think it might be well for this group if we sort of branched off into the Navy Material Command because this is where I think the dollars can be saved.

Before going into this, though, I think all of us should understand the organizational structure, the chain of command in the Navy. As you all know, the Secretary of the Navy is the number one man. There is some confusion about the second, the Chief of Naval Operations. Unfortunately, too many people believe that the Chief of Naval Operations is one office. It consists of many offices. They have various OPs who have different areas of responsibility and these people speak for the Chief of Naval Operations. Now within the Chief of Naval Operations, the Director of Naval Intelligence has been called upon to have the responsibility for the classification management program Navy-wide. So then we have the Secretary of the Navy, CNO, and the next coming down the chain is the Chief of Navy Material. And finally, the six systems commands.

Because of the complexities involved, a more elaborate system of classification system had to be established within the Navy Material Command. I think that most of you know that the Chief of Naval Operations are various OPs with CNO, levying certain task assignments upon CNM and the systems commands. Unfortunately some of these cross the chain of command. And when this happens, it was apparent to us that we needed a classification office within the Chief of Navy Material to monitor the various systems commands. So CNM is responsible for the six systems commands, the twelve project manager codes, and twelve laboratories. You can see that the Chief of Navy Material has a gigantic task. I think at this point they have done a remarkable job since June '66 when they established their program.

There are two basic concepts they have recognized that I think are vital to any good classification program. Number one, they recognize that classification is primarily a security function, and that it has its place in the security organization. Two, they have emphasized the necessity for vesting final authority in all classification matters in the classification manager himself, within that command.

So in a sense, the classification manager in a systems command is the same as the classified material control officer in any other Navy command. In addition, the classification manager is responsible for public affairs and information programs, for the review of press releases, foreign disclosures, etc. You might ask, "Why am I telling you all this?" It is my belief that anyone dealing with the Navy in classification matters should understand some of the problems, should have an appreciation of the organizational structure and should know where to go to get the answers in classification decisions.

Now, I have briefly skimmed over the Navy's classification management program, but before I leave there is one point I certainly would like to stress: the Department of the Navy, whenever possible, has encouraged the contractor to participate in the preparation of the 254 either before or during the contract. I know in many cases it is most difficult for the contractor to participate before the contract, or before the final contract is let. However, whenever possible the Department of the Navy encourages this participation. As a matter of fact, one of the systems commands has, as George MacClain pointed out, conducted a pilot program whereby they have contacted about 10 of their major contractors. They have taken the 254 with the contract, they have broken it down in as many components as possible. And I understand they were successful in determining 90% of the components could be treated as unclassified. This of course results in a cost avoidance both in production and in shipping. I understand that one of the contractors saved as much as $471,000. There is one point I am not sure whether I should go into but I intend to—perhaps the contractor, in general, is a little reluctant to admit to the Government that as a result of good classification he has saved some money. I think he is afraid that if he indicates this there might be some desire on the part of some people to renegotiate the contract. I think this team concept of the contractor and of the classification manager within the systems commands is something that's going to benefit both the Government and the contractor. So, it behooves both of them to try to get together and to identify that information that requires protection and handle the other as unclassified.

Another problem that was called to my attention concerns off-the-shelf items in connection with classified end items. Normally there is no problem if you have a classified end item and you procure the off-the-shelf item not identified with the end item. It's no problem. In this one case in point there was a very serious problem, because the off-the-shelf item when it was identified, not with the end item but with the contractor. I am afraid compromised the weapon system. The contractor conducted a study for the Navy, and he determined that it would cost about 2.4 million dollars to protect the information the way the Navy wanted it protected. There was a recommended solution. This particular solution was

to let the Navy Supply Depot purchase some of these items and the contractor could purchase it from the supply center. In this particular case the contractor only produced this one end item. So when they took the off-the-shelf item, using a simple formula they could actually predict the effect in this particular weapon system. Because this decision is still pending in the Navy, I would prefer not to go into it any further. The point that I would like to make here is that I think care should be exercised any time you are purchasing off-the-shelf items to insure that these items are no way identified with the end item.

In conclusion, I would like to state that I think the Department of the Navy has established the necessary machinery to have an effective classification program. I think the only thing remaining is to educate both the people in the Navy and those outside the Navy as to what is available. We have here Commander Poenicke, who is the classification man in the Navy Material Command, and I think everyone here should perhaps take a look at him. If you have any problems that cross over the systems command lines here would be a good man to contact—Commander Poenicke.

ROBERT C. ARNOLD
Department of the Air Force

Actually, I am not sure that my presence here today isn't classified. You see, Dick Durham had to go to Europe, so he had to be relieved from the International panel. And so Frank May took his panel, and that left this position open, so I am here. And that describes a chain reaction. In accordance with some of the interpretations of certain legislation we are getting these days, you are not sure whether the words "chain reaction" would be classified or not.

Truthfully, though, it is a real privilege to try to give you a picture of the role of the team concept during the various phases of the contract negotiations, administration, and so forth, as we see it up here.

Through the efforts of Leo Hodges and his people out at AFSC we have been able to sell the SPO people on developing as definite guidance as possible at the time that the proposed system package plan is developed, beginning the life cycle of the complex system. We recognize that this guidance is not very detailed, but this is developed as a result of an advanced development objective or as a specific operational requirement that is handed down. Once the package is approved, then, of course, we are on our way and proceed toward the contract negotiation phase. During the development of the guidance here, industry, as much as we would like to have them on the team of developing the guidance, is not really a part of the team. We are speaking now only of the development of guidance on the military side of the house—the use of the scientific technical man; the use of the security man who understands the problems that will be confronted in building the system; the use of the intelligence people.

Mr. Liebling talked about the im-

portance of foreign technology, the importance of intelligence input to any classification decision. We recognize very definitely that we must develop procedures for bringing into the decision intelligence, both domestic and foreign. Because if we don't consider this, we will either underclassify or over-classify. We hope that by the time contract negotiations are in order we have fairly well detailed guidance. We know that it will have to be further broken down as the system develops. At the time of contract negotiations we feel there's another part of the team that comes into play. We were very happy you know, to see DCAS support our team concept, which we had been throwing around for some three years, in their newsletter this spring, because it points out that the team can function in industry separately and distinctly from the military classification management team. At the time they are working with their contracting people, we would like to see the contractor and his staff actually consider the security involved and determine exactly when this end item that we have said is secret actually becomes secret.

We may find out that it does not become secret until the last circuit board is installed, something along these lines. We may find out that it doesn't become secret or doesn't reveal the information that causes it to be secret until it is almost through the assembly line. The result: your contract bid is certainly cut down, because you don't have to apply the protection.

Now, there have been a lot of people who have approached me with the idea, "Why can't the contractor come and work with the military side of the house at the time that he's working up his bid?" For instance, Contractor A says, "I don't believe this should be secret. Let's see if we can't get it down to confidential."

It sounds real good, but there's one problem, and that is the time available to get that changed guidance back out to all the contractors that are bidding. "Well, you don't have to tell the rest of them. Just let me know."

Well, you immediately see the reduction in security cost because of the downgrading. It's a problem. There may be something there where we can get the interested contractors together and take the basic guidance and work from there. But at least there is a role for industry at the time that the negotiations are in order. We would like to see the time when negotiations really include the classification management officer from the military as well as from the industry, sit-in on the negotiations. This is an important factor. It will save money. It will cut the cost of contracting. I think the time is gone now when we issue a secret contract where the end item is secret and we protect everything secret right across the board. We have to face this. This is costing us a tremendous amount of money. I should say it has cost us; it does not cost us so much any more. We need to break it down, just as various contractors are doing out at the systems or sub-systems they are

working on, on some of our complex systems.

Now the contract is let. We really get the team into play, because you have the scientific, the technical, the engineer, the security man, on the side of the contractor working with the technical intelligence and so forth on the side of military, through the classification management people. This is an important area to establish a focal point where changes go through.

Now, it is going to take time. It is going to take a lot of time where we don't have changes in classification going from the contracting officer on our side to the contracting representative on the part of the contractor himself. We have had examples where this has really hurt us—where the guidance going to the contractor was not approved. It demands coordination. During Mr. Moss's talk, and during Mr. Liebling's talk, there was, if not direct, indirect comment made on the necessity of valid decisions—valid classification decisions. Mr. Moss certainly pointed out that we would only suffer if we were abusing the assignment of classification. Probably more important than suffering, probably more important than not releasing information to the public, is the fact that when we overclassify, in the eyes of the technical man working on either the military side or the contractor's side, we destroy the integrity of the entire security information program. They put tongue in cheek and say, "Yes, we'll honor this." And this is the thing we have to destroy. This is a real challenge. It can be done through not just talking about the team concept, but putting it into being from the time we get an idea, all the way through. We need contractors' help after negotiations, because working together we can make the proper changes.

Now, I would like to mention just a little bit about the difference in the functioning of AFSC verus AFLC. By the time the system is under contract the classification is pretty much up to the top. We do have some retroactive classifications occasionally. We do have some upgrading because of changes. But generally speaking, by the time we are going along building the system, the classification is about as high as it's ever going to be. There is not too much downgrading or declassification while AFSC has it. Some time after acquisition, the responsibility for that system is transferred to the logistics command. As a result, some people, many contractors, many of our people have got the idea that AFLC is only interested in declassification. That's not true. It just so happens that the team they are working with inherits something that is already pretty well classified. And their problem is to determine how long that classification must stand. Now, unfortunately, when they need some information as to why something was classified the AFSC activity that classified it is many times out of existence and disbanded and no one knows why the thing was classified. So AFLC inherits a bucket of worms. Accordingly, we are trying to insist that when guidances develop

for these systems, the systems support manager at log command will sit in, or his representative will sit in with the development of the guidance. We also like to see the user—the conventional user, operational type—at these meetings to bring his requirements to protect the capability. This is because if we weren't concerned about protecting the capability we would really not have any reason to classify. We must protect our capability. So, one of the people that has been left out of making the classification decisions and the declassification decisions has been the eventual user. I am talking about SAC, TAC, and so forth. These people play an important part and our classification management representatives at these activities must work closely with the people that are setting up the detailed guidance.

We have been talking a lot this morning about savings of money. I must, merely as a matter of defense, I guess, point out that there has been some savings, some real savings. A couple of years ago we looked at the electronic equipment that we had in being. It just so happened that at that time I ran across the fact that the AN/APQ-13 still had a confidential classification assigned to it. This is an old radar set that we used in World War II on the B-29. It just hadn't been given any attention. We didn't have many; it wasn't a big item. But we looked at some 7000 pieces of electronic equipment that were classified in the Air Force, ranging from ECM equipment down through the various simple radar sets. As a result of that review, with the help—and this is certainly a team approach—with the help of headquarters people, the logistic and system command people, the operational people, and the engineers and technical people, in a period of about a year we actually removed the classification from 2100 pieces of equipment—about one-third.

Now this looked real good. How much money was saved? It's impossible to compute. You'd have to know exactly where they were being stored, exactly how many were shipped, and so forth. It would cost us more to determine this—well, we saved, we saved. And as a result of this, we now had a lot of unclassified equipment. We realized that when you think of equipment there is another item that you have to think of—technical orders. Here we had unclassified equipment, and when we looked at the technical orders we found that we were carrying the related TOs as classified. We looked at TOs and we identified 427 that were classified higher than the equipment to which they pertained. Now, I am not saying at all that there aren't certain technical orders such as operational instructions and so forth that shouldn't be classified higher; but there are many that reveal exactly the same information as the hardware and there is no reason for not downgrading those with the equipment. We have declassified, just recently, 168 of those; 259 are being reviewed at the present time, and will undoubtedly be declassified. Using the figures that these gentlemen

have presented today, and also you can play with RAND figures or any other studies, we find a savings of somewhere around a million and a half dollars a year on just technical orders.

I think that the contractors that prepare technical orders certainly have a little responsibility to help us out along these lines. We are prone to not consider everything about a given piece of hardware at the same time. In other words, what I am saying is that the information that the hardware reveals must have the same classification whether it's revealed in a document, a technical order, a parts catalogue, or where it is, and we must give our attention to all of these items.

I would like to point out just one other item that is quite interesting. By living with the written word—the Atomic Energy Act—the Director of Special Weapons was forced a couple of years ago to implement some policies. In a period of three and one-half to four months, they used up the 9,000 hours of overtime that had been alloted to them for the year to meet these new requirements and handle the paperwork. In accordance with this work that was being done, they had to come forward to this headquarters with a request for fifty-five additional man-spaces, and 152 pieces of equipment to store this pile of classified material that was being built up at a tremendously rapid rate. By working with these people, changing some procedures, we were able to eliminate this requirement and eliminate the requirement for overtime.

In other words, no matter what phase we are working in, whether there be hardware, manpower, or what have you, by working together we can save money. We can reduce the price of contracts, we can reduce the price of manpower, we can reduce the actual monetary outlay. But one of the things that we have been faced with over a vast period of time has been proving this. I think we all have a tremendous responsibility, and that responsibility is that we must sell our bosses on the idea that good management, no matter whether it is administrative management, manpower management, or security classification management, is effective and will produce a better product and will save money. Until we get to that point, which is a matter of education, we must keep throwing these cost statistics at people. The role of the team is important. The captain of the team must be the Classification Management Officer. He has got to have the initiative and the desire to do a great job. I think when we talk about the desire to do a great job, I have to steal a page from the life of a man that all of us know, and that is the desire on the part of Colonel Jim Cogswell to always do an outstanding job in this field. Thank you.

DEAN C. RICHARDSON
Defense Supply Agency

On behalf of the Chief of the Office of Industrial Security, Captain Larson, I certainly welcome this opportunity to discuss DCAS concept of classification management. When we were brainstorming this session in

Mr. MacClain's office, I said that I would speak on the CAS role in classification management, and one of my colleagues said, "Well, that ought to take about thirty seconds." I will take a little more than thirty seconds. As Mr. MacClain said, we do have an organ through which people can, both in Government and in industry, obtain some needed help and assistance. Also, I would like to commend keeping in mind Captain Larson's aim in the industrial security program—and that is professionalism. I am very happy to see familiar faces here this year in this same room, and some new faces in this room today, that were here two years ago when we had our meeting in these very dignified surroundings. And I think that this is good for the Society. We really do need professionalism in our program.

The classification management program is of course the cornerstone in the industrial security program. By the act of a contractor and the Government in citing a DD-441, the Security Agreement, the Government agrees to provide classification guidance to the contractor. Only when the Government places a classification on documentary material does the program then come into being. As you are aware, the ISM does not relate to unclassified documents, it refers to classified documents. There are two basic parts of the CAS role and the Defense Classification Management Program, the role of the ACO and PCO—and the ACO's responsibility is for subcontracting. And then there is the Cog Security Officer's role. In providing classification guidance to the subcontractor, the ACO must necessarily provide a well-defined basic classification guide issued by the PCO. If he's in doubt, he will go to the PCO and obtain the guidance and identify it in the subcontractor's guide that's prepared by the contractor.

The Cog security officer's role in the classification management process is one of monitoring compliance, or enforcement if need be. The Cog officer does not issue classification guidance. He does not make any classification determination. But he does see to it that classification guidance is furnished with every classified contract.

The Cog office monitors to insure that the contractors have been been furnished an annual review. If a contractor does not have an annual review automatically, and the Cog office does not appear to have issued a request for it, ask him to obtain an updated DD-254.

The Cog office tries to identify, and in some cases anticipate, problems in the contractor's program, and refers these to the proper contracting officer. So you don't have to always know who your contracting officer is. If you don't know, ask your Cog Security Officer. If he can identify it, he will. There are very few cases any more where the contractor cannot identify the contracting officer. The cognizant security office therefore acts only as a catalyst between the contracting office and the contractor. And this is where the frosting comes, because sometimes your mar-

keting types don't want to rock the boat and they don't want to cause any friction between the customer and themselves. So rather than argue with the customer, they go to the Cog Security Office.

We have had this situation come up many, many times, and just recently I have seen some pretty horrible examples of classification guidance. When referred to the classifying authorities in the Army, Navy, and Air Force, these were immediately cleared up. It was a matter of misconception, perhaps, on the part of the contracting officer, and it was immediately cleared up. If you are still having problems, go to Cog security. I want to emphasize that you should hit your contracting office. If no response, go to the Cog security. You may not get any better response but at least you have taken every avenue.

We hear a great deal about establishing a classification management team in the contractor's facility. Bob Arnold addressed this as did Dan Rankin. We in CAS strongly endorse this concept. In fact, we recently published an article that probably most of you have seen. Such a classification management team, composed of selected technicians, engineers, security personnel and contract management specialist, should participate in all phases of a classified contract performance by the contractor. On the Government side, we recognize this need for greater team effort. I am gratified at the result of a recent road show for ACOs and PCOs. We noted a greater awareness on the part of these ACOs in their security responsibility. More and more contracting officers are providing contractors with better and more timely guidance. One example is the annual review of the DD-254. To keep this momentum going, CAS is conducting a training seminar for DCAS personnel, who, when they return to their regions, will form a nucleus of a team to indoctrinate at least 3,000 additional contracting offices on their security responsibility, and this includes classification management. And by security responsibilities we also mean classification management, proper and timely.

Looking further down the road, we are now in the design phase of mechanizing CAS. This is sometimes referred to as MO-CAS 2. One of the processes that we are cranking into the MO-CAS concept is an automatic print-out of the DD-254 list in each contractor's facility as their anniversary dates come up. This is going to expedite the annual review, at least by notifying the user agencies of annual review requirements.

This is the way it will work: a month before the annual review, a list will be printed and sent to the Cog Security Office as well as to the contracting activity that prepared the form. Should no action be taken, the computer will print out the delinquency list which will be ready for mailing to the contracting activity.

That just about winds up my thirty seconds. I do want to emphasize one thing: the classification management specialists in the DCAS regions are not classifying authorities and

you can never get a classification determination from the Cog Security Office. They are not authorized to make it. They have no desire to make it. But they do desire to help you get proper classification guidance. Now, before I close—I am very happy to present some DCASR representatives who are here on a staff visit and as part of the visit are attending this session: Bob Pace from Los Angeles, Tommy Thomason from Atlanta, Larry Mullins from New York, and Dan Hartzell from Cleveland. These folks are the industrial security specialists in the DCASRs that I mentioned—Los Angeles, New York, and so forth—who will be monitoring your programs for classification management.

Another item that I would like to bring up very shortly here, George, is in reference to your "reference material"—identifying who is the originator of the reference material. Your Cog Security Office can help you a great deal. He may be able to identify who the originator was, and if he can't identify it he will get it for you very quickly, so you can deal with one man. Or, as Mr. MacClain has said, "Come to Mr. MacClain." Thank you very much.

KENNETH WILSON: Mr. Aitken, we are beginning to receive contracts in which a 254 specifically states that the documentation, if that's what it is, will be, quote, "paragraph-marked." Most of these are from the Army so far, although we have had some from other services. May we interpret this as including the option that the ISM provides? In other words, does the contracting officer—is he specifying paragraph marking in its detailed sense, a letter in front of each paragraph, or does he understand that there are alternatives which in many cases we believe are more satisfactory for a particular kind of document?

AITKEN: May I refer that question to Mr. MacClain?

MacCLAIN: I would like to answer it because it has been asked quite a number of times. We have put ourselves on record on two or three occasions in writing. Although the DoD Directive 5210.47 states three alternatives and although the ISM does the same, they are not equal alternatives. The emphasis is upon paragraph marking and there is no basis for choosing an alternative until after a good faith effort has been made to apply paragraph marking and a good faith judgment has been made that it is not practicable in that particular case. For example, you are not able to approach a particular document and say, "Which alternative do I want to use," and start out with the third or the second. That is not the way it is to work. I think that's a direct answer to your question. You must use paragraph marking unless, after really trying, you find you cannot do it. We are not so hardheaded as to think it can be done in a hundred percent of the cases. If you do retreat from paragraph marking, and you use the alternative of explaining within the document itself the parts of the document that are classified, you may find that you just as well could have done paragraph marking.

On the other hand, if instead of talking about particular parts by location, you start talking about the particular content of the document, and in sufficient specific terms so that people can identify that, that is also an appropriate way of doing it. It is certainly not appropriate just to attach a 254 to the paper. It is certainly not appropriate just to attach a classification guide to the document. It is certainly not appropriate just to refer to a classification guide thinking that the other fellow has a copy of it. You see, you, the person who writes the document, are the person who best understands what about it is classified. If you are using a 254 you may be the only person, in relation to your production, who really knows how the thing is classified in relation to that paper. And this is, therefore, the desire of the three options. Try paragraph marking first. It's really the best if you can do it. Retreat only after you have tried.

WILSON: Well, it's not a case of not being able to paragraph-mark the document. This can be done. The question is—and we have found several cases that we have tried—that paragraph marking is not the best way from a stand-point of documents that have a lot of associated classification between paragraphs. We had a case that almost got out from one of our facilities where two paragraphs on a page were properly marked "unclassified." The information in each paragraph was unclassified. The material, when it was extracted, was put on another page, which was marked "unclassified." Everybody did just exactly what paragraph marking would lead him to do. But there was an item in the first paragraph and an item in the other paragraph, that together made the two paragraphs classified. We have documentation of this nature and this is a problem that I think is maybe greater than we have really looked at until we got into this paragraph marking. Where you can indicate the classification of the paragraph—fine. You indicate that the page is at the level of the highest paragraph therein. But there is information in an unclassified or confidential paragraph that's associated with another paragraph of a lower level, and then it reaches a higher classification. We don't intend and we are not thinking of just putting a 254 in the back. We would certainly do our best to make a summary or a more detailed description of what information is classified in the document. But when you do have cases like this—and in our general area they are more numerous than we have thought—we tend to feel that paragraph marking can be a trap.

MacCLAIN: I certainly encourage any of you who think that you have this problem to face it honestly in this way: if you know that paragraph one is unclassified by itself and paragraph two is unclassified by itself, and the two together are classified, for goodness sake say so. You see, this is one of the hard problems about marking content, whether you take it page by page, paragraph by paragraph, or document by document, or

chapter by chapter, with something that's in the public domain. What you know about the classification content of the document, please put down on paper. Don't limit yourselves to the symbols that are made available to you for convenience. If at the end of marking a document by paragraph, supposing you take each paragraph absolutely alone, and then at the end of it you say, "I know there is some association in here that's a problem," one way you can deal with that is to include something within your document that says, "The following elements involving association within this document are brought to your attention." And anytime that any part or paragraph contains information responsive to this guidance on association, deal with it as such. This is, of course, one of the big objections. You say that paragraph marking won't work for this reason. I simply say that if you know that this is the case, say so on paper, put it before the fellow that is going to get the paper from you. And this will take experience, believe me. It may very well be that this association problem is one of the reasons why one of our brother agencies will not affirmatively adopt paragraph marking. But merely because it is a problem doesn't mean it's an insuperable one. We don't think it is, anyhow. I am glad you brought the point up, though, because it comes up frequently.

WILSON: I thought the choices you gave us in the ISM were equal level choices, from the way I read it, and the company policy which is on my desk for signature was saying that. So I'm glad I brought it up, too.

MacCLAIN: All we have to do is point it out to the DCAS. I am sure that we should write something for an industrial security letter to make this clear. We will do so.

FRANCIS MAY: I am from Headquarters, Air Force. I think the specific item here goes beyond what you said, George. I think Ken's situation is getting to the realm of a specification of the contract, so to speak. If his contracting officer has said that he wants the paragraphs marked, I believe that he has taken this out of the provisions that are in the ISM, by contract, and that Ken would not have any options. If he would want to be relieved from this he would have to go back to his contracting officer. I raised this on a situation that we had well over two years ago now, before we had the paragraph marking established within the ISM. One of our commands stated that they wanted particular type documents marked by paragraph, and they so stated, and the contractor asked for relief from this. We wrote at our headquarters and, unknown to us, CAS also got the same question and ruled the same way, that it was a contract specification, and therefore it would have to be honored.

MacCLAIN: Well, I think the contracting officer can lay on some requirements and then pay for them. But I think we should all be alert to a requirement that produces an unexpected and an unforeseeable problem in classification. We should bring

that to the contracting officer's attention and work out a solution that doesn't cause trouble to somebody. In particular, when you know of an association that has a problem and you have a way of putting it on paper, please do so. It's the best thing I know.

A. A. CORREIA: I know the case that Frank is talking about, and and we've been living with this for a year and a half. It's Air Force Systems Command Regulation 80-20, which says you will classify by paragraph. They tell you how to do it. And the contracting officer in these commands have all been briefed. And, on Ken's problem, I don't think you are going to get out of it, because it's a contractual requirement. If Mil Standard 847 is called out on marking documents, or AFSC Reg. 80-20 is called out in the contract instrument, you have got to comply with the contract instrument, and you have no choice. We challenged one in Autonetics, and the contracting officer came back and said, "We're familiar with the three different choices. We want the one we called out. You comply with it." And we said, "Yes, sir." And we complied with it.

MacCLAIN. I don't object. I don't object. I think that in compliance you can keep from falling into a trap. When you see the trap, say something about it so the next fellow won't fail to see it.

W. T. WILCOX: This is for you, Mr. MacClain. With reference to the retention of reference material obtained through DDC you stated that we would have to justify our need to know in order to retain this, after the completion of the contract. Well, how does this jibe with the technical objectives program and the guidance that's given the PCOs and ACOs in paragraph 7-104 of the ISR on encouraging a liberal view on retention of documents to permit contractors to have reference to technical libraries?

MacCLAIN: It is true that the Industrial Security Office is endeavoring to encourage a liberal attitude on the part of user agencies toward the retention of classified material. But it is still true also that retention is not unlimited in point of time, and retention doesn't even start without some kind of demonstration of need to know. What they are really encouraging, I think, is a liberal attitude toward evaluating the need to know. But as far as I know, retention is never authorized for an indefinite period now. I don't think it will be. Accordingly, the need to know review is constant, periodically.

F. X. JAHN: In answer to Mr. Wilcox's question, you do have, on page ten of this blue booklet that we were all furnished, the specific answer to the question. And I might say that George MacClain reviewed this with us before we printed it. It's right in line with what he said.

MacCLAIN: Was my answer consistent with what you have on that page? I hope it was because this has been a continuing view of ours, so I hope that we didn't cross up ourselves. I hope that you all have had a chance to see the Westinghouse pamphlet. I hope that also any of you others who

are producing pamphlets—and I know that there are some of you who are—will make them available to your brothers in the business. It's a great thing.

ALFRED DUPELL: As long as the retention clause has come up, George, I wonder if you would mind making a comment on that. In those contracts that I have cog over I find that my contracts have an 80% "in violation" in requesting retention. And it's something that must be done. I will say that in replying to the request for retention, we do evaluate where we are going with that particular contract. And this does make a big difference on the length of time. We have got to get the requests in. I reviewed something like 6,000 closed contracts, and there was less than 20%—in less than 20% of the cases was the contractor holding the documentation legally.

MacCLAIN: I am not sure that I understand your question, Fred.

DUPELL: Well, it's that we have got to emphasize the point that they must come in for retention of classified documentation upon contract completion.

MacCLAIN: Oh, I see. He's emphasizing that. Well, don't forget, when you get the ISM printout of the instructions on the 254, as revised, this point will be emphasized. Do your part. Come in with your request for retention and make a real good showing of your need to know. Don't simply say, "I need this because someday I will need this in another contract that I hope to get." Make a reasonable showing and come in on time.

JOHN WISE: In relation to the last comments, do cog officers actively participate in this evaluation on retention—I mean, versus the PCOs? The security people, or the PCOs?

MacCLAIN: I would like someone on the panel to answer that. Will someone on the panel take that question?

RICHARDSON: I can only state that again this is a PCO function. It is not the cog office's function. The cog office goes in and says, "Do you have retention authority?" And if they can't show that they have retention authority for classified information after the termination or completion of a contract, then, of course, the contractor is obligated to dispose of the material in accordance with the regulation. But it is the contracting officer's responsibility—the PCO's responsibility, if the ACO has been told he cannot provide this responsibility—it is the "owner of the information" who is responsible for providing retention authority.

FRED DAIGLE: George, you just indicated you were soliciting some information on cost savings as a result of classification management actions. Are you looking for case histories as references, things that have already been approved by the Government, or are you looking for something that you can go in for, some credit for cost-savings, or just what are you looking for in this particular vein?

MacCLAIN: I am not looking exclusively for those things that you

would take to your user agency and get approval of as a cost reduction sum of money. I am not trying to live within the framework of whatever the Department of Defense cost reduction program permits showing. I am trying to ask for past incidents, or incidents from now on in which classification management practices are cases in point showing that you are doing something unclassified that otherwise you would have expected to do classified, and that because of this change in approach you will save an anticipated number of dollars and cents, reasonably calculated. Some of you have already done this. I have heard of two or three instances where you can actually document it. The more you can document it, the better off we will be. A cost reduction versus a cost avoidance is a distinction that I don't know too much about. But, for example, if in laying on a contract in which you already agreed to pay a $100,000, based upon an assumption that it's going to cost that much to protect secret information, and then you get together and you decide that this can be handled unclassified so you don't have to pay out the $100,000, I suppose that since this is a prebudgeted amount, it would be a cost reduction as against a cost avoidance. And as far as I am concerned you have saved some money. I would be willing to call it either one. We would be glad to have either one. It would be well, I suppose, to show whether it's genuine cost reduction in that the intended cost has been reduced, as against an anticipated but now unnecessary cost. I hope that's not just semantics. All those cases are valuable.

DONALD GARRETT: May I suggest also that we are very anxious to learn of techniques that people develop by which they apply classification management pressures that result in savings in many ways. We would like to be able to accumulate these, and pass them along for everybody to consider, because there may be many circumstances where a similar technique could be applied again, resulting in savings across the board.

DONALD WOODBRIDGE: George, could you summarize the allocation or assignment of responsibility for declassification in the DoD?

MacCLAIN: Our attitude on declassification as an activity distinct from either classification or downgrading is that to the maximum possible extent the automatic system should be used, which will indicate at the time the document is created when it will become declassified through passage of time. And this decision is accomplished by the person who has the authority to decide that that particular document is classified. If this decision is made in industry, it's made pursuant to guidance; the original decision on downgrading is part of the 254 and is made in the Government. If, as a matter of fact, you do not have downgrading and declassification guidance of an automatic kind indicated on the paper, and in any case if you want to downgrade or declassify ahead of schedule or in the absence of a schedule, our view is that the authority

to declassify is integrated with the authority to classify in the first instance. But because in the Department of Defense the authority to classify is widely delegated, the authority to declassify is also widely delegated. It is not like, for example, the Atomic Energy Commission, which classifies by policy created by the Commission. The Commission itself, without any delegation, as I understand it, has to do all of the declassifying. That is not so in the Department of Defense. It does not take the Secretary of Defense to declassify something. It does not take the Secretary of the Army, Navy or Air Force to do it. Anyone with original classifying authority can also be the declassifier, but he should be the original classifying authority and he should know what he is doing. Now, we have a vast problem in the Department of Defense of trying to find out what to do about information that gets out into the public domain, which, as far as the people in the Department of Defense know, is still classified. This does happen and we know it does. Sometimes the information that is in the public domain, through a trade journal or newspaper, is there because the writer made a good guess. There are some very expert writers and they can make good guesses. And they are not likely to say point blank, when they write their article, "This is my guess." They are not likely to quote somebody who told them something if indeed it was a break of security. Therefore, a problem is always presented when something appears in the public domain that we thought was classified. The mere fact that it does appear in the public domain does not mean that it is declassified. This should be well understood. It does mean, though, that actions have to be taken to evaluate it, now that the compromise has occurred, and determine whether the information should continue to be treated as classified. And if we should decide that it should no longer be treated as classified then we have the responsibility of notifying all concerned. Now, this is something we haven't worked out very well yet. I don't know, Don, whether I have met your problem.

WOODBRIDGE: I think you met it largely by saying that the authority to declassify goes back to the originator or the original classifying authority.

MacCLAIN: You do have authority in the Department, the Assistant Secretary of Defense has the delegated authority from the Secretary of Defense, to accomplish some downgrading actions in the absence of getting it done elsewhere. And furthermore, I might say that in the same chain of command, a person higher up can overturn or reverse someone lower down, because it's a command matter. To that extent, we are a little bit more complicated, too.

I know we have no more time. Just let me say a couple of things. First, I regret we didn't have more time for questions. Secondly, on approval for public release, the 254 is not going to say anything different from what it does now. You will follow the channels to get approval for public

release for what you think is unclassified by following what the military department tells you. Nevertheless, the Director of Security Review in the Office of Assistant Secretary of Defense for Public Affairs is currently conducting a study to identify the best method of making a single channel for getting these requests into the security review. So you all are going to be doing it the same way, but we don't yet know what it is going to be. Another thing, automatic data processing for classification management decision and control is something we are studying in our office. In fact, we have selected sort of a pilot program to determine whether or not classification can be accomplished and monitored by automatic data processing. It's a small study, and it's getting started. Another thing I want to mention quickly is that we are well aware of the fact that industrial management people, especially marketing people, are not very much inclined to pull the classification management people from their own staff into the business of helping them to calculate a bid. As I have been informed, classification people in industry are considered as nuisances to marketing people to a large extent when a bid is being put together. We would like to hope that we can influence industrial management to realize the real benefits of getting a classification official within that company to help the marketing people put together a bid. We think they are going to be able to save a lot of money this way, on both sides.

CLASSIFICATION IN THE FEDERAL GOVERNMENT

By

John F. Doherty, Chairman,

Interdepartmental Committee on Internal Security

It is a privilege for me to attend this meeting and to have the opportunity to speak to you about an important contribution your association can make to the internal security of our country by the maintenance of an effective program relating to classified defense information.

The organization of which I am chairman, the Interdepartmental Committee on Internal Security, is known by the acronym ICIS and has been in operation for the last eighteen years. So permit me for a moment to give you a little background on the ICIS.

In 1949, the National Security Council studied the entire field of internal security and agreed that the necessary degree of internal security had not been attained. It was determined that the then existing inadequate internal security protection was attributable in large measure to the absence of a centralized coordinating mechanism.

There was a proliferation of internal security bodies with a resulting overlap of authority and duplication of effort. The National Security Council decided that the proper knowledge for our internal security requirements for integrated action with respect to the resolution of problems in this field required the concentration of responsibility in one central point. Maximum coordination of effort, without interfering with the responsibility or authority of any department or agency, required formal interdepartmental liaison.

As a result of the consideration by the council in '49, there were issued charters for two permanent interdepartmental committees. They were the Interdepartmental Committee on Internal Security and the Interdepartmental Intelligence Conference. The Interdepartmental Intelligence Conference, hereinafter referred to as the IIC, had existed for ten years prior to the charter from the National Security Council, and is responsible for the coordination of all investigations of domestic espionage, counter-espionage, sabotage and subversion, and all other related intelligence matters affecting the internal security. The IIC is chaired by Mr. J. Edgar Hoover, and its membership is comprised of the chiefs of the Intelligence branches of the Armed Forces.

The ICIS is responsible for policy coordination for all phases of the internal security of the United States other than those assigned to the IIC.

Pursuant to the provisions of the National Security Action Memorandum No. 161, of June 9, 1962, issued by the President, both the IIC and the ICIS were transferred from the supervision of the National Security Council to the Attorney General of the United States, who has the assigned primary responsibility of insuring the development of plans, programs, and action proposals to protect the internal security of the United States. On March 4, 1964, the charters of both committees were amended to reflect the provisions of this NSAM 161.

The ICIS in its respective field, and in collaboration with the IIC when necessary, is charged with insuring the establishment and maintenance of the highest practicable state of internal security. It undertakes studies and necessary actions to insure complete coverage is maintained by the appropriate departments and agencies in the field of internal security.

The ICIS is composed of members representing the Department of State, the Department of Treasury, the Department of Defense, and the Department of Justice. Its chairman is designated by the President after consultation with the Attorney General. Non-agency member representatives are invited as *ad hoc* participant members when matters involving the interests or responsibilities of their agencies are under consideration.

Problems considered by the ICIS pertain to defense against unconventional attack, such as biological, chemical, radiological warfare; entry to and exit from the United States of potentially dangerous persons and material; the security problems at-

tendant upon the presence in the United States of certain foreign diplomatic and official personnel; with industrial security; and with the protection of classified defense information. And it is about this problem that I would like to talk this morning.

As you know, Executive Order 10501 governs the protection of National Defense information, which, if disclosed to unauthorized persons, could result in danger to the internal security of the United States.

The Executive Order, after defining the types of National defense information that may be classified in one of the three categories, also fixes responsibility for the protection, declassification, and downgrading of classified information. In addition, it limits access to such information to trustworthy individuals, and restricts access to those having a need to know.

The National Security Council assigns the responsibility for conducting a continuing review of the implementation of this Executive Order to the ICIS, in order to insure that classified defense information is properly safeguarded in conformity with the provisions of the Executive Order.

In the past many surveys have been conducted, and at present the ICIS is engaged in an in-depth review of how Executive Order 10501 is being implemented. Every department and agency having authority to classify defense material under the order was requested to report on any problems it may have concerning the implementation of the order. At present, we are studying these responses. Many agencies have reported they have no problems or changes to suggest. Others have made detailed suggestions with supporting statements designed to accomplish monetary savings and/or increased efficiency.

I would like to digress from the discussion of classified information briefly and bring to your attention the existence of other information known as "unclassified technical or scientific" information having a strategic intelligence significance.

Mr. Hoover in an article appearing in the June 1966 issue of the *Nation's Business* captioned "How Red China Spies on the United States" cited several instances of attempts by the Chinese to buy or otherwise obtain technical publications by mail sent from seemingly innocent addresses beyond our borders. The Chinese, because they do not have diplomatic representatives in the United States nor membership in the United Nations, resorted to such a subterfuge to obtain this technical data. Mr. Hoover on another occasion related that a former Communist spy who defected to the West reported that the Soviet military attache in this country is able to acquire, openly, 95% of the material needed to complete his intelligence assignment.

This country, on the other hand, has no source of such valuable material readily available to it in Communist countries, where travel is restricted and the small amount of printed material is available only through controlled sources.

The acquisition of this unclassified information of a technical or

scientific nature having potential strategic intelligence significance has been a cause of concern to the ICIS for some time. In an effort to obtain technical information of comparable value from the requesting country, in return for this almost one-way flow of technical information from the United States, a clearing house was established in the Department of Commerce. One of its purposes was to assist Government departments, private citizens, business and industrial concerns who are solicited for such information by representatives of Communist-bloc countries. However, we have been advised recently by the Department of Commerce that there are thousands of exchanges between academic institutions and Federal agencies, and institutions in the Soviet-bloc. And in light of these circumstances, the central coordination of the exchange program, in their opinion, is ineffective. The ICIS is looking into this problem and hopes to resolve it in the immediate future.

Aside from the beneficial security and economic factors derived from a proper classification system, we should not be unmindful that the Soviet-bloc countries are relentlessly engaged in espionage here in the United States, to attain the technical and military supremacy necessary to their objective of world conquest. The intelligence personnel of these countries in the United States have been on the increase and their intelligence operations have been expanding. The number of official personnel of the Soviet-bloc here, as of February 1, 1967, totalled 931, and they were accompanied by 1,296 dependents, some of whom have intelligence assignments.

Since 1951, the Department of Justice has initiated numerous prosecutions under the espionage laws, the more recent of which were the Butenko, Wayland, and Boekenhoff cases. Just to show you that espionage is still being carried out, and that the Department of Justice, when the evidence is available, vigorously prosecutes these cases, let me indicate to you the kind of information that these three individuals obtained here in the United States.

John William Butenko, an American citizen employed as an engineer by the International Electric Company on a top secret defense contract, was indicted in November 1963 for conspiring to commit espionage with three members of the Soviet mission to the United Nations, in violation of Title 18 USC 794, in that they conspired and agreed to transmit to the representatives and agents of the U.S.S.R. information relating to the national defense of the United States, particularly information relating to the command and control system of the Strategic Air Command, which information was to be used to the advantage of the Soviet.

On December 2, 1964, the defendants Butenko and a helper were found guilty. Butenko received a sentence of thirty years, the other twenty years. These cases are pending appeal.

Wayland, a lieutenant colonel in the U. S. Army, was indicted on July 12, 1966. He was charged with conspiring to deliver to the Soviet

Union classified information relating to the National Defense, in violation of Title 18, USC 794. The information involved in his case pertained to our atomic weaponry, missiles, military plans for the defense of Europe, estimates of comparative military capability, military intelligence reports and analyses, information concerning the retaliation plans by our Strategic Air Command, and information pertaining to U. S. troop movements. Wayland, on March 1, pleaded guilty and was sentenced to ten years on one count, and five years on another, the sentence to run consecutively.

In the Boekenhoff case, which is now pending before the Fourth Circuit Court of Appeals, he was indicted and charged with having, from June 1965 through October 1966, conspired with the assistant commercial counselor of the Soviet embassy to transfer or transmit to the Soviet Union highly classified information relating to the electronic, communication and cryptographic systems and the equipment of the Strategic Air Command, and classified traffic information going through such equipment and code cards connected therewith.

In every espionage prosecution brought under the provisions of Title 18, 793 - 794 it is encumbent upon the Government to establish that the information that had been unlawfully obtained or transmitted relates to the National Defense, and that the person possessing or transmitting the information had reason to believe the information could be used to the injury of the United States or the advantage of a foreign nation.

The phrase "National Defense Information" is a term of broad connotation, which has been construed by the courts to encompass not only military information and intelligence data but any information the revelation of which could prejudice the United States in its foreign relations. The classification of information by a U. S. Government agency is not, however, determinative of the issue. The Government is required, under the aforementioned statutes, to introduce testimony as to how the defense interest of the United States would be prejudiced by the unauthorized revelation of the information.

Nonetheless, while not determinative, the classification of information is an extremely important element in the Government's proof in an espionage case in at least two areas. First, it is evidence of the Government's intention to withhold the information from the public. This is a necessary element of proof. If the information, for example, is in the public domain it will not support an espionage prosecution. Secondly, it is useful in establishing that the defendant was put on notice that the revelation of the information could injure the United States and that its dissemination to persons outside of the Government was not authorized. The classification becomes more important in proceedings under Title 50, 783, which prohibits a Government employee from communicating to a foreign country without authority any information of a kind that shall

have been classified by the President or the head of any department or agency as affecting the security of the United States. Here, it is essential that the Government show that not only the communicated information was classified, but also that it was classified in accordance with the rules pertaining to the classification of information.

From the foregoing, it can readily be seen that an improper classification of information would defeat prosecutions under Title 18,793 and 794, and might even present serious problems under Title 50, 783. Moreover, in all probability it would have a more adverse effect than just the loss of a single prosecution. For example, the Government has in the past enjoyed singular success in convincing the courts, the juries and frequently defense counsel, that the information involved was properly classified, was sensitive data, involving the nation's security. As a result of this success in our earlier cases, we have in subsequent cases escaped serious challenge on this issue. It is clear, however, that if it could be shown in a particular case that the Government improperly classified information, this would, in effect, invite challenges to classification in future cases. Not only would this add to our evidentiary burden, but since the Government's witness testifies to the national defense character of the information, he would be subjected to a much more extensive cross-examination. This would have the probable effect of compelling the Government to commit to the public record more details of the sensitive information involved than we are now compelled to do.

By every standard, then, improper or careless classification of information by Government agencies could have a deleterious effect upon our ability to successfully prosecute future espionage cases, and accordingly would result in serious damage to our internal security.

In conclusion, then, let me state that those of us who have the responsibility for the protection and dissemination of classified defense information must be ever mindful of the increased number of Soviet-bloc officials residing within our borders.

We should also keep in mind that these individuals are not satisfied with the technical and scientific information available to them just for the asking, but avidly seek to obtain our defense secrets.

It is only by our being constantly alert to those desires that their efforts to "bury" us will be made unsuccessful. Even though we have in existence what I believe to be an effective defense information program, I also feel that we could do better. I also feel that if we reexamine our existing programs with these three things in mind it would be of great assistance in making our programs even more effective: one, there should be a more thorough indoctrination of employees charged with the protection of classified defense information, including constant reminders; second, where warranted there should be more stringent enforcement of these practices and

procedures; and third, the violators of these practices and procedures should be subjected to more serious administrative and disciplinary action.

You may rest assured that your contribution to the protection of classified information, regardless of how insignificant it may appear to you to be, will immeasurably contribute to our total defense effort and make espionage in the United States unrewarding and unproductive for those bent on stealing our defense secrets. Thank you very much.

JAMES LANGFORD: With respect to Executive Order 10501, some of us in the civilian agencies feel somewhat uncomfortable with the use of the term "National Defense" in the order. My question is: When, within the context of 10501, do you consider the term "National Security" to be synonymous with "National Defense" and would you please comment on what you conceive to be the difference between the two terms?

DOHERTY: If you recall, Executive Order 10290 was based on the security information concept. Executive Order 10501, which superseded 10290, was based on the defense information concept. Now, as to the difference, I think that as I pointed out security information as such could include information relative to one's behavior, such as excessive drinking, criminal record, and things of this kind. But the defense information concept is more aligned to the defense of United States information. In other words, the kind of information involved could be advantageous to a foreign power, that is basically the concept for defense information. I don't know whether that answers your question. This is a problem that has come up very often—that is, the distinction between security information versus defense information.

HOWARD MAINES: Mr. Doherty, let us take an example and pursue it for a moment, if you will—the supersonic transport. Here we are in a technological race with a couple of other competitors. The Government is probably going to lay out something on the order of two billion now, and I think it will probably wind up at four billion, if we continue to inflate, etc. So it would seem that from the economic standpoint the taxpayers of this country and the Government have a tremendous investment in what amounts to national security. It's not a military weapons system, presumably, although some of the technology could spin off into a weapons system development. Within the meaning in 10501 of "the interests of National Defense," could this type of information be classified—the new metals or materials, for example, that are being developed to withstand about 2,000 degrees or maybe the turbo-fan engine, or the lubricants that let that thing operate?

DOHERTY: It seems to me, Howard, that at the present time this is the kind of technical and scientific information that's already being released, and it's solely dependent upon the Government to make this classification. Now, if you have a prime contract with the Government for the

development of this particular supersonic transport, I think you have to abide by the classification requirements. And if you feel that it doesn't have any relation to the national defense, then you don't have to classify it. If you feel that that kind of information does come within the purview of the definitions of 10501, then I should say you would have to classify it.

MAINES: I guess that's what I don't know. Does it come within the purview? It's certainly very valuable information. There are many areas. I just throw out the supersonic transport because that is widely discussed at the moment. But there is a great deal of gold flow going to depend on this. It has a potential of fifty billion dollars, I've read in some estimates, and the country that gets there first with the mostest is going to hog the show on that kind of money. It just seems to me that that's within the "interest of National Defense" just as much, you might say, as is the weapons system or the atomic bomb. We can live and die through the cold war channels just as easily as we can through the hot ones, I guess. Is there any possibility that 10501 would ever get into those areas, or is there anything in the mill that you can talk about?

DOHERTY: At the present time I don't know that this was suggested in the survey that we now have under consideration. But I think that if it constitutes a problem insofar as defense is concerned, they would raise it within the ICIS and we would be very happy to look at it.

GEORGE CHELIUS: Mr. Doherty, what do you define as information in the public domain—what is officially released by the Government organizations, or information that might appear in trade magazines, newspapers, etc., that has not been officially released?

DOHERTY: Well, in view of the recent amendment to the Administrative Procedures Act, Section 3, which is known now as the Public Information Act, if the information does not come with one of the exceptions specified in the act, then it's accessible to the public. They have in the act enumerated certain areas that would authorize the Government to withhold disclosure, and if the information about which you speak is not within one of those exceptions that it would have to be disclosed.

CHELIUS: Assume that it was within the exception but published in a trade magazine. In other words, assume that somehow a certain amount of guessing went on and they came up with the right conclusion, would you consider that a public release?

DOHERTY: Well, certainly not. I would say this: the effect of its classification has been lost, but in fact the information is still classified. And one of the difficulties in this case is that a piece of information bears a classification and then gets into the public realm through some magazine where it's very, very difficult to determine whether or not the Government has officially released the information. In many of the

cases we consider, individuals working on highly classified material can project and conjecture and come up with pretty good guesses as to a particular item that is highly classified. But that doesn't affect the classification of the information.

CHELIUS: The engineers in my facility ask me, when we determine that this information is classified, what investigative mechanisms begin to look at the responsible individual releasing the information? Is there any investigation related to trade magazines or publications and have there been any prosecutions related to this?

DOHERTY: I know of no prosecutions for items that appeared in trade magazines. I do know that we have had a number of cases that we've considered. But the difficulty in many of these instances is that the originator of the information makes an exceptional number of copies. They are disseminated through the particular department or agency and it is almost impossible to come up with the individual solely responsible for making the release improperly.

MacCLAIN: Mr. Doherty, I want to thank you for a statement you just made. I think it is one of the clearest statements I have ever heard and will help us to deal with this question of how to treat information that somehow got into the public domain and some of us think it's classified. If I remember correctly, you said the effect of its classification has been lost but it is, in fact, still classified. And I think this is clarity in the utmost and I do want to thank you for it.

PANEL—INTERNATIONAL ASPECTS OF CLASSIFICATION MANAGEMENT

Francis W. May, Headquarters, Air Force, Moderator

MAY: Ladies and gentlemen, this afternoon we are privileged to have a distinguished panel to enlighten us on the international aspects of classification management. In the normal course of business, we as classification managers are concerned with assuring that sensitive defense information is appropriately classified so that everyone handling it will give proper attention to the safeguards and controls. Among other considerations, our classification determination in relation to the information's impact on national security is to keep such information from individuals and foreign countries having interests adverse to those of the United States. In the complex international situation of today it is often necessary, and to our Government's best interests, to permit dissemination of classified defense information to friendly nations in International organizations, but only when based on a judicious evaluation. Our panelists, representing various functions within Government, are all concerned with that judicious evaluation.

As in any chain of events, someone must start the ball rolling, so to speak. In a typical situation involving industry, a contractor may start the ball rolling by contacting the Department of State, for example, and then waiting for a decision authorizing dissemination. Most likely he waits impatiently, because he is not aware of the internal processes. He will learn much about this subject from this panel discussion.

JOHN W. SIPES
Director of Office of Munitions Control, Department of State

I have no prepared statement and I think probably some of you here have heard what I will be saying, before, at various other society meetings. But I think that perhaps in order to put into perspective what my office does in this area in terms of the title of this panel—International Aspects of Classification Management—I ought to give you just a word of history.

I think it comes as a surprise to a lot of people, even people within our own department sometimes, that the State Department is in the business of controlling the export and import of arms, munitions and implements of war, and technical data. But I think that when one looks at history a little bit it can be documented that back as far as 1793 the first secretary of state commenced this kind of control in an embargo on cannonballs. And this has been a function of the department ever since, when there has been any control exercised, and certainly and particularly in times of war and national emergency.

Formalization of the control was accomplished in the Neutrality Act of 1935, which for the first time established what we now know as the United States Munitions List and actually commenced a formal system of export licensing. Of course that authority has changed but the thrust of the control, certainly since World War II, has not changed. The thrust of our control is certainly not in terms of the normal type of trade, that is, in terms of commercial considerations. It is definitely political, with certain overtones of military security considerations.

The first statutory licensing authority commenced in 1935, and there was then published a munitions list promulgated under the administration of the National Munitions Control Board, which was chaired by the Department of State. But in 1954, Congress enacted Section 414 of the Mutual Security Act, which says that the President is authorized, in furtherance of world peace, national security and foreign policy, to control the export of arms, ammunition, implements of war, and technical data related thereto. This says "in furtherance" if you will note the language. The export must be "in furtherance" of those objectives.

Pursuant to that statute, in 1961 the President, by Executive Order 10973, which was a reissue of an earlier Executive Order, delegated the function of carrying out this statute to the Secretary of State. The Secretary of State then has published in various editions through the years what we know as the "International

Traffic and Arms Regulations" which were last amended March 20 of this year.

The Section 121.01 of those regulations, which I hope most of you are familiar with—if not, we have plenty of copies in my office and I am sure most of your companies in their international division or general counsel's office are rather familiar with it—is the United States Munitions List. Now this list, by virtue of the language of the Executive Order, is published by and promulgated by the Secretary of State with concurrence of the Secretary of Defense. Items under this rather special authorized control as being arms, therefore, are not within the jurisdiction of the Department of Commerce, as other exports are. There must be an agreement, really, between the Secretary of State and the Secretary of Defense as to which items should be included. And this list is not immutable. It changes from time to time as the technology develops, as we have developments in the sophistication of weaponry and new inventions, in lasers and masers and air-cushioned vehicles and submersibles and what have you. So we may have additions. We likewise have deletions. Chlorine, an early World War I gas, is no longer really used in that area and we have dropped it off the Munitions List, and we take other items off from time to time. But this is the key list as to what is controlled by the State Department. And we find in that list, under Category 17, classified articles, and there is a definition: "All articles including technical data relating thereto not enumerated herein containing information which is classified as requiring protection in the interest of national security . . ."

So by definition, classified articles and material are within the export control of the Department of State. We find that there are further references in our regulations, which I would like to draw your attention to, relating to the handling of classified information.

We have a provision that requires us to approve any manufacturing, licensing or technical assistance agreement that an American firm or entity may have with a foreign firm providing for either the manufacturer being brought under license for a Munitions List article, or technical assistance to a foreign entity or firm in an area where the technology would relate to a Munitions List item. And this sometimes involves classified information.

We have a provision in our regulations that says, in connection with a license agreement of this sort that has been approved by the Department of State, the following:

Exportation of classified information in furtherance of an approved manufacturing license or technical assistance agreement, which provides for the conveyance of classified information, does not require further Department of State approval provided:

(1) The United States principal certifies to the Department of Defense transmittal authority that the data does not exceed the technical

and/or product limitations in the agreement approved by the Department of State and,

(2) The United States principal meets the requirements of the Department of Defense Industrial Security Manual relating to the transmission of such classified information and any other requirements of cognizant U. S. departments or agencies.

What we are in effect saying is that once we have addressed your agreement with a foreign firm to manufacture a weapon system abroad that may include classified elements of weaponry or classified data, and we have approved it in terms of the parameters of the agreement and the project, you do not have to come back again to the Department of State to get permission to transmit the data provided you meet the two requirements we mentioned. But you are within the parameters of the agreement and you meet the technical requirements of the ISM on the transmission. We do say that the agreements that you send in to us for approval must outline the classified information involved, indicating the highest degree of security classification. You have to specify that in the agreement. Some of you that have had dealings with our office may know, however, that many times we may approve a manufacturing licensing agreement with a proviso that is quite to the contrary provided that no classification information is involved. But this isn't always the case.

I think you would want to look at what we said to be technical data, because there again we bring directly in the definition of classified information as being included within our definition of technical data. We say that "as used in this subchapter, the term 'technical data' means (a) information concerning articles on the United States Munitions List which enables their use, operation, maintenance, repair, overhaul, production or manufacture; or (b) research, development, and engineering technology concerning an article on the United States Munitions List; or (c) any technology which advances the state of the art or establishes a new art in an area of significant military applicability; or (d) [and this is the pertinent part here] information defined in 125.03 as classified information." And classified information is either (a) equipment; or (b) information relating to a United States Munitions List article which has been assigned a United States security classification as requiring protection in the interest of National Defense.

So there again, by regulation, all classified equipment or technology is covered by the Munitions List. We do have rather detailed spell-out in the regulations on how you go about receiving this authority to export classified technology data. We say in Section 125.12 of our regulations, that any request for authority to export classified information by other than the cognizant department or agency of the U. S. Government must first be submitted to the Department of State for approval. In the event classified information is involved in a proposed exportation, a letter must

be submitted to the Department of State setting forth the full details of the proposed transaction, accompanied by five copies of the documentary information that you propose to export.

The letter to the Department of State—really to our office—must (1) indicate the highest degree of security classification of the equipment or information involved; (2) show the cognizant project or contracting agency; and (3) if the equipment or information was not directly contracted for, whether it was derived from U. S. Government sources, project development, bid requirements or contractual arrangements.

The classified information as we have defined it, which is approved for export by the Department of State, of course may only be transferred or communicated in accordance with the requirements of the Department of Defense Industrial Security Manual. This, of course, is relating to the transmittal of such information, and possibly there may be, in cases of atomic energy type matters, some additional requirements of other Government agencies.

There is a note here in the regulations for clarification that: "The approval of the Department of State is required for the exportation of classified information to be disclosed to foreign nations either in connection with visits to foreign countries by American personnel or in connection with visits to the United States by foreign personnel."

We have a further note stating that the jurisdiction we exercise does not extend to a United States Government agency when they are acting as such. "The exportation of technical data by the U. S. Government is not subject to the provisions of Section 414 of the Mutual Security Act of 1954, as amended. A license to export technical data is not required therefore when all aspects of the transaction are handled by U. S. Government agencies." This exemption has no application to the situation where the United States Government, on behalf of a private individual firm, acts as a transmittal agent either as a convenience or in satisfaction of security requirements.

What we are saying is that if the United States Government—the U. S. Navy—proposes to give information, classified information, say, to the Brazilian Navy, this is the United States Government acting and it does not come within the province of my office. It gets into an area of action that Mr. Freund will be telling you about, and certainly is not unrelated because the rules and policy that govern this, of course, govern us all alike. So when we address a commercial request for the exportation of classified information, we are governed by the same rules that govern the Government agency that would propose to release information.

I must just mention a little bit of general information. In case you are not aware, we do operate under statutory criminal penalties. Any violations of our regulations involve the maximum of 2 years and $25,000. We haven't had too many convictions under that. We handle about 30,000

applications a year, and somewhere close to a two billion mark in terms of dollar value. We do not deal in any way in Munitions List articles with the Soviet-bloc, Red China or Cuba, any of those countries. We don't really address a case that suggests exportation into those areas. We would not consider classified exports to those areas. I think just as a matter of passing interest, we do control imports in my office under the statute. This is something that is unique, perhaps, because our friends in the Department of Commerce, under the Export Control Act of 1949, as amended, have no authority in the import area. Our import activities are primarily in the business of small arms and miscellaneous articles most of the time. Most of our problems are in the export area.

CHARLES K. NICHOLS
Acting Director, Foreign Disclosure and Trade Control, OASD

Ladies and gentlemen, I think John Sipes has given you a very good sketch of the principal source of many actions that take place within the Pentagon on hardware exports involving classified information. This represents, however, only a relatively small area of the total activity that Defense has to address itself to in the field of classified disclosures or releases of classified information to foreign governments or international organizations. Basically, I would just like to describe for you the procedures and the organization, relatively new in the Defense Department, that have been developed over the last year for attempting to exercise our responsibilities in this area on a more timely and coherent basis than has been done in the past.

The basic responsibility for disclosure of classified information and for passing on requests for exports of military hardware now rests in a single office in the Office of the Secretary of Defense, International Security Affairs. Previously, these responsibilities had been dispersed to various activities around the building.

The organization in the Office of the Assistant Secretary for International Security Affairs has been established primarily as a policy control organization. It has no direct administrative responsibility over the military services or the Joint Chiefs, or any of the Department of Defense elements that are engaged in classified release activities. It is our function to establish policy or interpret national policy, to attempt to coordinate the activities of all of the various channels, organizations and sub-organizations including military commands, unified commands, throughout the world. But this is all done through a process of coordination rather than through a process of direction. I think the philosophy behind this concept is sound and that, as I will explain to you a little later, there are so many activities within the Defense Department structure for managing and conducting these release activities that for a single office to presume to put itself in position of administrative control would simply be unrealistic. Rather the philosophy is to establish policy, to pro-

vide guidance, to seek coordination, unity of action, and unity of interpretation throughout the structure in the hope that this would create a cohesive system worldwide.

There are essentially two basic problems with which we must deal in this central position. First, and I think the most important although by no means the most time consuming, is the matter of policy coordination. The second, which is far more time consuming and difficult, is in the general area of guidance and management.

In the area of policy coordination, one of the first and most evident problems with which we have to grapple pretty much on a day to day basis is a conflict of philosophy. This is between the elements in the Department of Defense and in the Government charged with responsibility for military sales and with responsibility for contact of foreign governments in developing military programs, and on the other side, the very serious and very severe restraints that must be imposed for security reasons on all of the elements of the departments that are engaged in military sales or in contacts with foreign governments leading to the development and improvement of military systems. It is, I must say, our most serious problem and one with which we must grapple on a day to day basis. The rule we have tried to apply is that the decision to be made first on a sales program or on a military systems program, is the decision of, do we want Country A or Country B to have System Y? If it is within policy, if it is proper for the United States to supply System Y—all things considered, including security, including balance of payments—we attempt then to get a decision on a broad basis that would say "System Y is right for Country B." The problem is then whether to release Documents A, B, C, D, E, and F. The security classification, confidential or secret, becomes a relative one.

I must say, however, that applying this concept in practice becomes extremely difficult owing to the fact that we have a very aggressive sales organization, which is proper as it should be. The constraints of waiting for a policy decision on a broad basis impose restrictions that the sales officers throughout the Pentagon are certainly finding difficult. But I must say I believe we are making some progress in getting an appreciation of the importance of having these actions done on a broad policy rather than on a piecemeal basis. There are a number of subsidiary policy questions that we have to grapple with on a regular basis, not least of which, of course, is a constant concern with the impact that this contact through military channels will have on relations with foreign governments or international organizations. We have constantly before us the problem of satisfying legitimate industry demands for openings for export markets. And last, and certainly not least important, we must at all times be aware that Congress has a very great interest in these matters and must be satisfied. On the problems of guidance and management, which is the second

major category of problems that we must deal with at the OSD level, we have, as I said before, set up an office that has the responsibility for central guidance and control of all foreign disclosure and activities within the Department of Defense. We do not have within the Department a formal committee structure for coordinating or for seeking control. We attempt to do it through indirect contact, each of the services, each of the major OSD offices involved in releases of classified military information has designated representatives whom we are in daily contact with. We seek their advice as much as they seek our advice. We attempt, through a free exchange, to get them to act in accordance with the general principles.

There is, as Mr. Freund will describe later, the National Disclosure Policy Committee, of which the Office of the Secretary of Defense and three military services, and other elements in the Department, are members. This Committee serves as a central coordinating policy guidance group for the Defense Department as well as for other elements in the Government that are concerned. We do not, however, duplicate this structure within DoD. We seek to do our job as informally as we can. We feel that this up to now has proved fairly satisfactory.

One of the important instruments for providing the necessary freedom of action through Defense to deal with release of classified military information is the delegation of authority route. The basic authority rests with the Department of State. This authority in turn is delegated to the Defense Department through membership on the central committee, the National committee. The actual delegation of authority, however, to offices and individuals who do the actual job of releasing classified information is fanned out on a very broad basis. There are, for example—and these are rough figures—276 separate offices in the Washington area who have been delegated authority to release classified information. These are probably the main channels through which classified information is released. In addition, we have approximately 175 accredited representatives of foreign governments who are attached to various DoD elements, who are authorized to receive certain categories of classified military information. There are approximately 600 project officers throughout the world who have, either directly from the Office of the Secretary of Defense or from one of the services or other defense elements, authority to release classified information in carrying out what are generally termed "defense exchange agreements," which authorize release of classified information to foreign representatives or representatives of foreign governments on specified projects. There are other delegations, which I won't go into in detail. But altogether, it is estimated that there are nearly 1,000 separate channels through which classified military information may be released to foreign governments and international organizations. I am sure that my friend Mr. Freund will be some-

what shocked at these figures, but I am sure that he understands that we keep very effective control over most of these channels.

Some other interesting figures. As to the sources of requests we get for release of classified information, there are three general categories. One has already been explained by Mr. Sipes. These are the classified releases connected with export control licenses that are submitted from the State Department for DoD review. They represent, as I said, a fairly minor percentage of the total. I think the most frequent requests come directly from foreign governments through one of the various channels I have just described. These may be here in Washington—the attaches, the representatives—they may be through the field level to a unified command, or defense attache type. It is almost impossible to describe the variety, the sources. Foreign governments are the principal source of such requests. In some cases we receive requests directly from industry, usually in connection with an export license request.

The other figure is that during the course of an average year, in recent years, there have been something in the neighborhood of 235,000 documents released through various release channels. In addition to documentary releases, there have been many, many more individual actions involving usually oral or visual transmission of classified information. Nobody has an accurate figure. It would be impossible to estimate accurately how many individual releases may be made. And there is no provision yet for reporting back to any central office in the Defense Department on each and every release that is made by some element of the Defense Department. We have in prospect an automatic data processing program which may in a year or so provide us with details on daily information on what releases are made through the various channels in the Defense Department, but this is some time off.

I think this is about all I had to say except that, looking to the future, I can see no great changes likely to be made in the basic policy on release of classified information by the Defense Department. We are governed by national policy; we are governed by an international situation that, I think everyone will agree, is not likely to change radically in the immediate future.

We do hope, through continually banging away at the management problem, to improve the performance so that the legitimate export interests will not be in any way hampered unnecessarily by restraints imposed by the classified control program. But I would not expect that there will be any dramatic improvements over the short term. Thank you very much.

RICHARD B. FREUND
Special Assistant to Deputy Undersecretary of State

My presence here today, while a pleasure for me, is probably a mistake for you. Mine is very much of an inside job, with all the restraints that exist in telling society what it really wants to know. In a way, you are about to receive one of those typical

letters that is half long-winded excuses for not having written sooner, and half explanations why the letter needs to be closed, with maybe a sentence of news sandwiched in between. You might comfort yourselves with the old saying that "What you don't know won't hurt you." I don't go along with that one, and therefore will try to sandwich in two or maybe even three sentences of news.

It might help to have some idea of what is going on between the time of request for authority to disclose classified military information is submitted and the time the answer is given.

First, allow me to make clear that I am speaking as a State Department official who happens to be the State member and Chairman of the National Disclosure Policy Committee, the NDPC as we call it. But I am not in any sense speaking for that interdepartmental body. Nor am I at liberty to tell you what goes on during its meetings.

It should be carefully noted that the NDPC has no authority to disclose atomic information, a subject about which Admiral Dare will speak to you.

Our disclosure policy is such that requests from foreign governments and defense contractors and U. S. military and civilian officials are also subject to the same procedures. Requests for permission to disclose classified military information, whether embodied in hardware, documents, pictures or for oral conveyance, normally come in the first instance to the State Department only in connection with requests to the Office of Munitions Control, as John Sipes has already explained, in connection with export permits. Otherwise, they come direct to the cognizant military service or other defense organization, as Nick Nichols has described. Such requests are all subject to the same considerations even though the policy provides that in some instances action is delegated to a single disclosure authority while others require NDPC approval. I am not shocked by the numbers of delegations to disclosing authorities.

The committee consists of—aside from State, the representative of the Secretary of Defense, representatives of the secretaries of the Army, Navy and Air Force, observers from the Joint Chiefs, the Defense Intelligence Agency, NASA, and the Office of the Assistant to the Secretary of Defense for Atomic Energy Affairs. Also, there are full members from the AEC and CIA. You can imagine what clam bakes we have.

What are the considerations? Simply answered, they add up to the point that the interest of the U. S. must be served by the disclosures. That's obviously too simple. What we mean is that the foreign policy and military objectives in the United States must be advanced by making disclosures while taking carefully into account the risk of compromise through substandard security systems in recipient governments.

You have heard from Mr. Nichols about the military objectives aspects already. I will attempt to deal in my very limited and restricted way with the foreign policies aspects. Basic to

all disclosures, for whatever reason, is that U. S. relations with the proposed recipient Government or international organization must be close and friendly enough to make further consideration worthwhile. If that criterion is met, we go on to consider the more complex foreign policy aspects. To illustrate, we must consider at least the following: (1) Will the information be likely to be used for purposes of which we approve? (2) That may be so today, but what are the prospects that the recipient Government is sufficiently stable and determined to maintain the desired usage? (3) Will otherwise appealing reasons for selling qualified equipment be offset by adverse effects on other governments' economies, especially those that would undermine our economic aid efforts? (4) Classified military information frequently relates to sophisticated equipment. Will its disclosure fly in the face of U. S. arms control and disarmament policies—for instance, by creating or worsening local arms races? (5) Will sales improve our balance of payments position and the wellbeing of our defense industry? Or will we be creating new competition with the opposite effects in the long run? (6) By disclosing a certain amount of classified military information, will we give a false impression of our readiness to give more, including equipment or production rights, only to worsen foreign relations by failing to fulfill such impressions?

I would like to pause for a moment at this point, and mention that I was very happy to see the Westinghouse Electric pamphlet, in which its employees are instructed to ask questions when in doubt about a thing being classified or when they think it ought to be classified and it doesn't have that great big stamp on it. The whole business of classification is something that you are experts in, but I have observed that during the earlier stages of research and development the point where that stamp gets plunked on frequently isn't reached. It is finally when it gets to someone in the Defense Department. So there is sort of a point there where you defense contractors have a very heavy responsibility. Erring on the side of caution, I think, is a very good idea, and that is why I said that I was pleased to see the Westinghouse Electric pamphlet.

Lastly, we are very insistent that no other country that has some of our classified military information passes it on to a third country without our permission. The reverse, of course, applies here. We have to be careful that something we worked out with the British is not given to a third country without British permission, for example. It's a joint venture. If we fail to exercise great care, and get advance approval, in one sense or another we have worsened our relations with the people involved and we have also given them a sort of free ticket to do likewise with our information. Not only do our country's interests require careful consideration of all these foreign policy questions—and more—but we must keep under review our disclosure policy toward each potential recipient, and by con-

stant I mean at the minimum, annually, and frequently more often.

Sometimes world developments make such reviews and consequent changes in policy matters of high urgency, and you only have to read the newspapers or stare at that box to know what I mean. And obviously that creates considerable uncertainty for defense contractors—which we regret, but that's the way the world tumbles. We may be openhanded one day and absolutely embargoing the next, and usually for no cause of our own. Something happens somewhere else in the world and we've got to take that into account and serve the national interest.

Well, now I must close. Sincerely yours . . .

JAMES A. DARE
Chief, Joint Atomic Information Exchange Group

Thank you. I notice the way they have arranged the panel is that the gentleman on the other end and myself seemed to be involved, more or less, with operating groups. My purpose here is to speak about the operations related to nuclear weapons.

Gentlemen, I have heard it said, and I am sure that you have too, that artillery was invented to lend dignity to what might otherwise have become a vulgar brawl. In this context, nuclear weapons must have been invented to dignify some higher level squabbles. In the process they have some side effects that complicate life in security and classification.

One of the most impressive aspects of nuclear weaponry is the fact that both the AEC and DoD have rules governing the use and exchange of information. This can result in various interpretations among our own experts.

To make matters a little more complicated we have expressed our desires to cooperate in an atomic way with our nuclear allies, our NATO allies. This led to the 1958 amendment to the Atomic Energy Act which opened the way to some official exchanges of this kind of information. All services were affected as was AEC. With all the possible channels, it became clear that a single controlled channel for dissemination would be desirable. The Joint Atomic Information Exchange Group, JAIEG, was formed in late 1958.

This group is jointly staffed by the AEC and the DoD. However, most of the interested customers are in DoD. So the group is physically housed and associated with the DoD, and in fact is administratively supported by the Defense Atomic Support Agency and located nearby.

Now, the JAIEG performs two somewhat unrelated functions.

First, it operates centrally to obtain coordination between the Atomic Energy Commission and the Department of Defense in determining what is to be released. After this determination has been agreed upon, and in fact has been approved at the highest level, the JAIEG then monitors the operation of this agreement, monitors all the transmissions, and if necessary, obtains rulings on specific releases and may go back to the originator

recommending alterations or deletions.

Second, JAIEG is a depository for copies of all transmissions. This is simple for documents. It is not so easy nor quite so credible for verbal and visual transmissions. However, to the best of our knowledge, the records exist in our files of all official communications of atomal information. The word "atomal" by the way, is the NATO term for information relating to nuclear weapons.

The machinery we use to accomplish these functions might be of some interest. The bilateral agreements are not intended to be precisely alike. They are based on a need-to-know principle in the interest of the U. S. Government. They are quite variable, in fact.

The United Kingdom agreement is the most liberal and provides for considerable cooperation in the 144b (military information for planning, training, intelligence, and compatibility purposes); 144c (weapons design, development, or fabrication); and 91c (materials—weapons and weapons systems) areas.

The Australian agreement is most restrictive, having been established under the Atomic Energy Act of 1954 prior to the 1958 amendment.

The NATO agreement is quite extensive in 144b (military) areas but does not permit any 91c (material) cooperation.

All other agreements are oriented toward full military cooperation in the 144b and 91c areas, the latter confined to non-nuclear parts of atomic weapons *systems* only.

On the U. S. side, our customers are generally government agencies or services who wish to sponsor either an exchange or transmission of data. Because these transactions must support the national interest, I expect that this list of sponsors will not grow and will continue to be rather restricted, even though the source of information may be from a larger community, such as industry or study groups or educational institutions. However, we at JAIEG are quite willing to discuss procedures and problems with anyone who has a legitimate interest.

JAIEG headquarters is located at Courthouse Square in Arlington, on the third floor of the building known as Courthouse Square West.

In my few years of service as a staff officer, I have learned that one always keeps someone between him and the work. I brought my two deputies with me. I would like to introduce Mr. Jim Goure, who is a Deputy for the AEC, and Captain Bob Gaskin, who represents the DoD side. We would welcome you any time you have a problem that you want to discuss with us. Thank you.

GEORGE CHELIUS: I represent the Douglas Company in Santa Monica. I would like to direct my question to Mr. Sipes. I have a number of them, actually. The first is, under 125.30, the definition of technical information, is there any move afoot to define "technical information" in a more precise manner? The contractor or the individual proposing the release of information is faced with the primary burden of deciding

whether it is technical information. If the contractor decides in the negative then he would be free to release the information without going through the Department of State. This brings the question, what do you consider to be technical information? Could it include basic scientific information as well as technical data, and is there some way that we can narrow the "gray area" of technical information?

SIPES: We just finished revising the definition in the December issue of the regulations. At that time we called upon all the industry trade associations—the AIA, the EIA and NSIA—to help us. At the spring meeting here in Washington the AIA had several similar questions from the floor, and we again invited industry to give us their contribution as to definitions that might be useful. We don't have any great pride in authorship. We called upon the Department of Defense to help us also in defining this. But I should point out that I don't think that this is pertinent with respect to the forum here because all classified information is within the definition. So I think that the problem your company would have in this regard is with respect to certain unclassified brochures and that sort of thing. Because if it's classified there's no question.

CHELIUS: Well, we would agree that if it's classified there is no question. But many of us are called upon to make basic determinations concerning unclassified information—as to whether the information must go to the Department of State or the Department of Defense. And therefore we need a better definition a relatively unprofessional person can make at least a preliminary determination from.

SIPES: Yes, I understand the problem, and we are quite open minded about any improvement in that definition and it is constantly under review and we would welcome any suggestions that you might have.

CHELIUS: My second question refers to the Industrial Security Manual. Recently, in the 1966 revision, they added a Footnote 9 to Paragraph 5n. I can read it briefly, if you are not familiar with it or don't have the Industrial Security Manual. It says:

"In addition to the requirements of this paragraph, the release of unclassified technical data is also governed by the Export Control Act of 1949, administered by the Secretary of Commerce." And "Section 414 of the Mutual Security Act of 1954, as amended . . . administered by the Secretary of Defense through the International Traffic and Arms Regulations."

The question is, what does Footnote 9 mean to the contractor? Also, note that it refers to the International Traffic and Arms Regulations and the Export Control Act of 1949. We had been following the procedures under the ITAR and requesting permission for foreign release through the Department of State. When and what are we required to coordinate with the Department of Commerce?

SIPES: Well, all exports save those on the Munitions List or technology

relating to Munitions Lists articles are within the province of the Department of Commerce. The export of some of your commercial data or some of your commercial equipment such as your commercial aircraft, or General Electric's refrigerators, for example—all of this is subject to Commerce control under the Export Control Act. So only the military or the Munitions List items related to such come under the ITAR. The Export Control Act, particularly in the areas where validated licenses are required dealing with anything that has a strategic significance, is at least as complicated a procedure as getting a license out of my office.

CHELIUS: Would you suggest, then, an individual wishing to present a paper at a foreign symposium would have to have his paper approved by the Commerce Department if it did not fall under the Munitions Control Act?

SIPES: I am not an expert on the Commerce regulations. The Commerce Department's export data controls—I don't know just exactly what words to use—but they are somewhat more permissive than our controls.

NICHOLS: Well I can answer part of that. Commerce puts out a comprehensive schedule and they have in there a detailed description of procedures necessary in connection with technical data controls. It's equally informative as the ITAR, if not more so, on detailed procedures to be followed.

CHELIUS: If I might, I would like to ask for comment on one further matter. Under the ITAR regulation it states that if information has been approved for release by the user agency and has, in fact, been released on a national basis, there is no longer a requirement to have it approved for international symposiums. What is really the intent of that particular provision, and are local public information officers aware of it?

SIPES: The exemption in the regulations they should be aware of, because with respect to information that has been approved for public release and has in fact been released, we have extended that exemption on a worldwide basis on the theory that it doesn't seem necessary to do an unnecessary thing. I mean if it's released here, by public release, by having been given at a symposium or forum, it's quite likely that an attache of any country could have been in attendance. So, we have extended the exemption under 125.30a (1) and (2), in the regulations, on a worldwide basis.

CHELIUS: Is there a move to change that particular section of ITAR?

SIPES: There is consideration being given to language that says, "not only approved for public release, but in fact released."

JAMES LANGFORD: Mr. Sipes, regarding the actual control procedures at ports of embarkation to insure that export licenses have been obtained and approved for the actual export of equipment and hardware out of the United States, who monitors this and how is it done?

SIPES: Well, the Customs Agency Service within the Bureau of Customs

is our enforcement agency, as it is the Department of Commerce's enforcement agency for enforcement of the Export Control Act. You would have to hand over, actually, the original, signed, with the State Department Seal, a copy of your license, and also an export declaration which you have to fill out when you make a shipment involving any Munitions List items or technical data. By the same token, the Postal Inspector's office is responsible for what is exported through the mails. We have found that quite a few Postmasters around this country have never heard of the export control regulations or Munitions Control regulations. We are going to embark upon a little educational program in that regard.

J. S. TROUTMAN: Did I understand you to say that if a professional society, for example, publishes a journal they have to get some sort of a license before they can send it to a foreign subscriber?

SIPES: No, I didn't say that. If it has been published in a scientific journal—without addressing the question of whether that was correctly published or not initially—once it has been published, you do not have to get an approval from my office.

DEAN RICHARDSON: I have a question that perhaps no one here has asked but it has been asked of me many times and I would like to raise it for Mr. Sipes. What are the requirements on a contractor for the export authorization for export of foreign classified information—no U. S. involved—only foreign classified that has come in to them, they have built something, now they are sending it out?

SIPES: W 'l, I don't know whether I have got the right answer to that. I would normally, if I received that question sitting back at my desk, I would call you up over there and ask you what the answer was.

RICHARDSON: Well, I think the answer that has been going back to the contractors has been no export authorization is necessary. The application has come in, it has been bounced back, and I just wondered.

SIPES: I would say that, of course, sounds like a good answer. Of course we all are obligated, as you know, under the bilateral arrangements with most of these countries to treat that information in the same manner from a security handling situation as we'd treat our own.

CHELIUS: Is it possible to speed up approval of technical information, unclassified technical information by first submitting it to OSD, Public Affairs, and obtaining approval of the fact that it is unclassified and suitable for release, then submitting this to the State Department without having to go to Public Affairs before coming to your office?

SIPES: I wouldn't recommend that. I thought Joe Liebling was going to be here today, too. I don't see him. But it would seem to me that this would lend itself to some duplication and would be likely to slow it down because under the procedures that have been put into effect in DoD now—and Mr. Nichols can probably address this better than I—this is exactly the entity within the Pentagon

to which we refer these things. We send them over from my office. So I don't see really why going there on a separate route when you are intending to export as distinct from making a domestic public release— why that would speed up anything.

CHELIUS: Does it go to more than one agency after it arrives at the State Department to go to the Joint Chiefs? Does it go to the Army, Navy, Air Force, as well as OSD, Public Affairs?

SIPES: Within the DoD it is up to them as to the spread out that they give it. I can assure you that most things do get referred to several entities within the Pentagon. We go to a central point in our own reference, which is Mr. Nichols' office.

MAY: As an added remark here, when they submit it to the Office of Security Review they should have it in sufficient number of copies. Usually, they have some set rule as to number—five, six, or ten—whatever it might be. And at this point, they farm it out to the activities within the Department of Defense that have the primary interest in the information contained in the document, and action is based upon the consensus of the comments that are received.

SIPES: It seems like the questions bear out my contention all the time, that most of the problems are in the unclassified area.

MAY: Very much so.

SIPES: There is such a gray area that it's unbelievable.

C. F. POENICKE: I would like to address Mr. Sipes, please. My basic question is, do you have any relationship or control over the Department of Commerce clearing house for federal, scientific, and technical information? I think we all realize that unclassified technical data that would ordinarily be the subject of your regulation control—the ITAR control, export control—is in the clearing house. It is my understanding that Public Law 776 of the 81st Congress which set up the clearing house, did so with the intent that information would be made readily available to American business and industry. The clearing house, though, as we know, does in effect export. I would like your comments on that, sir.

SIPES: I don't think we have any direct control over the Commerce clearing houses. They, as you indicated, are established by statute. They have certain statutory injunctions—really in the business of freedom of information sort of thing.

LANGFORD: To expand on that question a little, the new Freedom of Information bill presents the possibility of a foreign national obtaining unclassified, unrestricted technical data from an agency and then shipping it out of the country through diplomatic channels. Do we see any procedure or law to stop procedure of this type?

SIPES: I would rather beg off on that one. I happen to know that particular problem is presently being considered by our lawyers in the department a little bit.

L. S. AYERS: Have we in the discussion today discussed at all the third party role? One Government agency, according to Mr. Sipes, is not

under the controls of the Munitions Control but if one agency of the Government—as in the case of NASA or ACDA—having in its possession legitimately classified information even including Restricted Data, atomic information, which it has received from a foreign country, does it have any obligation to do something with that material if it wishes to send it to another foreign country or third party.

FREUND: As I said earlier, we require others to obtain our permission, and I think if it is classified military information, as defined under existing policy, we would feel the same obligation toward the government that furnished it to us before our passing it on to a third country.

AYERS: I am not sure that I see the distinction between that and the answer that was given a little earlier, although the one point that we are talking about now is defense information as compared to industrial information, I guess you could say. If we have no obligation on non-classified but must protect a foreign country's information that we receive through some legitimate means but may retransmit it, what is the prevention from retransmitting the classified? What is the mechanism that brings us up short to keep us from doing that?

FREUND: I am not sure that I see the distinction. So long as you are talking about classified information.

DARE: There is a distinction on Restricted Data, all right.

SIPES: And not only do we feel obligated to not do this but we have undertaken this in various agreements.

DARE: Make it clear on Restricted Data or Formerly Restricted Data that there is only one way to receive it, and that's through our channel. And there is only one way to retransmit it—through that channel.

AYERS: That was one of the points that I wanted to bring out, in the RD field. Do we have as good a control on military information, defense information, not including RD or FRD? I think this may be for Dick Freund.

FREUND: I doubt that we do have as good a control. The volume, the sheer mass involved, is absolutely overwhelming. That doesn't alter the obligation that we have. But you are just that much surer when you have got a smaller volume of stuff and it is all handled through one channel of JAIEG and that sort of thing.

HOWARD MAINES: I am not too sure that I have a question and I am not too sure that it hasn't already been answered, but if it has been I don't understand it. We have a little problem in NASA, about the determination of the advantage to the U. S.—is it any net advantage to do it? That has to go up to a very busy person, and a very high level person, to say, "Yes, it does," or "I can't see where it does or not." Quite often we hear the answer out of the technical type that "I haven't got the slightest idea in the world about whether it is to our net advantage to release it or not. Why doesn't the State Department make that determination?" Is there an answer to that?

FREUND: I think there are at least two channels for handling it just that way. One is that if it is identified as classified military information, then it becomes subject to our national disclosure policy, and it does go to all concerned—the cognizant area of Defense and also, if necessary, to the NDPC. If it is not established to be classified military information, and you wish to check with State, you do have our Office of Scientific Affairs which I am sure would be glad to oblige.

MAINES: Maybe it's just our own internal regulation, then, that requires them to make this determination, rather than coming down from the basic policy.

LANGFORD: The advantage determination, of course, is required by the presidential directive on the subject of foreign disclosure. The problem I think we have within NASA is not having a committee similar to yours—it is guidance or criteria as to what constitutes a net advantage to the United States. It could be as loose as to maintain friendly relations with a friendly power. This is a pretty weak net advantage. However, it has been cited in some cases. I think our problem might be unique to an agency that doesn't have the guidance of the National Disclosure Policy Committee.

FREUND: I do suggest in that case that your observer on the NDPC might be a good channel to pursue this further in internal interdepartmental discussion.

TECHNOLOGICAL INFORMATION AND PUBLIC RELEASE

James J. Bagley, U.S. Naval Research Laboratory

One of the most difficult problems facing classification management is, "Should technological information be released to the public?" We know from our conversations of the last couple of days that public release does in fact mean foreign release. So today, I will discuss the question personally. The ideas are mine. I released the talk for publication. It does not have the normal *imprimatur* of higher authority, and I am certain it does not (for Chuck Poenicke's benefit) reflect the opinions of the Navy Department.

What I intend is to raise several questions to possibly stimulate some thinking, and I will be fully prepared to duck if and when the rocks start flying. And again I would like to assure you that I know of no regulations in the offing and I am not raising or flying a trial balloon.

The title of this talk, which was picked out by Les Ayers, by the way, used the term "Technological Information . . ." Now that is very, very vague and imprecise. So what I will do at the moment is to define it: Technological information is information generated by exploratory development, advanced development

and test and evaluation. Please note that I did not use the word "research" because research and technology are not necessarily synonymous. Research produces knowledge, which in turn creates the need for development. Development produces technology, which in turn produces information; and it is information that causes the problem. What is this information and how is it used? Obviously it is a source of press releases, talks before technical societies, both foreign and domestic. It contains information used in patent applications, requests for export licenses, technical data that we have been hearing about. The uses and the reasons for information are practically endless. It is time I think now to introduce two new classifications (I will, again, be prepared to duck), and they are unclassified information, and information not classified. Is unclassified a classification? I maintain that it is. It is a classification that requires the least restrictive control. It applies to information that is passed, really, among the people who need it, who want it. Is it public information? No, it is not. Unclassified information is not necessarily public information. And I think this is where some of the confusion begins to reign.

As we have heard in the last two days, there may be many defensible, valid reasons that could stand a test of law that say that unclassified information is not public information. Hence the new term of classification known as "unclassified."

When is information not classified? Very simply, it is information upon which a classification decision has not been made. And I am sure that in your own houses, your shops, your offices, there are tons of information of this category—information that has not been reviewed.

Are unclassified information and information not classified classification management problems? Frankly, I think it is more of a problem than classified information. Why? When information is classified a decision has been made. There is no guess work. The only basic remaining decisions are the degrees of protection required. Unclassified information and information not classified are far different animals.

This is a free society, a society as we know based on the right to know. Under the Freedom of Information bill there is a requirement for maximum release of information.

Information, as you all know, is a vital cog in the wheels of progress. To a scientist, it is publish or die. We may not agree with this but it is a fact. To a contractor, it is publish or advertise, or go out of business. To the government, obviously, it is an informed citizen. And there are all kinds of pressures involved in the release of information. And we in the classification management business must be ready and able to stand the heat of the kitchen.

There are guidelines for classified information. Simple, again. The identification of information that requires protection in the national interest. For the unclassified, the guidelines are not that easy. There must be maximum disclosure as I said except

for what would be of assistance to potential enemies—and it is here where the going gets rough. There are, of course, regulations of the services, the various statutes we have heard about in the last couple of days, governing the release of unclassified technical data. But do you know the rules? Do you know the items covered by the various laws? Do you have reasonably current information on items that are on the restricted list? Or about items removed? Are you aware of the agreements between the United States and other countries that developed a need for exchanging information? If you have these, consider yourselves lucky. But there are other factors that must equally be considered. What is the propriety of release? Are there ethical considerations involved? Do you have the authority to decide that a piece of information is or is not releasable?

I personally have felt that there is too much diffusion of responsibility. Think of it now. How many people in your organization are concerned with the release or handling or generation of information? Scientific offices, contracting offices, public information offices, classification management people—each has a very important part in the decision. Do they get together, or does each go his own way? To paraphrase an old saying of Harry Truman, "The buck must stop somewhere." Where does it stop in your organization? Who in the final analysis is responsible for saying, "Yes, it will; no, it will not?" Is there a person in your organization who makes this decision, or is it so fragmented that responsibility cannot be established? Think about this one.

Each of the services has regulations covering technical information, technical data, public information. I think, frankly, there are too many regulations. But that is a personal opinion. But do the people charged with carrying out the regulations talk to each other? In my experience it's rare. Each operates in his own little sphere. The scientific officer is concerned only with the technical product and couldn't care less about something else. The contracting officer worries only about compliance with the contract, how far his neck is stuck out, whether he will pass an audit. PIO interest is obvious—spread the word. Then there is a classification manager. What role does he actually have in the process? How big a member, how important a member of the team is he, in fact? Does he have sufficient technical knowledge of the problem to make a critical judgement on information? Does he, when the pressures of release are very strong, have the ability to substitute less critical verbiage to do the job and satisfy the pressure? In fact, does he understand the language of the PIO, the contracting officer, the budget officer, the scientific officer? Does he have available knowledge of what a potential enemy is doing in a technical area of interest?

I think each of you should ask yourselves these questions. And many other questions can be raised that I believe you should ask yourselves.

So, in the final analysis, it is my

own conviction that the classification manager is the man on top of the pyramid who must ultimately stop the buck. It is he who can be the coordinating factor, the person in the best position to make a critical judgement. To do this he must take a very broad view. He must take tough—big, tough decisions. He cannot think only in terms of "keep it all back" "don't release anything." He must always be able to make a balanced judgement as to what should or should not go, and be prepared to substantiate his position. He cannot I think accept prior guidance that a particular piece of information is, in fact, unclassified. He must be able to satisfy himself that it is or that it is not. He must be able to correlate the isolated pieces of information in the same report or text so that he can make a judgement. And he should have available to him the resources to do it.

There is another decision that has been imposed upon classification people in the last couple of years—the distribution statements attached to every DoD technical report. What are the limitations that should be placed on the particular piece of information? Is it information suitable for public release? Should it be withheld from the public? I maintain that no Department of Defense contracting person can prejudge the fact that a particular report, piece of information, or what have you, will be unclassified. He doesn't know, and it is very, very difficult to make such judgements under any circumstance. Again you have the technical data requirements of a contract. What is the role of the classification manager in the preparation of either one of these documents? Does he know it? Is he part of it? Is he with it?

In the final analysis, I think the classification manager is the one, as I said a moment ago, who must stop the buck, and his job is to create a decision that cuts across many technical lines and disciplines and professions.

It is he who sets in motion a long, complicated, costly chain of events, as we all know. Because it is he, in the final analysis, who says to the physical security people, "This is what I want protected." So to do his job, he should be multi-disciplinary in education, eclectic in philosophy, have the wisdom of the ages, the hide of a rhinoceros, and I guess in the final analysis, as the kids say, be a real cool cat. But it is a tough job. And I thing that it is far broader than many realize. And sooner or later it will be encumbent upon all of us to develop the technical know-how to stand up and be a peer among peers. And to be of the stature of all the other people who make decisions; and not ever be low man on the totem pole. Thank you very much. Now, shall I duck?

MacCLAIN: I think the general rule is that if a document doesn't show that it is classified, people treat it as unclassified. And I think that is a pretty good rule to follow because if this document is created under conditions of Defense Department interest, there is a built-in requirement, of course, that it be considered for classification right from the very

beginning. I would not, therefore, be inclined to want to support marking documents as either unclassified or not classified, but rather let the situation ride. In fact, I don't quite see an advantage of doing what you suggested be done.

BAGLEY: I agree with you in part, but there is a basic reading of 5400.7, that alludes to the fact that information that is for offical use only, for example, need not be so marked. What I am saying is, and the only point I wish to make, is to knock in the head this old fallacy that "just because it's unclassified it is public information." It is not. I think that the bills that we have heard about for the last couple of days make this point amply clear—that just because it's unclassified it doesn't necessarily mean that it is public information. If you talk to the normal Public Information officer, for example, his first assumption is it is either classified or unclassified; and if it is unclassified, give it. This ain't necessarily so.

MacCLAIN: Well, it is my understanding, Jim, that people who sit in public affairs and conduct security review, after they have finished the decision of whether it is classified or not, by going out and asking, they then have to ask themselves, "Is it otherwise non-releasable?" I think they do this. But I don't know.

BAGLEY: The key point in what you have said, George, is that a decision, a considered decision is made by a person having authority to make the decision. Unfortunately, the reverse is true—that things are assumed to be public information which are in fact not public information, because no decision with authority has been made.

MacCLAIN: This sounds like a dialogue, but if you do not mind, we will go on.

BAGLEY: Sure.

MacCLAIN: I think actually where the Government is concerned, and it is in the business of creating information at some expense, it is probably not a valid assumption that it's necessarily public information if not classified. For the simple reason that there are so many—we know now—restraints upon its release on the one hand, and there are now some injunctions on its non-release on the other hand. I think we have come to a point where we turn around now and realize that the burden of withholding is now on the Government, without a doubt, and with 5400.7 on the books everybody in Government who is charged with the custody of information is certainly going to have to address himself to the very question, "Is it releasable or not?" This little gimmick that says, even if it is not marked FOUO yet perhaps it is not releasable, is a very difficult rule to live by. And yet, just for example, personnel records that are not public information, of course, are not marked FOUO, and a person recognizing it as a personnel record would know this. The injunction that everything not marked FOUO has to be considered for non-release is one very hard to live by. I don't know how anyone can; but we must.

BAGLEY: The point is, we must

live with it. It's here in the books; we must be able to defend our own actions. What I am saying essentially is, if you are going to take an action, take the action with knowledge. I think this is the cause of most of our problems. Now, you and Don know certainly the exercise that I have been going through on this Foster Committee bit, and this is releasing, reviewing, re-reviewing information going from the Defense Documentation Center to the clearing house, and the information is marked "Distribution Unlimited," and yet another review is being made of the thing to say, "Can it go?" It's a tough chore. But my own thesis is that information should be released with knowledge and with authority. If you don't have the authority to release, you don't have the authority to release, period. Particularly now, under the new law, there must be reasons for doing something or reasons for not doing something. As I said in the beginning, I wrote this before I had read 5400.7 and heard the discussion of the last couple of days. But I still basically have not changed anything.

MAINES: Yes. You took the shoe off the right foot and put it on the left, didn't you, Jim?

BAGLEY: Yes.

MAINES: The philosophy was expressed as the intent of Congress, and was that information would only be withheld with knowledge and authority—that unless there is a reason to withhold with knowledge and authority then everything is in the public domain.

BAGLEY: This is true. What I am saying, the shoe should fit both feet. You withhold it with knowledge; you release it with knowledge.

GARRETT: Did I gather you suggest that the classification manager should be the man who has the responsibility for assisting in this public release determination as well as in the determination to classify or not to classify?

BAGLEY: No. You heard Dan Rankin, for example, talk about the role, the responsibility vested by the security manual in the Classified Material Control Officer within the Navy. This is a specific responsibility. Now, I don't remember the Army regulation clearly enough, but I believe it is somewhat the same thing.

CLASSIFICATION IN DEFENSE-ORIENTED CONTRACTOR FACILITIES

N. V. Petrou, President, Westinghouse Defense and Space Center

I truly welcome this opportunity to express the Westinghouse Defense and Space Center's security philosophy. We are really proud of our effort to equip our armed services with materiel and I know that we are equally proud of the effort we are carrying on in our security administration.

Classification management is truly an involved subject that is really beyond my ken and I am no expert in it, but there are a few highlights that I can remark on.

First, I would like to define classification management as we see it. The term is rather simple. Classification management is the continuing evaluation of security requirements to make certain our national defense secrets are properly protected with a minimum obstruction to our efforts to produce defense materials.

Protection of our country's secrets is very important; equally as important, of course, is production of materials to defend ourselves. We certainly cannot let security strangle production.

Then our concept in this area of classification management really is attained not by any ordinary approach but a continual approach. It is a kind of approach that generates enthusiastic support continually and challenges the imagination.

There are four points that I would like particularly to cover wherein classification management effort can best be applied:

First, sound and specific interpretation of the Security Requirements Check List, the DD Form 254, on production contracts.

Second, the procurement of classified hardware from subcontractors.

Third, mechanized control of the accountable classified documents including the procedures that require strict need-to-know, the prompt destruction of unnecessary documents, and the ready identification of the accountable documents by contract number, and, finally, mechanized downgrading.

Fourth, stringent requirements to determine the real need for closed areas.

I have listed first "sound and specific interpretation" of DD 254s because the greatest return comes from the application of classification management principles in this area. I am quite sure all of you are aware that the average DD 254 really offers very little in the way of specific instruction and guidance. There might be an x mark in the corner that says Accuracy is confidential; or that Altitude is confidential, or that something else is secret. The question is how to interpret this.

In our case we have many classified contracts—in the hundreds by the way—each of which has a pro-

gram manager. Our standard procedure calls for the program manager to be fully responsible for the security in this area of assignment.

Many times a program manager will be the one best qualified to interpret the security as spelled out in DD 254 for the managers and for the supporting people who report to him. However, the fact that we make him a program manager, does not qualify him as a security expert.

So it is at this point that we expect him to avail himself of the services of our security department in carrying out his responsibilities. We have found no one who does not welcome our security department's offer of such assistance. I kind of make sure of that anyway.

At the outset of our classification management program, which we have now been operating for about three years, we concentrated on the major production contracts. And what it amounts to, is getting a member of our security department to meet with the program manager, with the engineering director, the security representative of that particular division (in my case I have 4) where the contract is being performed, and we try to resolve security problems that are identified at that moment in time, and the solutions are discussed. Ultimately, a knowledgeable engineer on the staff of the program manager is assigned the job of writing a security guide for that particular production contract. So every contract has its own security guide.

We have security guides prepared on all of our contracts. We have to update these, of course, and we must keep abreast of the changes in DD 254 requirements. I would say the big contracts run about thirty pages long. To give you an idea of what this amounts to, I will pick a particular air borne missile control system radar. This guide totals about twenty-four pages. I would like to read its purpose as it is stated in the guide.

> "To alert individuals working on the contract to the existence of classified information; to provide guidance as to where it may be encountered; and to provide an interpretation of and guidance in complying with the classification requirements imposed on the system. . . ."

Then the guide spells out the security interpretation for every security requirement on the DD 254.

In the next part of this guide we give the general rules on the contract that deal with drawings and specifications, identifying classified hardware, how to handle the classified hardware and that sort of thing.

We are then really able to achieve what I consider to be rather smooth flowing operations by having an authoritative interpretation of the security requirements of a particular system available in the guides. At any given time we may be involved in the design and manufacture of as many as seventy-five different systems. The security requirements vary from one system to another. Also, engineers vary among themselves, and security interpretation becomes quite a job. With a guide, we have found that this solves most of our problems. We have

these guides, incidentally, properly signed off by those who have the burden of security interpretation, and this way we eliminate the time consuming arguments as to whether something is or isn't classified. The final answer is in the guide.

The next area where we have benefited from classification management is in the procurement of classified hardware. In the same kind of control system that I mentioned, we have something like 200 end items or "black boxes" that we subcontract. Our security department determined that we were delaying our procurement because of time consuming procedures whenever a DD 254 had to be furnished to a subcontractor.

A rough idea would be given by running through one of these procedures. The manufacturing information writer pulled out a classified drawing. He went to an engineer and the engineer went to get a proper DD 254, and a few minutes later, another manufacturing information writer would go to the same engineer and he would have to form another DD 254. This went on to the purchasing department. And you know how all this paperwork goes on and on. We generated something like 6,000 DD 254s to sub-contractors on this one program alone.

The task, of course, is quite staggering. Oh, incidentally, I didn't put in the acting contracting officer too, who was on our premises, and he has to sign off. He practically goes through the same routine we did—his own engineering staff, interpretation, you know, and that sort of thing.

The problem was, I felt, properly tackled by our classification management supervisor. The program manager in this case agreed to make up lists of parts which would take the same DD-254. In other words, they would categorize all classified components into about five lists, and for each list we prepared a basic DD 254. These lists and the proposed DD 254s were then reviewed carefully and agreed upon by the ACO's engineers ahead of time.

Now, when our manufacturing information writer pulls a drawing all he has to do is look at the part number which gives him the applicable list, and then he goes to the proper DD 254.

Another phase of our classification management program is to closely examine requisitions to see if the item can't be purchased off the shelf.

As a result of consultations with the Naval Ordnance Systems Command, for example, we have authority to delete contract numbers or identification by nomenclature in order to eliminate classifying an item by association. Incidentally, this authority extends to all of our classified contracts under that particular command.

In Block 15 of the DD 254s that go to the subcontractors we specifically point out, for example, that "this unit becomes unclassified if the signature characteristics are not associated with the prime contract number and/or system nomenclature." I want to urge everyone to be alert to the possibilities of handling procurement

as unclassified if possible. Of course I might add this decreases the shipping costs to the Government. In one case, we have estimated that in one lot of 200 antennas we saved the Government $13,000 in shipping charges alone. Peanuts it might appear, but very important when you multiply that number by 100.

A third area that I would like to quickly cover deals with savings of security costs in the mechanized control of accountable classified documents. We used to do all of our recording, circulating and dispatching in a very manual and plodding and slow way. We designed a mechanized system, and at the present time in Baltimore alone, which is three-fourths of the total operation, we handle 50,000 accountable documents right now.

In addition to identifying these accountable documents by their acquisition numbers, we record them by contract number. And, of course, this means that when we have a contract close-out, we can readily identify every accountable document that's in the house pertaining to that particular contract. This is a tremendous timesaving advantage.

Of course another more important, I think, feature of our mechanized operation is to record the automatic downgrading dates of acquired or internally-generated accountable documents. So about every half year we get a printout of our accountable inventory and if no action has been taken in the downgrading, then the downgrading is flagged automatically.

The last and fourth phase of our classification management program may seem rather mundane and parochial, but to me it is a very important one. This deals with the stringent requirements for determining the necessity for a closed area. I am quite sure you are aware of the fact that in a large manufacturing operation a bunch of small closed areas certainly is an impediment to all of the operations. And I also have found that the program managers like to put in closed areas just so they can keep their own mistakes away from the careful eye of management.

We have seventy-five closed areas. I believe it's very important from the standpoint of good classification management that someone in management be absolutely certain that a closed area is necessary.

This determination and responsibility is vested in the security department. We have a Closed Area Request Form and Inspection Report, which has to be executed by the area supervisor, by the program manager, and finally, by the security department representative. It requires that the program manager sit down and say why he needs a closed area and put it in writing. As a matter of fact, it also says,—while we are at it—what classified components go in the area and, for instance, whether they are small enough to be stored during non-working hours.

We found that our security department sometimes can suggest ways and means of avoiding a closed area. This particularly happens when they have conferences between our security and program managers. We find that

much cost avoidance is possible in an area where you don't need a closed area. And there sometimes occurs some simple thing like putting dummy panels on the equipment and just put the real panel on when the item arrives in its final assembly area.

How much of a savings is effected when we have worked out something like this? It is very hard to say, but I do know that every closed area costs a lot.

I think it is important to note that what I am really trying to say is that there is much to be gained by having a classification management supervisor to take a look at these things, in writing, from his point of view. He comes up with, and he's charged with, solutions that people on the program who are concerned with the engineering, manufacturing, and product reliability simply don't think of.

In conclusion, let me restate the four basic points that I have tried to emphasize, First, we talked about a sound and specific interpretation of the DD 254 by means of guides. Incidentally, we have a letter from one of the user agencies expressing appreciation and congratulations for our efforts in effecting realistic classification guides for vital Navy programs. It points out that the results are both tangible and intangible and furthermore were most rewarding. We have, for instance, declassified all the components of the Mark 45 Torpedo system by some really careful analyses and considerations. In the customer's own words, he said: "The joint classification effort is an outstanding example of cooperation between industry and the Department of Defense and should result in substantial monetary savings to the Government as well as more effective production."

In the second area, the procurement of classified hardware from subcontractors, all I can say is I know that each DD 254 that these people were handling before cost me $15, and their not being handled certainly is a saving.

As far as the mechanized control of the accountable classified documents is concerned, although I know that the mechanized system that we now have is about $6,000 more in cost than our non-automated system, I know that by the automatic degrading that we are getting, and the foolproof way of splitting out the identifiable and accountable documents, we are saving much more than that amount of money.

Finally, I am sure you will agree that the security savings through being careful about closed areas is tough to estimate, but it's obvious that it's pretty good.

I would like finally to remind you from Paragraph 10a of the Industrial Security Manual, that: "Contractors are encouraged to advise and assist in the development of the classification guidance in order that their technical knowledge may be utilized and they may be in a better position to anticipate the security requirements under the contract and organize their procedure and physical layout accordingly."

We have accepted this encourage-

ment wholeheartedly. We feel that we have been successful to some degree, and it can go a lot more. And, incidentally, I do want to point out one thing—that you can't get this sort of thing done without a good alert staff (in our case a Naval plant representative) that is always attentive and responsive to our suggestions.

We also found that by getting our engineers personally involved in classification matters and getting in here to Washington, for instance—I am lucky because we are close to Washington—we get them much more sensitive to classification matters. We found that the classification officers here in Washington are interested in the same viewpoints as we are. Thank you.

PANEL—INDUSTRIAL ASPECTS OF CLASSIFICATION MANAGEMENT IN WEST COAST DEFENSE/AEROSPACE INDUSTRY

Richard J. Boberg, Aerospace Corporation, Moderator

A. A. CORREIA
North American Aviation

Ladies and gentlemen, it is certainly good to be back here again. I remember this fine meeting place here two years ago and all of the work that everyone here in the Washington area did to get the International Conference Room. It certainly is my pleasure to be here as a panel member to present the classification management program in Autonetics, North American Aviation, in Anaheim—better known as Disneyland, U.S.A.

I feel that to acquaint you with what we do at Autonetics I have to acquaint you with the Industrial Security Division.

We are a division within Autonetics Division of North American Aviation. We are divided into four separate functional areas.

Protective Services furnishes all plant protection, lock and key services and all other plant protection, throughout the plant.

Investigation does applicant review work, running investigations and checking on applicants.

Clearances, Audits and Accountability processes all requests for clearances, verifies facility security clearances on prospective subcontractors, and performs all incoming and outgoing visitor accreditation functions. They also manage the central document accountability control register and they have audit teams to verify proper accountability within all holding organizations with Autonetics Division.

This is a typical type of organization, from my experience in seeing industry when I was on the military side of the house; most industrial oranizations are pretty well patterned this way.

The final functional area, of course, is the one that we are interested in here today, and the one that I am most interested in, because we call it the Classification Management and

Program Support function. Now, this functional area is responsible for maintaining an updated security manual, updating and revising the company standard practices procedures, security education program, review of all proposed public release papers, and other papers to be presented at symposiums, and all areas of classified material handling, such as transmission, storage, disposition, reproduction, classification, marking, and establishing required controlled areas for classified hardware manufacturing.

As you can see, the Classification Management and Program Support area is what we feel a big area because we are the ones that basically support the customer and the contract, and the contract effort by our engineering areas within Autonetics.

There are six security representatives assigned to this particular area, and five of them perform the functions that I just mentioned to you, in supporting the programs. Some particular programs, just to name a few, are the Minuteman guidance systems, the F-111 Avionics, SINS, ILAS, ASCOR—a number of them. And, of course, there is our computer program that we are working on also in what we call Data Systems.

Each rep provides classification interpretations for his division, and prepares all 254s and 254-1s for subcontracts in his program support area. In my case, I support the Minuteman program with special support areas of Cryptographic Security Officer for the company. I also support the Atomic Energy Commission contracts that we are presently working on. Actually, they are Sandia Corporation contracts.

My responsibilities are to interpret the security direction furnished by the customer and write a company guide with all the details necessary to protect National Defense Information. As an example, the Data Systems Division (DSD), which works computers primarily within Autonetics, supports Minuteman in the computer area. They support the Minuteman Division, which is my primary division. Constant interface between the security reps on programs is a function which we have got to have. Otherwise I would be going into another man's area of support, such as Data Systems, and he wouldn't even know what was going on. So we are constantly interfacing and exchanging ideas.

Now, Minuteman in this case is the lead division. So we establish the criteria. We assist the security rep from Data Systems in writing the 254s. And actually, as was brought out here yesterday, it is a team effort. It is a team effort between myself as the program support rep, the other security reps supporting the Data Systems, and the engineer, and anyone else that we need to bring in from a standpoint of writing a good clear 254 or a 254-1 for subcontract. And this is done immediately after the buyer establishes a requirement with the other division, the other part of security, indicating they want to know what the facility clearance is of a number of different contractors because they are going to place a subcontract with someone.

When we get the buyer's notification that he has selected a subcontractor, immediately then is when we

prepare the 254-1 or 254, whichever applies.

All the security reps are required to sit in on technical direction meetings and technical interchange meetings within Autonetics with the customer where a change in the required controls are necessary on a piece of hardware. We have had it happen a number of times that hardware we were presently working on was upgraded because of configuration change, in a couple of cases from unclassified to secret, and from confidential to secret. And certainly this changed the requirements for security. It changed the requirements for controlled areas. It changed the requirements in many concepts in purchasing areas, subcontract areas, and there is quite a bit of effort. So only through sitting in on these meetings, technical interchange and technical direction meetings—again, a team effort—only on these occasions can you really get the information you need if you are going to give classification support and write good, clear classification guidance to your subcontractors.

All the security reps have different programs, as I say, to support. As the Minuteman program support rep, I support it regardless of where it is. In fact, yesterday at noon I got called out to our Autonetics field office here. They had some Minuteman problems, and I was over there for a couple of hours.

I have to support Minuteman at Cape Kennedy. If they have any problems I have to go out there. I support them at Vandenberg. In the cast of 254s on contracts on the Minuteman, I see that field offices get copies so they will have updated direction. I see that they can make changes to all of the security direction received, to make sure they are right up to date, and that when their cog people come by and run their inspections they have all the information on file that's required. In addition, I go to Hill Air Force Base and Newark Air Force Station, and any other field office that is established to support Minuteman. I am the security rep that is notified in case anything comes up.

Finally, all the security reps interface with the sixth man. There are five of us that are program support, and the sixth one is our contract closeout man. We receive what we call a Contract Closeout Inquiry (CCI) from the contracts office. When the security office receives this form this particular rep coordinates with whatever program that contract was on whether radar, guidance, computers, Minuteman, or whatever it was. The two reps, the contract closeout man and the program support man, immediately start taking action to determine how many classified documents we have charged to that particular contract.

Our classified document accountability register codes all accountable classified documents charged against that contract. And when the closeout comes, all we have to do is go to the computer and tell the computer to give us a tab run of all of the documents that were charged to that contract. And then we start our justification for individual holders for retention authority, if we have to ask for retention authority.

Again there is coordination necessary with the document accountability

register people, to be sure that they don't assign a contract code number to a maintenance and repair contract. I found that they did do this. And engineers are strange people. I have been dealing with them for quite some time in both areas. If they get a number in their heads like 0348, which was a good example, if they get a number in their heads, every document they write when they call in for a control number they will give 0348. So we had a maintenance and repair contract that we should have been using other documentation on, and instead every new document they generated they charged it to 0348. When we came for closeout on this contract the contract had 248 documents charged to it and it shouldn't have had one.

After we coordinate with all the holders of the documents and we get justification from all of the people we consolidate this, give it to the buyer and the buyer goes to the customer for the contractor's approval and retention authority. After we receive the retention authority each document retained under this particular authority must be annotated on the front cover or the title page with the authority for retaining the document, the period of retention, the date of the authority, and the headquarters or agency that issued the authority. In this way, every document in our files is either on an active contract, and is marked as such, or it's on a retention, with a specific period for retention.

Again, one of our responsibilities as a security rep is that if we get retention on a particular contract we have to see that we get the continuous guidance in case there is any change in classification.

In this case, as you can see, we are constantly with the engineers. And it is fortunate that I know a number of people in the business, like Elmer Yost here. And certainly I know my replacement at BSD. I have been able to just call people. We have a suspense system on 254s that we use. And we get them. Either that or we get a 254-1 that tells us there is no change.

We have had no difficulty. It has worked real well. But all of the reps, of course, have to be constantly with their program. As we say down there, "You have got to get out among them if you want to let them know you are available to them." There are many details, of course, that I haven't been able to discuss here. But there are a couple that I would like to bring out. More and more we are getting into a situation where concepts are classified or associations with things are classified, and really the hardware in itself is not classified. Certainly you all know that hardware is not classified; it's just a bunch of garbage. But then when you put it together, it reveals classified information. In one case, our buyer was going to go out and he got verification of facility clearances of cleared contractors that could do this particular job for us. We almost didn't catch this one, but fortunately we did. We were ready to go out to a cleared contractor for a particular job. The job was secret, and really it was just an association or concept thing. Actually, there were ways in which we could send this job out without relation to program. From the cleared contractor, the cost on the

first two units was $2,000 each unit, and $1,800 for each unit after that. From the uncleared contractor the first cost $854, with a learning curve reduction as the units were processed. Well, through a means of identifying and controlling the manner in which the hardware went to this uncleared contractor—and this was all approved by the customer—we saved some $67,000. This was a cost plus incentive fee or CPIF contract. Certainly the customer was very happy about something like this, and we don't feel that we have compromised the program. In fact, we know we haven't. But the one thing you have to be careful about in something like this is that the contractor doesn't relate the program through his financial records. We had to make sure that we had a cutoff in the financial records to not relate that effort to a particular purchase order related to Autonetics which would be related to the program. But this is one of the things. In fact, there was one of the gentlemen here that I was talking to about this. We were discussing this yesterday, about the cutoff within a financial area, to make sure that you don't compromise the program by associating and relating. In another area we did the same thing and it was a savings of $50 a unit by being able to manufacture the thing as unclassified. In one area in Los Angeles, one contractor has approval by the cog office to manufacture an item in an uncontrolled area with regular manufacturing people, no clearances or anything. But the particular piece of hardware doesn't pick up any identity with a system, and actually it's a travelling wave tube, it doesn't pick up any identity with any system or any program until it goes into what is called a bonded area. And this tube could be used in many, many systems. It can even be used in television industry. So the people in the manufacturing line don't know what this thing is being put together for. When it picks up an identity it is picked up as confidential. In fact, they are doing this for us on a subcontract.

Classification management is something that you have got to be with constantly. Thank you.

GEORGE L. CHELIUS
Douglas Company, McDonnell-Douglas

In describing classification management at the Douglas Company I will address myself to six areas.

First is the use of classification committees. We feel that by the use of classification committees we have unanimity and agreement as to exactly what is or what is not classified under a particular contract.

Secondly I would like to discuss an area that is of grave concern to our particular corporation, and that is our work on independent research and development. This is constantly a problem. Our management has directed me to study, and has taken a considerable interest in exactly what information in independent research and development might become classified.

I would like to go into, briefly, our regrading and declassification system. We downgrade on an average of 700 to 1,000 documents a month through our automated system. We are also concerned with contract terminations,

the public release of information, and an educational program. The application of a security classification to information developed by Douglas personnel, as in the case of other contractors, is based on classification guidance furnished by the contracting officer or the user agency consistent with a DD Form 254, a security classification guide or letter in lieu thereof. It is also based on the individual's knowledge that the information is in substance the same as, or would reveal, other information known to be currently classified. The engineer/scientist is responsible for determining the classification of information he generates. I would like to emphasize that. We have found that a security specialist does not always possess the technical background from which to determine questions of classification. But we in classification management can guide the technical employee to the path of proper classification management by extracting from him through the use of questions and comparisons the essential information that requires assignment of pertinent classification elements.

To assist the technical personnel a classification committee is formed or is established for each major contract or subcontract to ensure uniform implementation of the security guidance furnished. The classification committee consists of the manager of security as chairman, a contracts representative cognizant of that special contract or weapon system, and a member of the appropriate engineering projects office or design section as specified by our administrative chief engineer. The classification committee convenes at the request of any member of the committee or as soon as practical after the receipt of an original Security Requirements Check List or revision thereto.

The committee is responsible for the review and interpretation of the original DD Form 254, or revision, and establishes detailed security classification guidelines for the contract concerned. Where it is determined by the committee that clarification of DD Form 254 is indicated, the contract representative is responsible to negotiate with the appropriate government agency to obtain a revision or clarification. The manager of security maintains a liaison between his office and the user agency's classification management offices. This liaison helps us understand the Government's philosophy in classification, and also assists in maintaining consistency with other user agency programs or contracts. Upon the committee's approval of the Security Requirements Check List, the security office distributes the check list in accordance with established distribution.

In addition to technical personnel —and I am referring to distribution of the check list—in addition to our technical personnel we also distribute check lists to all levels of management, all vice presidents, senior directors and directors, including our marketing, management, planning, and other supporting functions.

In addition to major programs we receive a number of smaller research contracts for which it would be impractical to establish such a committee. In this situation the manager of security and the technical personnel

function as the classification committee. In regard to these contracts the technical personnel quite often call upon the security office to provide classification guidance based upon our knowledge of other information know to be currently classified.

A major effort in classification management is directed toward our Independent Research and Development efforts. Basically our IRAD program does not stem from contractual relationships and therefore, under the existing Industrial Security Manual, would not require the assignment of security classification. However, our experience has indicated that IRAD programs are the base for advances in the state of the art. Further, it is specifically directed towards the Air Force's Technical Objectives Documents, the Navy's Technical Area Plans, and the Army's Qualitative Development Requirements Information Guide. Through these programs the contractor is encouraged to respond to various technical areas of interest by the user agency. It is interesting to note, for example, that the Air Force's TOD program has thirty-eight individual books, referred to as technical areas of interest. Of these thirty-eight, eighteen are classified by the user agency. Therefore it must necessarily follow that the user agency wishes to protect certain information not related to a government contract in the interest of national defense. Accordingly, certain aspects of the contractor's Independent Research and Development program could be classified.

IRAD is a program identified as an entity for a contractor which does a significant amount of Government business. While the program represents a contractor's independent technical effort the costs are shared, usually on a negotiated basis, by the Government, who benefits from the state of the art.

At Douglas we have taken additional precautions to establish a classification committee for all information generated under our independent research and development programs. The committee consists of the deputy director of research and development and myself. Each quarter a judicious review is made of the 160 individual projects within the IRAD organization. This review often includes a discussion with the principal investigator, engineer/scientist. In this review we include discussions with the principal investigator of the project to ascertain his feelings concerning the classification of the work he has in process.

When the committee determines that information generated under our IRAD program could represent a significant military advancement, a tentative or pending classification is assigned to the information, and it is forwarded to the responsible user agency for determination. In some instances it is not necessary to forward such information for a determination because it was properly classified by the principal investigator based on his knowledge of the current state of the art and his recognition that such information is, in substance, the same as, or would reveal, other information known to be currently classified by the user agency.

In other areas we have also found

it necessary to establish classification committees. These directorates are basically responsible for supporting management planning. The personnel involved in gathering planning material are not always technically oriented and therefore occasionally desire classification assistance in making their determination. These support organizations find it necessary to call upon their committee representatives to assist in a classification determination.

The classification committees play an important role in review and reclassification of information upon receipt of a revised Security Requirements Check List. After approval of the revised Form 254 the management of such functioning department or engineering project office designates an employee to be responsible for the review of the following types of classified material: engineering drawings, documents originated by the engineering project office or design section, or documents received or distributed by an engineering project office. In any case, when the reviewer or originator is unable to make a determination regarding reclassification of the documents, assistance may be requested from the classification committee chairman.

Our secret document accountability system is an independent function of classification management. However, both functions are closely related. For example, our secret document accountability system is fully automated. Our control cards provide spaces for recording contract numbers or subcontract numbers, RFQ and RFP, document date, and regrade codes. When a document can be downgraded under the time-phase provisions of the Industrial Security Manual the tab run automatically indicates such action is necessary. The tab runs are distributed to our control employees on a monthly basis for the necessary downgrading action, in addition to the required inventory.

Another significant benefit is derived by the use of contract numbers. For example, at the termination of a contract we are able to locate all accountable classified information generated during the contract performance.

Secret document accountability obtains a printout of accountable material by contract number from data processing. This tab run is forwarded to the contracts termination manager who is responsible for coordinating destruction of duplicate copies, and obtaining retention approval from the user agency. To date we have found that this process has been well accepted by the user agencies and seldom is retention denied when we can justify our need-to-know.

We also monitor the public release of information including foreign release of information within the purview of the International Traffic in Arms regulation.

When our technical personnel generate papers for public release at a symposium or seminar it is the responsibility of our public relations representatives or personnel to obtain the necessary user agency approvals. Before requesting user agency approvals internal approvals are *required* from patents, marketing, our corporate public relations, our divi-

sion public relations and the cognizant vice president in charge of the engineering group (in the case of an engineering paper). In the case of an advertisement, it is the responsibility of the group vice president to approve it.

Each approval throughout this process certifies that the document has been reviewed for classification and found suitable for public release. The function of classification management is to monitor these procedures and provide recommendations where necessary and when requested.

The last aspect of our classification management is by far the most important. It is primarily an educational program developed to assist management and engineering and/or technical personnel in the principles and functions of classification management. We specifically define the terms used in classification management, the types and levels of classification, the classification authority, the considerations upon which to base a classification determination, and a basic review of downgrading and declassification process.

We hold classified technical discussions with various engineering project officers within our facility. We also brief management and supporting groups, those that have a need-to-know, on a classified basis, concerning information that we generate or that we feel is particularly significant from a standpoint of security classification.

I think that in summary, then, we have a unique system in the use of classification committees wherein we tie contracts, engineering and security together. This presents a united front and has proved most effective in our organization.

We are continually concerned, as I mentioned earlier, about our independent research and development. However, the deputy director of research and development we have found to be most cooperative. He has taken trips to the Washington area and to BSD to talk about classification management. He is very much aware of the problems of security and the need to apply classification to certain independent research and development information. I must stress, however, that the life blood of a corporation—a profit-making corporation—stems in part from its independent research and development.

Therefore, gentlemen, especially those of you in the user agencies and the Department of Defense, it is most important, if the contractor is going to classify information that he believes is of significant military advantage under his independent research and development program, for you to provide a means of communication between the scientists of our corporation and those of other corporations and those in Government. At the present time, we have been unable to establish or find this channel whereby we might communicate in an interchange of information with other technical personnel in other corporations. I think this is an area demanding your attention. I am sorry to be so forceful but I am pretty concerned about it. It demands your attention. We do want to protect information but you must provide the scientist and engineer with a means of communicating his ideas with those

of other interested members of the scientific community.

In closing, I would like to address myself to one other area. We come to a symposium such as this and we hear about some of the faults and some of the complaints, you might say, of various organizations with the classification program. I think this is justifiable. However, I think a great deal of credit should be given to the members of the user agencies, to the Department of Defense. I have been with the program only two years. Dr. Welmers, last year in Los Angeles, suggested that the scientist feels like asking the classification specialist, "Won't you walk a little faster . . ." Well, I think that classification management within user agencies and the contractor is merely a reflection of the guidance that the user agency or Department of Defense wishes to impose upon it. I think that we are catching up. I think that we are traveling faster and in a straight direction to where eventually, perhaps in the next two or three years, science and classification management will be on an equal or par with each other. I think that a good deal of credit must be given to user agencies and the current attitude within the Department of Defense.

JOHN W. WISE
Hughes Aircraft Company

Good morning, ladies and gentlemen. I have only been in Hughes Aircraft Company for a very short time, something less than three weeks. About two weeks before I terminated from my previous employer, the fellow I work for at Hughes now called up and said, "John, how would you like to go back to the NCMS conference in Washington?" I said, "Fine." He said, "Well, I thought you would. We volunteered you to give a talk there." I said, "Thanks a lot, Pete. What is the subject?" And he said, "the Classification Management Program at Hughes Aircraft Company." I couldn't very well back down since I had already given my termination notice to my old employer. So here I am.

I did manage to learn a little bit about the program. When I speak of it, naturally I am not speaking of things I have done in three weeks, and my talk will necessarily be a little more general than some of the other members on the panel. I am going to explain what has been done to date in classification management within the Hughes Aerospace Group and what we plan to do in the future to develop an expanded comprehensive and effective program.

In order to illustrate the magnitude of the job facing us at Hughes, I would like to give you a very brief sketch of the company.

Hughes Aircraft employs over 32,000 people. The hub of our operations and the location of the great majority of our people is Culver City, California, and the greater Los Angeles area. The company's space program accomplishments have included the Surveyor, which was the first USA spacecraft to soft-land on the moon, and SYNCOM, which was the world's first synchronous communications satellite. Other major product lines, of course, include several kinds of Air Force, Navy, and Army guided mis-

siles, radar and computer systems, and air defense control systems.

The organization in which our security department, and my function, is located is the Aerospace Group, and we employ approximately 22,000 people. Our group is organized into five product or engineering divisions, two production divisions, a flight test division, and a field service and support division. Each of these has its own semiautonomous procurement and contracting organizations. As of 31 May 1967, we had 266 active classified prime contracts. Approximately fifty percent of these were Air Force, about twenty percent Navy, ten percent Army, a very few NASA classified contracts and about twenty percent that are commercial or with other DoD contractors. These include both research and development and production contracts for several major space and guided missile programs as well as a variety of research projects on laser, infrared, radar systems, and various and assorted electronic developments. In addition, we have 127 active classified subcontracts, and these involve the same variety of work as do prime contracts. In view of our span of control considerations, the number of people involved, the variety and complexity of the products we market, and the numerous customer agencies we serve, we feel that we have quite a challenging job in upgrading our classification management program.

What kind of a program do we have today? We like to say that for the past four or five years we have had about the same sort of program as have the majority of other large DoD contractors. And if that statement is not vague enough for you, I will try again. But seriously, we feel that we have complied with the Industrial Security Manual on matters relating to classification requirements. But we have not necessarily pulled the various individual actions necessary to effect such compliance together into a central program, nor have these functions necessarily been performed within a central organizational unit in the company or in the security department.

We have kept files of all prime contracts, including DD 254s, to be able to answer classification questions as they arise (also, I might add, to meet the DD 696 inspection requirements). These DD 254s are reviewed as they are received and, whenever it has been possible to obtain additional guidance from customer agencies, it all has been translated into a Hughes format for classified guidance for our employees. We have not attempted, to date, to control or limit the distribution of 254s throughout the group and, therefore have experienced some controversies, as many of you may have, resulting from various interpretations, and have had to arbitrate these controversies among our technical people. We confess that we need to increase our efficiency in this area.

A unit of our department is presently concerned with the preparation of DD 254s for subcontracts we award. These have customarily been extracts from the prime contract 254. We do keep suspense files and we attempt to keep up with the requirement for annual revision of DD 254s.

As to classification review, we have a member of our organization who concerns himself with reviewing material for public release within the meaning of paragraph 5n of the ISM. And we have also reviewed other material periodically upon request. Beyond that, we have not, in recent years at least, been undertaking any large scale classification review.

To sum it up, we feel that we have been in compliance, but that we can do a great deal more. Within the past two years, our Aerospace Group management has become increasingly aware of the need for a complete and coordinated, centrally managed, classification program. Finally, this Spring they became convinced of the need to emphasize and accelerate development of such a program. And that is why I am there at the present time. So we have a "go" signal now. It's up to us to produce. We have convinced the management and now we have to show them some results.

So how do we plan to improve our program? Well, as a starting point, we are going to draw up a long range time-phased implementation plan to insure that the various elements of the program are pursued in a specified order of priority. So I will discuss some of these capabilities we plan to accomplish. They are not necessarily in the order in which we plan to accomplish them.

We feel it necessary to firmly establish the classification management office as the font of all classification expertise within the Aerospace Group. We also intend to establish it as the central point of contact for all activities outside the company and for all outside agencies we deal with: customers, cog agencies, DCASR, classification people, and what have you. We feel it particularly important to develop a good rapport with our major customers and to gain their confidence in our program as it develops.

As to prime contract 254s, we are going to develop the capability to review all of them as they are received and judge their adequacy. Further, we intend to prepare a Hughes format classification guide for all of our programs and to dry up the distribution of 254s within the company—for general use that is.

We will, of course, develop and schedule educational programs as necessary to supplement our classification guidance.

In the subcontract area, our goal is an ultimate capability to prepare detailed 254s for all the classified procurements made from our engineering divisions. And this may well be the most difficult part of our program to accomplish simply because of the volume of work, the number of people we deal with, and the number of divisions of our own we have to deal with.

We feel, however, that the subcontracting area is a most important part of our security responsibility and we intend to develop techniques and procedures that enable us to monitor our subcontractors' compliance with their 254s. We are convinced that this is an inherent part of our prime contract management responsibility.

At the present time, we have a sizable classified document inventory. We have approximately 50,000 secret

and an estimated 250,000 confidential documents in our inventory in the Aerospace Group. We plan to institute a systematic review program as soon as possible. And, of course, we will concentrate in the beginning on the secret documents because these are the category that costs the most. We estimate that over a period of time we can significantly reduce the inventory through downgrading. We are pretty positive of this. We are going to undertake the review of more original material and we feel that this, coupled with better and more detailed guidance to our employees, will result in a fewer number of secret and confidential documents being added to our inventory. Finally, in the area of classification review we intend to strengthen and expand our capability to provide classification support and analysis in the proposal area.

I like very much Ken's explanation of the way they do this in Sylvania. I think it is a very good approach.

We know the effectiveness of our program will depend on how much and how well our employees use us and how they comply with the classification requirements as we present them. Therefore, we have planned an aggressive publicity program. We will gain exposure via the company newspaper, participation in management staff meetings, posters, flyers, any way we can spread the word, plus a series of regularly scheduled orientation talks to reach all our employees, to let them know who we are and what we can do for them. Of course, by the time we get to this phase of the program we have to have established a good capability to be able to react and make our services available.

As to manning, we know that the scope of the program we have outlined will be and is more than a one man job, but to date we haven't attempted to crystal-ball any ultimate requirements. Instead, we try to identify through this long-range plan just why, when, and how many additional classification specialists will be required.

This concludes the formal portion of my talk as I prepared it. This is how Hughes is facing up to the classification management program today. I hope it has been of some interest to you. I would like to be able to return in a year or two and give you a progress report.

I wanted to just ask whether we might generate some additional discussion in suggestion fashion here in a couple of areas. One is in the document disposition aspects on contract completion. As a matter of interest, among the people out here, how many of you deal directly or have a direct part in these proceedings of requesting retention authority or disposition authority upon contract completion? The reason I asked, it is of some interest to us. In some of the companies we know of, it's done by contract administrators and what have you. We have found through previous experience that it is advantageous for classification people to become involved in this. It is, in my opinion, just one other means that you can keep a handle on the whole area of information, document control, and what have you, within your company. Of course it is all something

that we know the cog agency people throughout the years have had a lot of trouble effecting compliance with, and apparently they still are. If that was an accurate show of hands, I think some of you are overlooking an area that's most important. As illustrated by Ken's discussion yesterday, this is how you can get in on things from the very beginning and follow them through from birth to death, so to speak.

There was one other thing I wanted to ask yesterday when we had the DoD representatives up here. I wasn't able to because we ran out of time, as you will recall, but I did talk to George MacClain about it later. It might be of some interest to you. I am sure George won't mind me mentioning this because it wasn't a private conversation in any sense. I was interested to note that when Bob Arnold was discussing a team concept within the Air Force now, he made a passing mention of an intelligence member as a member of his team. And it has always been of concern to me and to people who have been in classification for a number of years that we have a definite void in this whole classification business, and this is that we are unable to apply any intelligence aspects to our classification considerations. By this, specifically, I mean we classify certain articles as secret, pertaining to a certain weapon system, and we don't know but that the Russians have had this in production for two years. And if they have, we're wasting money by classifying our actions in areas like that. So I asked George about that and apparently it is something they are still working on. I think this is the most serious omission in the program and a basic consideration. And as my contribution, recommendation-wise. I would certainly urge that this loophole be closed soon. Thank you.

ALFRED DUPELL: I would like to make one short comment on a comment that you just made, Mr. Wise. As PCO from a user agency, we do try to do exactly what you suggested on cranking in the intelligence so that we get some idea where the other side of the fence is when we write security. Unfortunately, my office, like the office of most people writing DD 254s, isn't staffed adequately and never will be to keep up with all of the intelligence take. So we try to get it in compendium form and there are several agencies here in town that can provide it. I think that just about all of us, at least here in Washington, do try to crank in intelligence on our DD 254s. It does help. I concur with you completely on that. I have two questions for Mr. Correia. On your computerized systems of document control, do you crank your confidentials in?

CORREIA: No, we do not crank in the confidentials. The only time we control—actually control—confidential is on proposal activity. From the time the proposal comes into the company we include all classified so that if we are unsuccessful or if we no-bid we can be sure that we can return or dispose of every bit of it. In just a rough check, from the time that I have been with the company—and we are attempting to clean this up right now—we have 5,000 or more documents on all proposal activity in

which we were unsuccessful and no real positive action was taken to return this or to destroy it and certify to the prospective customer that we have destroyed it. And engineers—they are the same in the military I found when I was with BSD—they are pack rats. They want to keep this stuff "just in case." I know the first or second year I was with BSD we started a program and we destroyed in six months tons of classified documents from the Atlas program that were absolutely useless. This was in some 300 plus storage containers. We do not control the confidential except in the proposal activity. But to add a little more to your comment there, we instituted a program in BSD when I was there that wherein if the engineer was not completely familiar with the up-to-date state of the art technology, say in the electronics or in the reentry vehicle area, we did call in the foreign technology people. I know engineers are constantly attending seminars and symposiums, and we in classification management need to do the same thing. And this is how they keep up their knowledge of the state of the art in a particular field of technology. We found quite some time back that in the area of liquid propulsion—with what the Russians can put up with liquid propulsion—our liquid propulsion technology we don't have to worry too much about. And foreign technology people made many comments that it's absolutely useless to classify this kind of information, because others have got just as good—in some cases better. That foreign technology man can play a real key in putting a 254 together. Certainly the customer has this benefit. The contractor can go back and ask the customer to coordinate with foreign technology. We did in a couple of cases on some contracts and it was very beneficial.

DUPELL: I have one more question. On the retention of classified documents, what we have been trying to do from my agency is to transfer the accountability of these documents to a contract which is in current use, your latest contract, in other words. On the retention authority letters we send back, we direct that the accountability will be transferred. Does this create any problems for you?

CORREIA: Well, I can give you a prime example. Again getting back to the term "pack-ratting," we actually had a contract that was closed out and we went to the customer and we asked for retention authority. He said pass it or put it onto another contract. Well, what happens eventually, if you keep adding to this contract without proper screening, you end up with a couple thousand documents charged to a contract. And then what happens when you get that contract for closeout? You've got a mess. So what we did, we got down to a point where, through screening, we eliminated 412 documents that we really didn't need because they were available through DDC, through the technical agencies that you can get this from, and actually we kept seventy-two documents on the particular contract, and we did use the contractor's recommendation to put it on a present active contract.

DUPELL: That's no problem?

CORREIA: No, none at all. All we do in our case, with our control

—and we have the same control that George mentioned here—we have a contract code, a group marking, classification, and everything identified on our control system in the computer, and we just change from a 0348 customer code number, put it to the new customer code number, and the cards all drop out of the computer and go into the new system.

CHELIUS: We have a little different system. We continue in follow-on contracts to carry each contract document in our control system, and then, say if we had five follow-on contracts we would have five individual listings which would, if we still wanted to retain the material, go in for retention under the five separate contracts, showing that each one had been granted retention under the updated contract.

DUPELL: I have one other question on that. If we authorize retention of a contract that is dead, completely closed, then according to the Industrial Security Manual and the Industrial Security reg, we have to update your DD 254 each year for as long as you keep it. It was our intention--and I would like to get an answer from the panel or anyone else on this—in transferring accountability to a current contract to eliminate the necessity for bringing DD 254s up to date each year on dead contracts. Are we doing this when we transfer accountability? Ken, can you answer that?

KENNETH WILSON: Yes, we are very happy to see a user agency take this approach, Fred. We have a similar system to Tony's in that we go into our computer with a new project number, which is assigned to each effort, and it automatically changes all the documents under the old number to the new number. It is one of these microsecond type operations in a computer. It does mean that we get away from having to have the suspense file on whether or not we have a current 254 on an old contract that's long gone. So we find no problem with it and we like it. It reduces our paperwork. And we also take a step, as Tony indicates, in that we allow ourselves only one copy of any document received from an external source and not more than two of any document that we generated ourselves to transfer to that new contract. This is a self-imposed thing by management. There is only one copy in the library and one copy probably in the follow-on project manager's office and that is all that is allowed, so that we don't get this pack rat buildup that Tony is so worried about. That worried us, too.

BOBERG: We all have that problem. I might comment in passing on something that I think might have become obvious to you. I didn't review these presentations before we got started here, but one thread seems to follow. It was Dr. Hammer, I think, the other day who was talking about the 9s. It's not a hundred percent case but I know there is a prevalence of it, and that is the EDP document control system of one form or another that seems to be prevalent among the firms that are represented here. And I think these are many of the larger firms. I think that those of you who have to do with your document accountability and who have

not gotten together with the folks that have EDP, and tried to sell that type of system for your document control are missing a bet. As Ken knows, we at Aerospace Corporation designed such a system for the primary and exclusive purpose of accounting for secret documents, and it does it very well. That went into effect in 1963. Since that time we have been able to use that system without additional expense—or if there was any expense it was very limited—to help us in our classification management program. You can do a great many things, such as identifying documents for which retention needs to be requested on the cancellation of contracts. It's a very simple programming process to have it show on your printouts that documents require downgrading under the automatic downgrading system. This a point I think you might be taking from all this.

JAMES BAGLEY: I have a question for Mr. Wise, just for my own information. I know that Hughes, particularly in the tube division, has a considerable IR&D program. Is it your intent in the future to include classification management input into the IR&D program as used?

WISE: I don't know if I can answer that very explicitly at this time. But from past experience, I would say yes, you should apply it, and can apply it with much benefit in the independent development area.

ELEANOR JOHNSON: I would like to know how is the accountability maintained on DDC documents—the first gentleman, please.

CHELIUS: Where received on particular contracts they assume the contract number in our automated data processing system of the contract number of the user agency regardless of what number they are generated under. If they come into our technical library, however, they do not assume a contract number. We indicate that no government contract is involved. Before indicating this, however, the manager or requesting individual must certify that he is doing this not under a Government contract. If it came in under any Government contract then we would indicate the Government contract and the documents would be destroyed when the contract terminated. So we have a fairly good handle on the DDC documents. Now, there are some basic documents we use for research purposes that we do not put contract numbers on because they are pretty well applicable to most systems. Guidance is an example—some of the guidance areas. We have the SLV2, our Thor missile, we have the Spartan program, some of these various programs, and we may want to study guidance on more than one program and it would be inappropriate to destroy some of the information. If at a termination of contract we referenced all DDC documents to a contract, then eventually we would destroy all of them because we really couldn't justify retention on a follow-on contract. So for some of the general information we feel is applicable to a number of programs, we indicate there's no Government contract. The engineer/scientist has to certify to this, and they go to our library. Furthermore, any document—and this is

a directive from our general manager —any document that is not circulated or used, charged out to an individual or not circulated within the company for a period of six months must be destroyed.

CORREIA: Let me add a comment to what George just talked about, and I am glad you brought that question up because it reminded me of a point. You know we in industry have a real problem with field-of-interest registers. There is not enough thought that goes into whether or not in a contract the contractor is going to have a requirement for field-of-interest register. Now, we don't expect them to fill it out. Our library people fill it out. But if they will just check whether or not it's authorized, we fill out the field-of-interest register from our library services, it goes to the Air Force plant rep's office and if it's authorized on the 254 they sign it off and send it to DDC and we start getting documents. But if it is not authorized, the Air Force plant rep will not sign off a field-of-interest register, so we have to go right back through this whole chain again, go back to the customer and say, "Would you please authorize field-of-interest register on that 254 for that contract?" So there is some thought that has got to go into that 254 or that field-of-interest register requirement that is on the 254. You can't just check "yes" "yes" "yes" or "no" "no" "no".

DUPELL: I have got to defend the Government on this one. This is one time that I have got to admit that I am one hundred percent with George MacClain instead of fighting him. He changed the DD 254 form. And instead of all of these columns that were on the old form now there is a simple little thing that says DDC field-of-interest register may be approved or is approved. We check it yes or no, anyway. Either you get it or you don't. For the last twelve months I have probably chopped off about 1,000 DD 254s that said yes. Another question I had for you though, Dick: on DDC documentation, which is a heck of a headache to us as PCOs, how do you correlate this when you get DDC documentation on the long range scientific and technical development program? How do you handle that in your company? You know you don't get these on a contract. You are spending company funds under this long range development program. We do authorize access to DDC-4. How do you tie those in with the rest of your classified inventory?

BOBERG: I think the only answer I can give you, Fred, is the same as George did. We don't necessarily try to associate DDC documents with a contract number. Perhaps if we have a contract number it is a phantom one for purposes of our document control system. I think essentially the answer is we don't correlate that in that sense. Does that answer your question, Fred?

DUPELL: Yes.

BOBERG: And I think this represents a cross section of the panel.

DUPELL: Incidentally, there is a loophole in our retention program, George.

MacCLAIN: We went through the business of first of all dropping the reference to the DDC out of the pro-

posed revised 254, but it's back in. The people who operate the DDC and who are responsible for the policy for the DDC know perfectly well that the 254 is not a field-of-interest register in and of itself. It's not an authority to get anything, in itself, as far as the DDC is concerned, but they do wish that both the contractor and the user agency will face up to the problem at the time of writing a 254, and remind everybody of the existence of the DDC. One of the things about the DDC is that it is of no value unless people ask it to produce some documents. For this reason, the people who are responsible for the DDC insisted, and we went along, that this reminder be in there. Now, I think we all have to recognize the fact that when a 254 is being written you simply cannot foresee with accuracy whether the DDC will or will not be required. Nevertheless, the form is going to require a yes or no answer. I don't know how it is going to work out. But our instructions say that if you do put in a "yes" then the user agency is asked at the same time to fill out a field-of-interest register form and send it in, which means that if they can at that time anticipate the field-of-interest that goes with that register they will take that step concurrently with putting out the 254. It is a separate document, however. So much for that. Now, I am wondering how, in connection with your independent research program, you are able to establish an authority to obtain DDC information when you would have no contract with which to relate it. You can't get into the DDC without an FOYR. Who provides FOYR for an independent research program? And if it is provided by the authority of one of the military departments then I should think you would have to attribute it to that department in your records. And I would also think you would have to have some kind of a program for controlling retention of those documents for periods of time. I ask these questions without expecting answers. I don't know what to do about it. I think this is the question Fred was getting at. You build up a retention of DDC documents which are unrelated to any contract, and I don't know what you do with it.

BAGLEY: In the first instance, Fred alluded to the long range scientific program. A basic requirement of the program itself is that there be a project number. For example, I have quite a few of them. It's essentially a contract number—53124, whatever it happens to be. So, in fact, you can tie down the IR&D program that has been authorized by the Government to a specific project number. Then within that, if you extend it, you would have additional project numbers.

CHELIUS: Jim, what security guidance do you furnish with your independent research and development program?

BAGLEY: This is a void that we were talking about yesterday, because under the basic terms of the basic program the only requirement—and someone correct me if I am wrong—is that the person or organization be a potential contractor. Obviously, an organization or firm doing work of this sort cannot predict accurately

what Government organization will be the final recipient of a proposal. So guidance in this sense, I think, has got to be on an *ad hoc* basis so that a communication can be established. In one particular case the probability will be that the corporation will file a proposal to the Air Force even though we, the Naval Research Laboratory, authorized the program to be established in the first instance. But you see, the kicker is that we, too, are working for the Air Force, in this sense. So, I don't think that you can furnish any particular positive guidelines, but in each one of the cases that I am referring to it is a specific carry-on of work that had been done specifically under contract to us. Therefore, the guidance that we had under the old closed out contract is directly applicable to this. But this is about the only thing that I can say. It's a real void, I'll tell you.

CHELIUS: One of the problems within the technical community, and I think this is basically our responsibility, is that an engineer feels that if he writes a particular program name on a document, such as Spartan or Titan, then it assumes an identity with a program and becomes classifiable. And yet I submit that certain information within the Government and within industry, certain concepts, should be classified themselves. I think for independent research and development I would like to see user agencies write general guidance in the area of propulsion, and in the area of guidance systems, and in the areas of counter-measures, and in any number of areas. You can go down the line. Distribute these to the major contractors through your independent research and development efforts, through your TODs, TAPs, QDRs. Distribute these to the contractor. Now, the Government research and development organization, Army, Navy, and Air Force, are tied in. As I understand it, any contractor that works under independent research and development would submit his IRAD program to the user agency who has cognizance over his facility. For example, I submit mine to Wright-Patterson, and they make subsequent distribution to Army, Navy, Air Force, and NASA. So this means that all of the user agencies might be involved in the program. I could think of one example that we have. In ASW we have no contract and yet we have done some independent research and development. I have no guidance in ASW. How do I classify some of the work in ASW? I don't know this. I have no means, no contractual means, to get the guidance. This is why I think that if we are going to classify research and development—and we have no objection to it—someone within the Department of Defense is going to be faced with the proposition of writing guidance that would specify the minimum classification in the areas I mentioned. I think this would benefit the contractor. Now, this doesn't necessarily mean that information related to a particular contract could not assume a higher classification. But the minimum consistent classification for each area of interest I think should be issued to all participants in the various programs, TOD, QDRs and TAPs.

BAGLEY: May I add a comment

to that. I think that you would be getting yourself into a trap if you did this, because this would assume at the first instance that you know where you are going. The purpose of R&D is not necessarily that. If you have IRAD programs which are broadly connected with ASW, certainly I think the answer would be to go to the appropriate Navy desk—ASW project office, for example—who then could give you guidance based on the fact that you have some sort of a program in IR&D which he might well be interested in. But as far as furnishing general guidance I don't think you could live with it, because you would then automatically have a restraint put upon you that you might not well like.

CHELIUS: I think we would rather live with a situation where I could discuss and know the classification of something than write justifications when someone in a particular service says, "Gee, why haven't you been classifying? Look at Program X over here. It's all classified. Now, why haven't you or why aren't you classifying your IRAD program?" And this has happened occasionally.

DUPELL: We do try to tell the people who are going to be the recipients of it as much as we can possibly determine at that particular time about what's classified as the system exists now. We try to extrapolate what we are going to have to protect on the new effort but we do it on a case by case basis. We just don't have any across the board guidance.

CHELIUS: One further thing. I would like to know, between Jim and Fred, how many contractor-developed reports you have personally reviewed for classification? We find that they go to the technical side of the house but they really don't go through the classification management side of the house. At least it's not my experience.

DUPELL: I take it Jim Bagley and I have the same set up on that because when one of these comes in and there has been no detailed guide our engineers will come wandering in with it and say, "Look, here's one, let's go over it." I have personally reviewed several hundreds of them.

CHELIUS: I don't want to dominate this. For example, we sent something on cryptographic system to a user agency for approval only to ask for a classification determination. It was urgent, actually. We wanted to publish it so a number of our technical people would have the use of an unclassified idea of what cryptographic information represents, and they were processing that as an unsolicited proposal. My experience has been, we can't write in and just get a determination of classification.

DUPELL: They can in my command. I receive maybe five or six of these every week. They will send it in and say, "We are protecting this as though it were secret. Please give us a classification review." And we do it.

WILLIAM FLORENCE: Following through with Mr. Bagley's suggestion about the entrapment you can find yourself in by using these classifications from some vague guide, I believe. Mr. Boberg, we are at the point here of the basic question as to whether we are talking about official Defense Information under Executive Order 10501 where these classifica-

tions apply, and on the other hand considering information that is not within the Executive Order although it is information of importance to a contractor. Now, this is a basic question that we must always consider in all of our relationships Government contractor-wise, both ways; and to the extent that there is information that is not within Executive Order 10501, certainly as this last suggestion was, an inquiry would be made to the appropriate Government point of contact about any specific security for that information. If it's information properly within the application of Executive Order 10501, then the United States Government is obligated to state specifically whether the category of top secret, secret, or confidential shall apply. And there should be no question as to the Government's responsibility on this. Thank you.

MacCLAIN: I wanted to ask a question of George Chelius. He made a plea for an arrangement whereby independent research workers could communicate across facilities. I wonder if without taking more than available time he could indicate what his obstacle is?

CHELIUS: Our engineer says, "I want to go to Company A." I process a visit request on a Category IV exchange of information. The visit request goes to the contract officer, and as we have not cited the applicable contract, because it is independent research and development, he will deny the request.

MacCLAIN: Are you saying specifically that even though the Government is giving him money for independent research, they will deny the opportunity to talk to others who are doing such work?

CHELIUS: We haven't been able to find the avenue to communicate; no.

MacCLAIN: I think if there is an avenue, Dick, it would be very well to have it stated.

DUPELL: I get involved in that quite a bit on independent research, and again it's all tied in to this agreement with various corporations that they have with the Government on this long range development program. We will honor a visit request for a Category IV visit on the basis that you need it as part of this program, and this doesn't create any problem.

CHELIUS: As part of the current contractor's program?

DUPELL: No, no, as part of the long range development program. You are agreeing with the Government to spend company money on research.

CHELIUS: Who approves the visit request?

DUPELL: UPCO. We get them all of the time.

CHELIUS: Our independent research and development contract with the Government is not a classified contract. And I believe that is consistent.

DUPELL: No, wait a minute. It's not a classified contract because it is not a contract. It's an agreement but you can process a visit request on that. I think Don Garret has got more details on that. I will talk to you about that after the meeting if you would like.

DONALD GARRETT: I believe it is true that in the QDRI and the

TRP and these other programs the Army, Navy and Air Force have, it is possible to obtain DDC documentation based upon your expressed interest and your authorized interest in these programs. Am I not right, George?

CHELIUS: That's right.

GARRETT: Second point: when you do obtain particular documentation you do embark on a particular research project on independent research. It is generally possible for you to locate a DoD activity that has an interest in it which can give you competent classification advice, such as suggested in the ASW situation.

ROBERTO GARZA: I would like to direct a question to Mr. Wilson pertaining to his presentation yesterday. I believe you indicated that as an alternative to paragraph marking in the case of a classified document, you proposed putting the Security Requirements Plan at the back of the document. Did you or do you have any other alternatives that you propose using?

WILSON: Yes, we had a four-pronged approach, each identified by the type of document we intended to use. First was the paragraph marking which would be for short documents and where there wasn't any associative classification hazard, or little, that we could see. Secondly, we have a group of documents under one area where we must number all the paragraphs and it also requires a table of contents; so we plan to use or utilize the table of contents as a point to identify the classification of the paragraphs. Thirdly, we have documents in many cases that are, in fact, almost entirely of one level of classification. Each paragraph perhaps is unclassified except for a few classified paragraphs. Our approach to those was to make on the back of the title page a statement to the effect that all paragraphs in this document are on the level of unclassified or confidential unless specifically marked to the contrary. Finally, of course, was the approach of putting the SRP in the back. Now, if I used the past tense, of course I am probably still reeling from the three-salvo broadside that George hit me with yesterday, which has changed a lot of thinking, at least on my part. I still do not recognize in the ISM any order of priority for the alternatives, as much as I may look for it. The second salvo, of course, was that if I paragraph marked every paragraph in a couple of hundred pages, as I must, then I was to identify any associative classification hazards in the thing. This, of course, requires a review procedure that wasn't contemplated in our cost evaluation of paragraph marking. Then finally he made a statement, if I understood him correctly—and I hope I didn't—to the effect that it was not adequate to put a 254 or a summary thereof in the back of the document. But to say that this 254 is adequate guidance to mark every paragraph in that document, but isn't adequate guidance to mark every use of extractive classification, is rather an approach that I am somewhat astounded at. So, when I state my program I state it in the past tense for those reasons.

BOBERG: Despite the fact that we are out of time I think it has to

be appropriate that we ask Mr. MacClain to respond to that.

MacCLAIN: On borrowed time. The real purpose of paragraph marking is so that the people who have the opportunity to identify classified information will do just exactly that at the time that the information assumes the form that other people can obtain. One might set up almost any system for doing this. The idea or objective is to communicate the classification content of that document to the next fellow that has it, as well as to identify it to the person who is creating the document so that he himself will do a right job. As I said, we certainly would not want to establish a formalistic system that would accomplish nothing in substance. Anyone who wants to give classification guidance to the next fellow along the line and who knows that the guidance is desirable, certainly should do it, by any conceivable form. But right now, we happen to believe that the most effective format for this is paragraph marking. And until it is proved to the contrary, this is our present pitch. As I say, it's what we think at this time is the best form. If you, for example, consider page by page marking of documents, it is not right to assume that you go through a document and put the overall classification at the top and bottom of every page. This accomplishes nothing except the protection, page by page, at a certain level, whether or not that page needs any protection. As you know, the rule is that you will mark each page according to the content of that page. In connection with the problem of association, if a document becomes separated into parts, and all of your guidance for the pages is on one single sheet of paper, what have you got left? Nothing, really, in the form of guidance. This is a hazard, and maybe we have to live with it. I don't know. But the hazard is that if you put something on the back or on the front and nothing any other place you haven't helped the next guy if the thing falls apart. And so paragraph marking has the virtue of going with the paragraph wherever the paragraph goes, and you can't get around that one. As far as the 254 is concerned we do not contend that the 254 today is deficient except in some cases. But I think you all realize that you wouldn't justify your classification management program in your own facility if you didn't think it was necessary in a particular contract to take the 254 and work it out in relation to your own job. You interpret it locally. There is no one else in the world who could do a better job. And, accordingly, for you to simply take the original 254 which you had to interpret and then pass it along to a man who doesn't have to interpret it and couldn't even if he had to, you see it doesn't really serve a purpose. So although the 254 is indeed the basic guidance from the Government to you, the problem we are faced with is the application of this guidance to particular information that goes with it. Well, this is the rationale behind it. And, of course, you can't prove anything about all of this. We just happen to think that this makes a little bit of sense at this time.

THOMAS GRADY: You tempt us, Mr. Chairman, with the independent research and the 254 and the classification problems. But back to Mr. Wise. I commend his program for limiting or delimiting the internal distribution of the DD 254 and using a corporate form. Do you forsee any problems of obtaining user approval? For example, is it the same philosophy as the ISM and SPP, or do you do it without prior approval of the sponsor or the user agency?

WISE: We will seek user approval. This has its good and bad points.

GRADY: Would Mr. Garrett like to comment on that?

GARRETT: I thought that question should be addressed to Mr. Wise. It appears to me that I would say no, that you would not necessarily have to get the user agency's approval unless you have gone appreciably beyond the guidance supplied in the 254. This would be my immediate reaction to the question.

WISE: I would just like to add a few more comments as food for thought. If you do this, it has the advantage of precluding second guessing at a later date on what you have done, by your customer agency. It also has the disadvantage of perhaps having your ideas turned completely around in the very beginning, you see. So, it should be up to you. And again I would say that it depends on the type of work it is, the type of relationship that you have with the particular agency involved.

MacCLAIN: I want to make an additional comment. With respect to paragraph marking, not a single one of you is to blame for the fact that the DoD Instruction 5210.47 doesn't in so many words state an order of priority on marking. The ISM, of course, followed the same example. But there was never any doubt at the DoD level that the intended priority was paragraph marking, and there is no doubt at the present time. That is the way it is. In order that this matter be made more clear, I am sure we will have to get something out in the Industrial Security letter or some other way, and we will do that. The idea is that paragraph marking is required unless and until, in good faith and with some honest effort, you decide it just isn't going to work in a particular case. Then you may retreat to one of the others. A question has been raised about marking paragraphs for downgrading by groups. We don't require this. We say, if you think it is a good idea go ahead and do it. Accordingly, all the arguments that are made against group marking by paragraph are arguments to which no answer is needed. You don't have to do this unless you want to. Indeed if you did do it I don't know how you could take advantage of the effort that you have made, in the future, on that particular document. And, at this time, I don't know the answer. The other thing I wanted to mention had to do with the 254 itself. I should have mentioned this earlier but I forgot it. From the time that this 254 becomes effective there will never be another close-out 254 and there will never be another letter in lieu of. It is being reduced so that you have an original 254, a revised 254, and in some cases a final 254. At the end of the contract close-out, if nothing of a

classified nature is retained there will not even be a final 254. Until it does become established this way, of course, you continue with the present system. Thanks for the opportunity to make these few remarks.

PANEL – CLASSIFICATION MANAGEMENT IN THE NON-PROFIT RESEARCH ORGANIZATION

Leslie M. Redman, Moderator

JAMES G. MARSH
Sandia Corporation

Good morning, you all. I surely do want to add my expression of appreciation and congratulations to the others for our fine Seminar, to Howard and his crew who have done such a fine job. I was here two years ago. I am happy to be back, and look forward to 1968.

I have been given the assignment of discussing the Sandia Laboratory classification program. For the past two days you have been immersed in DoDs. I can't keep up with these initials and acronyms. Now I am going to give you a little bit of the other side of the coin and talk in terms of AECs.

Sandia Laboratory is located in Albuquerque, New Mexico. It has a branch at Livermore, California. We have two operations going to support Lawrence Radiation Laboratory on one hand and Los Alamos on the other.

We have a staff of about 8,000 people. Most of these people are scientists and engineers. We are a prime contractor to the AEC, but we do not produce nuclear weapons. Our main business is systems engineering. Sandia's main responsibility is to be the nuclear weapon systems engineering arm in the AEC contractor team. As such, Sandia takes military requirements and subsystems designed by other laboratories and performs all the engineering analysis and design to come out with an integrated weapon system, so that it can be ready for field use.

Sandia has this responsibility during the entire life cycle of a weapon system, from its conception through production monitoring, testing, and to military training, on through to stockpile surveillance and finally retirement.

All these missions, of course, affect the classification function. I think in our situation the principal key words I would like to emphasize are diversity and complexity. Before I discuss the form that classification has taken, let me spend a little bit more time describing the Laboratory's primary mission.

Of course you recognize nuclear weapons must be safe to handle, highly reliable, and able to withstand severe environments. Yet they cannot be fully tested in advance of use, at least as long as we are under the test ban situation. To meet the challenge arising from such stiff requirements, Sandia's technical staff is divided into some twenty directorates.

For convenience, these may be lumped into five broad categories of emphasis: Research—into scientific fields related to nuclear weaponry; development—of materials, processes, components and systems; testing—both environmental and field; manufacturing engineering, including development of product test equipment; and quality assurance, including stockpile surveillance.

In our business we find that our people have to be aware of the state-of-the-art development in a whole host of scientific disciplines because nuclear ordnance engineering has always been at the front edge of new developments. Among the things in which we claim some knowledge are: nuclear burst physics; nuclear effects studies; dynamic response of materials and structures; microminiaturization; ballistic case design; arming, fuzing, firing components; field and rocket-borne instrumentation; and radio-telemetry. That's just a few. Not all of these areas are equally productive of classification problems, although we seem to find enough. But basically we have divided the functions of our staff into seven physical functions.

Most of our staff time is devoted to such activities as advice and counsel. I don't want you to get the connotation of the psychiatrist and the couch, although sometimes it almost comes to that. We review documents, we prepare major written guides, and it seems that a large part of our time is taken up with liaison with other agencies of various types.

Lesser amounts of time are devoted to our education program, to our internal audit program, to reviewing documents for down-grading, and to the preparation of guides for subcontractors or suppliers. I only have time to discuss two of these, the advice and counsel function and the guide function. Both of these provide challenges I believe are unique at Sandia. We spend a large amount of our staff time to advise and counsel. This should not be interpreted as having people come to the classification folks for directives and orders and we just sit in a court of judgement and render decisions. That is not the case at all. These discussions and the relationship are more mutual propositions. A friendly atmosphere prevails. We make contributions on both sides to solve the problems. It is a give and take proposition. The technical man must first explain his classification problem and at the same time the classification man gets a briefing on a new program. These simultaneous steps are necessary if the right kind of advice is to be given to make sure that the information, process, the material, and product are to remain secure from the inception of the program.

I think is it obvious that unless these discussions are conducted with complete candor you get nowhere. You have got to have frankness on both sides of the fence. We get requests for advice in all forms, from the telephone, to lengthy personal visits in the office, requests for help, or by more formal memorandum. People who require our services may be any of several hundred Sandians

who are authorized to classify information and drawings, those who have been recently promoted to positions where they are now authorized to classify, and those project engineers who have new weapons programs for which formal guidance doesn't even exist. Requests, of course, come not only from the technical side of the house but the administrative side, such as the purchasing people who draw up the contracts that contain classified information, from those in public relations who would like to break a nice story in the *Laboratory News*. Sometimes we have to turn them down on those things. Requests come from contractors who have been given drawings, reports or materials, and even from some of you folks when you would like briefings on new programs and whatnot.

We have in our working force four staff people and a supervisor. I don't know if he would necessarily come under the heading of working force or not. He sort of sits back and preempts people from time to time. But our people do average from six to twelve consultations each day. The queries range from a casual thing that could be answered off the top of the head to a complex query from Washington asking us to justify things.

The second unique and challenging function we have is that of preparing written guidance. We supply our employees with guidance, and our subcontractors, other integrated contractors, and, of course, the DoD agencies when we work on joint projects.

Fortunately, for the purposes of this talk, we had to do a survey for AEC just at the end of the fiscal year, and we found out that in the last thirty months we had generated 220 pieces of written guidance. Of these, forty I would class major products.

We have our "local" guides, and perhaps some of you are familiar with our *Sandia Classification Handbook*. It attempts to cover in general terms all weaponry technology in enough detail to satisfy the average needs of the individual.

In addition to that, we prepare special guides on things like neutron generators and fuzing. Another item very heavily in demand is what we call our Mark guides. I think you folks have different nomenclature, but we produce a system guide for every program, such as the Mark 61 and so forth. We try with the advent of each new program to get on the street as soon as we can with a guide of some consequence.

In addition, we help in the preparation of guides that have a much broader policy implication. We were instrumental to some extent in helping to prepare the new guide CG-W-2. We have also been working with AEC/DoD folks on weapon testing and we have most recently been concerned with special guides in such areas as vulnerability and weapons materials, and a vulnerability guide. We have, perhaps, the only materials guide in existence, which has become a CG document. (CG stands for classification guide, issued by the Division of Classification in Germantown.)

With the services and joint working groups, we have assisted in the prep-

aration of guides for the Test Readiness Program for the JTF-8, and for the JTF-2 Low-Level Weapon System Evaluation Program. Some of you may be acquainted with that program. We spent quite a bit of time and effort and although we got a guide that was acceptable we never did get it approved. In addition, currently we are working on such things as Polaris-Minuteman Mk 12, Poseidon/Mk 3, and Minuteman/Mk 17 reentry vehicle systems. So life gets pretty complex and interesting.

Recently, since there has been relative deemphasis on the weapons programs, the Laboratory has sought to diversify its efforts, and is engaging in a number of reimbursable contracts that have their own unique classification problems. A number of these activities are involved with space. We have several contracts with NASA including a program to prevent contamination of other planets. We also do work in soil activation analysis. We have become active in the Vela satellite program for the downward-looking instrumentation, logic systems, digital data handling and reduction, and other related engineering matters. We contribute to the SNAP program, Systems for Nuclear Auxiliary Power, and one aspect of the contribution to this program is the responsibility for monitoring the safety of aerospace nuclear systems to determine if they would contaminate the earth's atmosphere upon reentry. We are also involved in design of isotopic heat sources, and as a design agency we have sat with the technical people discussing policy for a guide.

Perhaps from there we might go briefly into how we go at writing a guide, and I don't suppose in many ways it's too different from the way the rest go at it. Our first step is to seek out the technical staff people who are involved, particularly if the item is a new weapon program or non-weapon program. And the classifier then needs to sort of brain-wash the technical man to determine what is important to the program. For example, in a new space program he might be interested in the reentry philosophy and the heat generated. He would become involved with our materials people because of their current interest in the vulnerability problem. We do a lot of contact work for them.

But we have to ask the questions, are the techniques, designs and materials in the new program unique so as to require additional classification? And actually unless we get in the early phase of the program we have in all essence lost it. Once the facts are in, a detailed search can be made through existing policy guidance. And here, of course, we have to lean heavily on what is established by AEC policy. We can't go out and make our own without approval. Sometimes we suggest policy, but we don't make it. So we try to determine whether there is any existing guidance that covers the problem. If there is, fine, we just apply, as we normally do in the case of supplier guidance. If there isn't guidance, then we go through long procedures to try to get approval.

When agreement is reached within the company—and sometimes this itself is hard to do—we present it to Bob Henderson, chairman of our classification board. He is chairman of the board, and he is vice president of the Laboratory. About a year ago he was appointed as senior reviewer for the AEC. At any rate, that is our last line in the corporation before it goes to AEC-ALO for approval. Of course in the process of this I think it is evident that when we are doing a package for the nuclear laboratories, we talk with them. Or if we have something in a delivery vehicle naturally we must consult the services before we even draft our guide.

After approval is received and we make the required changes a copy is filed, and then come printing and distribution. Normally we distribute only to people who are internal to the corporation and then within the local weapons system within AEC. Of course it directly affects the contractors. Then the job is just beginning, because once you have a guide in existence, as you know, it becomes obsolete, and it must be revised and re-issued as the situation demands.

In addition to our other work, we had a request to completely revise our *Handbook,* to conform to CG-W-2, which is a neat trick; it is about a 200-page document and it will take some effort.

I should say, lest you think that because we are nonprofit we are not interested in expense, that we have recently completed a cost saving study for the AEC and I would hesitate to say that I could back up all the figures on that, but we did manage to find several areas in which we were able to point to considerable cost savings, one of which I think I could mention briefly. That is the fact that we were able to transclassify vulnerability information, thereby taking advantage of DoD clearances on subcontracts instead of having to go through the tortuous route of the Q, the ninety days, the $500. That is one area in which we think we have made a substantial savings.

We have also had a survey of our reclamation procedures, and we find that although we are not going to make any money we are going to spend a lot less disposing of material than we did before. So far, I don't have any dollars on that one.

I think that from what I have said you can appreciate the broad character of our activities at the Laboratory. Certainly it is diverse and complex. I have only been able to discuss advice and counsel and guide writing but I think that gives you a representative picture of what we do. It seems sometimes that we have at least 100 bosses all making demands at the same time, all wanting fast and thorough service and all burdened with exotic technical considerations, often scheduled so that our help is sought on a kind of last minute basis, which I am sure we all are acquainted with. This, of course, adds to the fun. We try to regard our job as providing service rather than posing restrictions. Our aim is to help the technical line find solutions to classification problems that are technically sound and administratively

feasible. We believe that this approach has contributed much to our general fine working relationship with the line organizations.

This is a quick brush of the Sandia Laboratory classification function. If any of you have questions later I will be happy to try to answer them.

EUGENE J. SUTO
Research Analysis Corporation

Good morning, ladies and gentlemen. RAC, the Research Analysis Corporation, is located off the Beltway at the McLean Exit in Virginia. We moved to our new building from Maryland in December 1963. RAC was established in 1961 to study major defense problems with the U.S. Army as its principal client, having then assumed the responsibility and staff of our predecessor, the Operations Research Office of the Johns Hopkins University. Together ORO and RAC have presented an unbroken chronology in the application of analytical techniques to military problems dating back from 1948.

The basic mission of RAC is to find more effective means of conducting military operations in its broadest context, ranging from insurgency through limited war to total war with nuclear exchange; in seeking out and evaluating preferred and alternate means to increase combat effectiveness; and applying advance techniques and methodology. We consider changes in national and international situations, and weigh recent developments in political and military organizations and strategy and tactics. This work is performed at our facility in McLean and at our various field offices overseas. We have a small office in Bangkok, some personnel in Saigon, another office in Heidelberg, Germany, and representatives in Singapore and with SHAKE, and with the United Kingdom.

In a basic mission in addition to our thrust on Army problems, we have undertaken a diversified program of independent research and studies for the offices of the Secretary of Defense, supporting agencies and non-defense sectors of Government whose needs demand the type of skills we have developed for our principal client.

Perhaps the most important aspect of our mission is its breadth, which today requires and permits RAC to study any subject from the rifle cartridge to the most basic questions of military strategy. We have at the moment over 800 employees. Of this number approximately 50% are either support or administrative personnel and the remaining are professional staff members with degrees in economics, engineering, mathematics, medicine, operations research, physical science, political science, and social science. RAC is divided into eight research departments. These are: strategic studies, combat analysis, unconventional warfare, logistics, military gaming, science engineering, economics and costing, and advanced research. We have a Computer Science Center for technical support.

Our library is considered one of the largest of its type in the metropolitan area and we feel one of the best in the country. It contains more

than 125,000 documents, 16,000 books and pamphlets, 24,000 maps, and approximately 30,000 visual aids. Additionally, we have active subscriptions to some 600 journals and newspapers. Our Editorial and Graphics Department edit and publish most of the publications produced by RAC.

The Production Section further reproduces approximately 300 study publications of various types each year. As you are probably now aware, our principal product is paper, not hardware. From these departments, combined annual output of paper—working paper, drafts and final studies—would range approximately 40,000 copies. These classifications range from unclassified through top secret with other variances of special category markings which require even more detailed special handling and control. In addition to the RAC products, we receive from outside sources about 20,000 pieces of classified material each year which entails constant checking for proper markings and groupings. Also, I might add, in the interest of our clients we are obliged to exercise a degree of control and protection on almost all the unclassified material produced by RAC.

This gives you an idea of our job to effect proper classification and control to meet DoD as well as other government imposed requirements to satisfy the client and give classification guidance to RAC staff members.

We are fortunate in that we have converted our document control system to an automated control utilizing the computer. This went into effect 1 January 1965, after about a year and a half of study.

The system maintains full control over locating documents and provides a given listing at any time of automatic downgrading of documents. The IBM cards designed to support the system serve as receipts, control cards, suspense cards, destruction cards, and the system further provides the location of material by study number as it would pertain to particular contracts.

We have complete and individual staff member inventories which are programmed at six-month intervals. Since we have this constantly growing inventory of over 100,000 documents, this is no small job. But we are able to supply individual staff member inventories for physical checking in a matter of minutes.

Some of the tasks that fall within our department of classification management and control are the preparation of DD 254s for our subcontractor, consultant, and graphic firms. We admit we don't have many of these. However, we do provide guidance and write these 254s for them. One of our main jobs has been to write the letter in lieu of 254 for our principal client. In fact, I got into this particular area about ten years ago, in writing a letter in lieu of a 254 as pertains to the Industrial Security Manual and as we had revisions of the manual we would constantly review this. We find that here was where industry was participating, in that we usually wrote the letter in lieu of and proposed it to our principal client, and with very few changes they

usually bought what we had proposed.

In essence, each year we have a program that is submitted to our principal client and in it we may have anywhere from seventy to one hundred specific studies. This is written in coordination with the client. It would contain scope of the work and perhaps in some cases indicate classification, although generally speaking in our work the classification could range anywhere from unclassified to top secret. And maybe that's all the guidance that we have for the time being in that particular study outlined. This is, as I say, reviewed by our principal client. We receive our work program back. Management then goes over it as it's been approved by the Army, and this is assigned then to particular study teams. We may have anywhere from three to ten technical staff members assigned to a particular study in a certain area. Here again, the team concept is used. What we set up working with the Army is a project advisory group assigned to each study. This group consists of not only the sponsor of the particular study but there are representatives from the various general staff agencies or other specific agencies. Somebody asked earlier, "What about intelligence participation?" Usually there is an Assistant Chief of Staff for Intelligence representative on this project advisory group. Through this meeting, then, about four times a year for most of the studies, they are able to furnish particular guidelines to steer the project on its proper course. At the same time, our member does provide guidance for classification, and the project people are free to come and see us along the way. What may start out as an unclassified project could take on a much higher classification. In fact, we have had studies that have started out with the collection of material from unclassified sources and they eventually were classified as top secret. In some cases they even went into the registered category. That category since has been eliminated but this does show you what can happen.

This doesn't always work out the way we want, however. We have had situations where documents have gone this route, unclassified documents, had complete review process, and then we were told that we could distribute the publication. We made a limited distribution on an unclassified publication, for example, and then we decided at a later date to process the document for clearance in the open literature. So it again went the route of clearance in the open literature. I received a call, "Gene Suto, what are you trying to do, release secret information?" I, in this case, went back to the staff members—it so happened there was a paragraph in a case that I am relating—and I was informed by the staff member concerned in the group, "Well, this information had been collected from *Aviation Week* and a number of other sources." I collected all this information, and this was truly so, and I supplied it to the group and then sent it back through the proper channels and here again there was quite a bit of disagreement. They still maintained, "Well, that

probably still is secret as far as we are concerned. However, in this case we will let it pass."

We do recommend, to our client, distribution statements and controls for all our publications. We coordinate the release of the publications to the Defense Documentation Center and the other addressees. We control the printing requirements, by the way, in our department of all the drafts and final publications. We feel that this is an important aspect, in that even though we have an elaborate procedure of review and approval by one of our vice presidents it will be passed on to us to really decide how many copies of a document we have to have printed to meet the needs of the client plus the needs of the Corporation. We are placed in a difficult position at times on this when someone feels that this document is the best in the world and it should be published and probably 5,000 copies should be distributed to all his colleagues. And then when we end up printing one hundred copies we really do have some problems. We do coordinate the clearance of publications in the open literature in this respect. Any of our documents proposed for clearance in the open literature are first reviewed by our research council, which is made up of five senior research staff members. They in turn first pass on a document from a Corporation point of view as to whether it should or should not be processed for clearance. After their review, in coordination with our contract administrator, we will submit the document for appropriate clearance.

Recently I have had the good fortune to sell management on the idea that we should create a new position within our department, titled Classification Specialist. Even though we have been doing many of these functions, we felt that we could professionally do a better job. Rather than recruit someone for this job, we moved Tom Bracken from our corporation. Tom was in charge of document control and he moved to this new assignment. One of his main tasks will be to develop a general security classification guide. We do have some guides in existence already and we have a RAC style manual. In addition, we have given guidance in our security manual. We have not yet come up with a general guide that would apply to all of our operation.

We implemented the paragraph marking on 1 November 1966 and two of the most common questions that I have had in this area have been, "To what detail do I mark paragraphs?" and two, "Must I paragraph mark the entire document if only a few pages are classified?" I submit that the essence of paragraph marking is to pinpoint in any given document the material that is classified. Our experience has been that in the general run of the mill documents, perhaps one-fourth or less of the material is actually classified. The balance is unclassified. Our policy has been to recommend wherever possible paragraph marking. If this isn't possible, we try to recommend preparation of separate annexes to a pub-

lication that are properly paragraph marked and contain only the classified part. If this is impractical we stress complete paragraph marking or in some cases specify a statement or classification page or guide in the publication that pinpoints which pages are classified, and those pages are paragraph marked. This does save the actual marking of each page and paragraph on unclassified pages. In a few limited cases, we have placed this information on the cover of the publication so there is no doubt as to what is classified.

The advantages of classification management in our type of corporation have been (1) the reduction of inventories, (2) applying proper classification, (3) better coordination with the client and within the facility, and (4) less cost per control if an automated document inventory and control system is maintained. Of course these savings aren't as evident as they would be in a hardware type of operation.

I do propose some thoughts that may have been proposed before but may improve this program. I think this has been tossed out before by DoD. Perhaps having four classification groupings isn't the answer, perhaps we should have only two classification groups—material that is not automatically regradable and should be examined every two or three years for specific regrading purposes, and material that is regradable. Also, we should perhaps set a more realistic time frame, such as every two years from TS to secret, from secret to confidential, and from confidential to unclassified, making a total of six, not twelve years. Another thought is, of course, elimination of the FOUO and similar markings on unclassified documents as now in effect, and require that we cite the particular exemption under the Freedom of Information Act that applies if restriction should be placed on unclassified documents. These exemptions could either replace or supplement the DDC statements now in use. Another thought is that there should be a more simple uniform code for paragraph marking, making it mandatory to include not only the confidential, secret or top secret but a notation as to date of the original group designation. I realize this is optional at this time in a more detailed fashion. However, we do have a problem. Sometimes a group IV confidential document remains group IV for six or seven or ten years because we continue to apply marking and never stress the date the material was originated.

As I look back on our last two seminars there has been considerable progress not only within DoD but within industry for those of us who have been thinking, selling, and applying classification management. There has been participation in the classification management program. We have been getting top management backing. There have been better communication and guidance between Government and contractors. A number of us have gone to automated document control. There have been a lot of thought and action in the reduction of inventory by contractors. We still look forward to a master classifi-

cation directory, some central depository on classification review, and better procedures on applying automated techniques to classification determinations.

In summary, I sincerely believe that we who have been practicing classification management have strong convictions that this program is here to stay. Those firms who do not have such programs will suffer and be criticized. It is up to each of us to sell classification management in the same way that security had to be sold not too many years ago to top management. Thank you very much.

LORIMER F. McCONNELL
System Development Corporation

Thank you, ladies and gentlemen, for bearing with us to the final moment. I am proud of you all. I am happy to tell you that I am going to make this as short as possible. I gave this speech a year ago in Cocoa Beach, and those of you that were there shouldn't have to suffer through the whole thing again.

I could start off by saying many of the features of the classification management programs that we have, others have described, and I want to spend most of my time on a couple of features that I haven't heard others talk about. But so that you will know who and what my company is like, I will give you a little sketch of System Development Corporation, so that you can see why we have picked the kind of classification management program we have to serve our needs.

SDC is a "not for profit" corporation, incorporated almost eleven years ago. It traces its history back to the RAND Corporation; we were a division of that corporation. Even earlier we were known as the System Research Laboratory of RAND. SDC's total population is around 3,000. Of that number about 2,000 are professional people. We have major offices in Santa Monica. We also have key facilities in Falls Church, Virginia; Lexington, Massachusetts; New Jersey; Dayton, Ohio; and Colorado Springs. We also have many smaller liaison operations at military bases throughout this country and abroad. Our major effort has been for the Air Force. Our first contract that put us in business when we spun off from RAND was for the Air Defense Command. We have since that time developed working relationships with other elements of the Air Force and with other elements of DoD and now even with Federal and local governments. So we are diversifying considerably these days.

It is always interesting to me to find out how a classification management program got started. I will tell you about what ours is, but let me just take a few minutes to tell you how it happened.

When I came to work at SDC I was given the responsibility for classification. They said, "You take care of that." I didn't know too much about it, really, but I got out and began to talk with people, technical people and others, and it became evident to me that although we had broad guidance there was very little detailed guidance for the individual technical man to tell him how to

apply this broad guidance in an individual situation. Coupled with that I had discovered that there had developed a divergence of views among the technical people as to just what and how much needed to be classified. Individual technical groups and sections and some individual writers often had their own ideas of the way it ought to be done. So I found that the problem I had on my hands was how to reconcile these divergent views, to provide assistance in interpreting existing guidance and to obtain guidance where it was lacking. Now, I think we have reduced the problem to a manageable size but we are still trying to solve it—one painful step at a time. I was told in those days, and I still am occasionally, that the contractor does not classify anything, that he simply marks in accordance with the military instruction. I don't quarrel with this. But the phrase bothers me somewhat because the rigorous language tends to imply that many contractors are to be provided with a kind of nut and bolt manual on how to classify everything. This doesn't, as you know, happen. It can't ever happen. So I think the contractor must participate to some extent in the initial and continuing development of the guidance. I believe what I have heard here in the last two and a half days would lead me to believe that most people here agree with that. The job of determining an individual classification in an individual situation is an extremely complicated business, is what I am saying, and no matter how good the written guidance is I don't think it is really ever going to solve the problem. Central management attention to the problems of classification management is needed. And that is why we are finding that there are people who are called classification managers. Those of us who are here today I think play a very important role in this whole thing. So I would stress that guidance alone is not enough—written guidance that is.

At SDC we are a staff office—we recently underwent a slight reorganization—and I am responsible for the classification management office. I report to our corporate secretary-treasurer as does our security manager, who is at an equal level with myself. In addition to classification matters, as such, my office, which consists of myself and three other professional people and one secretary, is responsible for documentation policy at SDC and for documentation matters, which, incidentally, fit very nicely with the classification business because we are oriented toward the content of information and documentation. We also handle problems concerned with proprietary information, trade secrets, copyright, and other things that relate to protecting information for reasons other than National Security.

Our functions include providing guidance to the line organizations, the technical line organizations which we try to educate as—if I may use the expression—junior classification management people. We try to infuse in our technical people the ability to conduct themselves as classification management people and keep our

office at a minimum level. It would be very easy for us to begin to enlarge our staff, double or triple it, and have everyone come to us to make classification decisions. But that is not an honest, sensible way to go. We try to hold our staff down and answer questions only when things just can't be answered elsewhere, but to continue to keep information on classification flowing to certain key people in our technical organization who can, hopefully, do the right thing. Although we are a staff office and have no line responsibility over anyone who is making classification decisions, we are the final corporate authority in classification matters. So, right or wrong, when we make a decision that's it. And this is pretty good. It has turned out that we can make decisions about as well as anybody and it kind of helps when you have one decision and not seven.

We have informal working relationships with our contracts management office, with our public relations office, and with our purchasing people, who all are likely to have something to do with some aspect of classification. Another thing, too—several others have mentioned this also—it is a corporate rule that no one may discuss an interpretation of classification guidance with our user agencies except us. There is a real good reason for this. We don't want our user agencies to be approached seventeen or a hundred different times on similar questions. It doesn't make any sense to do it that way. We have learned that through experience. I am sure others have also.

One thing I would like to take four or five minutes on is our system for handling classification challenges. We believe that it is a good policy not to play ostrich when there are problems; that is, we recognize that there are going to be problems, and that security classification is not a perfect art.

Dr. Hammer talked about "How many 9s do you want? I can't give you a hundred percent." I think this works in most areas of human activity, and we encourage people to come up, let us know when there is a problem. Let's say, if a document gets published as unclassified and somebody sees it and thinks that it ought to be secret, we try to encourage people to let us know about it, without feeling that there's an awful threat of doom associated with revealing this fact. We think that it is in the interest of National Security to find out about these things and try to do something about them. If we can't, if the rabbit's out of the bag, at least we let the proper people know about it.

In many cases, we found that under-classification is not a matter of somebody goofing, it's just a matter of maybe no one had formulated a judgment about that particular thing until the document got published. Maybe there wasn't clear guidance. Maybe there was a conflict of guidance or something like this, and the mechanism of having challenges flow through our office helps us to improve our guidance and it helps us to educate our people who feel very free about coming in to us. Very seldom do we find that someone just

out and out failed to do his duty. This happens sometimes, and certainly disciplinary actions have to be taken. People have to read their guidance. It's there in black and white. But by and large our challenge system has proven to be a very useful tool in helping us improve effectiveness of our classification program.

We keep some records, too. We try to prove to our management that we are worthwhile. Every once in awhile they look at these. A member of top management gets interested in the Industrial Security Manual and he wonders, you know, what is in there that involves us. It's not always easy to explain but we try. We try to argue that we reduce the amount of debate and argument on the part of the technical people by making decisions. Also, we have kept some track of documentation volume. We try to reduce the volume of initially published secret information. Our first effort I should say was to try to get rid of as much unnecessary secret as possible. When we thought that we had cleaned out the excess to the best of our ability, we felt the next best effort would be to concentrate on keeping the initial publication of secret data at a minimum. Over a period of four years we have been, I think, pretty effective in this. Our overall level of documentation has remained about the same. Our volume of secret documents has been reduced from around 150,000 to, the next year, around 80,000, to about 50,000, to 30,000. We think this is pretty significant. It is just a matter of getting to people who are publishing documents in twelve volumes, all of which are secret, and asking, "Could you maybe put all the secret in one volume?" "Yes, I guess so." It's just as simple as that sometimes, and the payoff is tremendous.

We feel this is the only kind of payoff we can find. We are in the software business and we don't produce hardware so we have to count paper. I am sure that people in hardware can come up with much better cost reduction programs than we can, but we are kind of proud of this. Also, I think it makes good sense from the standpoint of making the security program better. If you have got less to protect, you have got a better chance of really protecting it. We think that's a good argument.

One final note on cost: our technical services operation has figured out in terms of hard dollars and cents that it really costs them about $1.45 to process a secret document. Each document that is printed by this organization is sold to one of our technical departments. Really, the money comes out of the technical department's budget. If someone in one of our line departments orders a document and pays a certain price for it, it comes out of his budget—and he has got to have the money to pay for it. If it's secret it costs him $1.45 more, to cover the cost of the forms, the accountability inventory, and so forth. So we can really save our line departments a little money in this way if we can reduce or show them ways to reduce the volume of secret that they initiate.

That's the end of my talk. I will be glad to answer any questions later

on during the question and answer period. Thank you.

LESLIE M. REDMAN
Los Alamos Scientific Laboratory

Let me tell you a little bit about the Los Alamos Scientific Laboratory. It is in the mountains of Northern New Mexico, a site picked originally for security and the opportunity to fire high explosives without attracting undue attention. The Laboratory was started in 1943 to do the research and engineering for the first nuclear weapons. Its original mission included production of them. Now we are confining ourselves solely to research and development. About half of the work of the Laboratory is on nuclear weapons. Other activities include nuclear reactors for rocket propulsion, controlled thermonuclear reactions, some work on civilian power reactors, investigations into biology and medicine, and a great deal of basic supporting research in physics and chemistry and metallurgy. In addition to that, we are in the process, and it appears to be going forward, of constructing a large linear accelerator to do fundamental work in medium energy physics.

The Laboratory has always been under the University of California. It is organized in somewhat loose confederation of technical divisions each with an area in which to function. We don't work on projects but rather in terms of competencies. Because of our original mission and situation we have stayed quite closely to in-house activities. We have essentially no subcontracts for research and development work outside the Laboratory, and this has of course simplified the problem of providing classification guidance.

In the panel the other day, Mr. Pender recited the legal basis for what must seem to many of you the peculiarities of the Atomic Energy Commission and its contractors—namely, that there is a separate act; that it is the first statutory identification of a class of information or group of information that is, so to speak, born classified; that the Atomic Energy Commission as an entity (five people) are the only ones empowered to remove any information from the category of Restricted Data. Perhaps you aren't familiar with the way in which that operates, practically. The Commissioners, normally, merely make policy and say that, "This area of information is expected to develop very little that we want to keep classified." They did this in regard to the civilian power reactor. They are advised by a body of senior technical people, called the Senior Reviewers. The declassification system which the AEC has to have as opposed to a system of review for public release, is staffed by a group of perhaps one hundred responsible reviewers—usually contractors—scattered throughout the Commission's installations who are versed both in the subject matter and in the classification rules and policies.

With the passage of time more and more areas have been defined as unclassified. The Atomic Energy Act expressly states that the Commission shall have no policy to restrict the

dissemination of information except as provided in that and other acts. Accordingly, we have never had in the Atomic Energy program the problem of deciding whether something was fit to be published, because it never became unclassified under the Act unless that was true. Once it had been declassified there were no restraints available other than perhaps moral suasion to the publication of the information.

Because of our peculiar character and history, our classification management activity is very different from almost anyone else's. I have an office that has a total of three people in it. All of us have worked in research and development for the Atomic Energy Commission or its predecessor. Our principal function is to develop, in consultation with technical people, what it is about their programs that is no longer classified. This is a very happy situation in which to be for someone concerned with classification management, because you are giving permission to release, in a sense, rather than being concerned about what must be isolated.

We publish about seventy-five papers in the open literature each month, and issue about twenty-five more technical reports. All of those are individually reviewed completely by the technical information group.

That is a very brief summary. I think it hits the particular characteristics of the Laboratory of interest here.

I now throw the meeting open for questions from the floor.

KENNETH WILSON: I don't have a question but I would like to comment on that statement you just made, wherein you indicated that your task was to help them find out what was unclassified. That strikes me as a very interesting sales point for the rest of us, which I don't think many of us have tried to use. At least I hadn't thought of this approach. Yet it can be applicable in DoD industry classification management. Perhaps this might be something for us to think about. I intend to go back and start thinking positive, in approaching my engineers—taking the position that I am helping them to identify what they can release rather than what they can't release. So I would like to thank you for that little gem.

REDMAN: It flows directly from the Atomic Energy Act but it can flow farther than the AEC contractors certainly.

RICHARD BOBERG: I, too, rather than a question had some observations that pretty much apply to both this panel and the one prior to it. I want to underline a couple of things that were said. They were brought up for the first time, I think, by your panel. I had hoped that we would emphasize them more. There are some things I think need to be emphasized. One of them is the concept of document reduction, which is the responsibility of all of us. It is perhaps the basis of a classification management program. Another is the limitation by some practical means of reproduction of classified material. I have been doing some wrestling

with that problem in our particular corporation, and I don't think we have that kind of time. But I would be curious to now know how some of you contractor representatives have resolved this. As I recall, the Industrial Security Manual says something to the effect that reproduction of classified material will be kept to the minimum required to do the contract. The definition of that figure is always a difficult one where they are technical folks because of what's been mentioned before—the pride of authorship and the fact that everyone wants to send one to the president of the corporation. I think another part of a good classification management program is what was mentioned about the proprietory information, and also, perhaps, foreign mailing, which gets involved in our field. So I think these things should be underlined in the sense that they are parts of all good classification management programs. Thank you.

GEORGE MacCLAIN: I think you will recall that when Joe Liebling spoke at lunch on the first day he mentioned that there is indeed a payoff for the pocketbook of industry if they will take every reasonable step to identify what's classified so that they have less restraints on the use of what is not classified. It is a little difficult to know just how to communicate your unclassified information that hasn't been approved for prior public release. I don't have all the answers to that but I am sure that it is easier to do that than it is to communicate classified information. And therefore if you find that your management is boxing your ears because of the cost that you are devoting to close identification of classified information, remember that you always have a comeback: that you are releasing something for possible use to the company to make some money. And it may be that what you said and what Ken said and what Joe said is really a plus that we can all get.

LESLIE AYERS: I noted in Jim Marsh's presentation that he hinted he sometimes has to worry about classification from divergent sources and possibly divergent classification guidance. Jim, could you discuss a little bit what you do if you find that there is a disagreement between, for instance, the Air Force and the Atomic Energy Commission about any given integrated project.

MARSH: Well, I think I will sidestep that one, but that is something that the Commission and DoD haven't been able to settle in quite a while. I think what you bring up is really a problem to both sides of the fence. You have got a lot of projects going, as you are well aware. In fact, we are working for you folks right now. But we have this peculiar interface where we are trying to design a product for the military. We have the restrictions of the Atomic Energy Act. We are currently working on a device which conceivably could be used by the Navy or the Air Force. The problem is we naturally go first to our technical people, and they are dealing with one branch of the service. In the process of this we come to clear up what about the project should be classified. If we

have two services involved simultaneously, already you have a built-in possibility of dispute. Then we have to go to Mr. Durham to ask his good offices to help us solve this or we go to the groups individually or get them together. The problem really isn't so bad because after hammering things back and forth things can be resolved. But then when we try to get approval through our line of authority, which goes back through our Operations Office to Germantown, that's where the fun starts. And we find that there is a lot of crossover at the policy level and sometimes there is not enough information about the product. So we just go around in circles. It usually winds up with a big meeting, and a few people getting irritated. Normally with enough patience we can resolve the questions. And the reason I like to come to these meetings, there are a lot of you I talk to on the phone, or write to once in awhile, and we know we have mutual problems and we don't get together enough to talk about them. To me this is one of the real benefits I get from coming to such a meeting. I don't think I answered your question but it gave me a chance to expand on that a little bit.

AYERS: I knew there was no real answer. I was pulling your leg a little bit about the integrated project. But I think that anybody who lives in the classification business here in Washington, as a large number of us here do, has come to the conclusion that nothing beats getting around the same table once in awhile.

WILLIAM FLORENCE: Mr. McConnell, you have described an effective focal point in System Development Corporation for putting questions to the Government as to what the classification of information really should be on work that your employees are doing. Do you find as equally effective a focal point in the Government for giving you back the answers?

McCONNELL: Isn't it just about time to adjourn? No, I think I can answer that. We found that if we really go out looking for someone to give us an answer we can usually find someone. I mean that sincerely. I don't mean that to flatter anyone. Sometimes we are frustrated because of the time delay, and I fully understand that the military people we go to just can't come up with it like that; they have got to go some place else. So, it's fully understandable. But as far as ultimately getting an answer, yes, I think we do, if we go out and scratch hard enough and bother people enough, we get some kind of answer.

DONALD GARRETT: One of the list of 767½ questions that I was going to ask the panel this morning was, What is the average time it takes to obtain a classification interpretation from the customer? Are there any categorical answers that you can give?

McCONNELL: I don't think I could give an answer but I could say this: a decision quite often has to be made one way or the other, and if you are in a situation—this has been our experience—where you realize it is going to be awhile before you get the answer, all you can do is over-

classify until you find out. You can always downgrade it later. Sometimes you just can't get the answer as quickly as you feel you need it. But as regards an average, I don't really know. Sometimes you get answers right on the spot. Sometimes it takes a month or two. Sometimes it takes longer. I don't know what the average is.

GARRETT: Second question along that line: Do you have any difficulty identifying the party to whom to go to get an answer?

McCONNELL: We don't, we go to the user agency.

SUTO: I can add to that. We really haven't had a problem, in that you usually go through the user agency who can refer you to another source. We found in some cases by going directly to the user agency they don't have any objection if we pursue it further with the originator.

MARSH: I think you folks know that your channels are pretty well established. Sometimes we do have several problems. In fact I was happy to get to this meeting because I finally got to the top man—I should be talking to the Navy. But we have looked to Durham's office to be a point of contact because we have found that if we tried from our side of the fence to go to the individual our lack of knowledge handicaps us. So we use that as a point of liaison. I don't know if it is proper or not. It has been effective. Otherwise we get frustrated.

J. S. TROUTMAN: One of the things I had hoped to have addressed by this panel was this problem of working papers. I would like to know if some of these other groups have run into the problems of working papers. When do you bring a working paper under control? How do you manage its classification? How do you get in guidance? Have any of you run into this problem?

REDMAN: Let me start to try to answer that. The ideal condition I described earlier really does exist in our operation, and of the man doesn't put the proper classification stamp on it, the secretary will. And if she can't get an answer from him or the group leader, someone gets in touch with the classification organization and establishes what it should be. The security rules call for marking anything as soon as you stop writing on it, by the page, and we find, in general, that's done or the material is carefully protected until enough of it has been accumulated so that it can be reviewed.

MacCLAIN: Dick, Larry, and Gene, I think they are all primarily producing paper, and all have active programs to keep down the volume of classified paper at its point of origin to the extent that they can, and all have also emphasized that they try to segregate the classified. I wonder if there is any information available to them that would indicate a feed-back from their marketing people or their management in this connection. If you have thirty percent reduction in secret documentation, does that additional amount of unclassified information help your management to make money as far as you know?

McCONNELL: George, for my part I am reminded of the comment Jim Bagley made—that we have got a bigger problem with unclassified than with classified. (Not seriously.) But there is a problem there, because if you are dealing with a classified contract and information that pertains thereto you still have got to go to security review. I recognize their problem. They are burdened with all kinds of things going through that have to be cleared, and then have got the decision process of, "Well, can the public have it?" And this takes time.

MacCLAIN: I think this is an existing difference between DoD operations, for instance, and the AEC operations. Correct me if I am wrong, Les, but if your Commission says something is not classified they thereby say it is releasable.

REDMAN: That's what the Act reads, that it may be published without undue risk to the common defense and security, and they have no power to restrict the dissemination of information except as provided in that and other acts. So it's something of an experience for AEC contractor people to come to meetings like this and find that one basic concern of everybody else is one that has been legislated away from them.

BOBERG: I wanted to comment that I think Lorry's answer is the best possible under the circumstances. Unfortunately, George, I don't think I can give you a nice positive example. I wish I could, but it brings me to another thought I had which is obviously unsolvable at this time. It relates to the point that Lorry and Jim Bagley made earlier, that one of the things management has indicated to me—and I think it might be a problem elsewhere—is the growing redundancy of markings on documents, be they classified or unclassified. I am speaking of the markings now required through different regulations, emanating perhaps from different statutes or different executive orders and so forth. Many of these markings go on the same document and many tend to be duplicating. This does relate to unclassified documents because certain of them are required, and this is a growing problem. I think it relates, too, to our first day's discussions starting with Congressman Moss who said something to the effect that he would like to see a simple statement rather than "for official use only,"—exempt or not exempt. This is the kind of thing that would help us all in this area.

ARTHUR VAN COOK: Lorry McConnell mentioned the cost of a secret document would be $1.45. It is this type of cost data, if you have it available, Lorry, I would very much be interested in putting a finger on. In fact, I am interested right now in all cost data relating to the handling of classified documents in transit, the cost associated with the conduct of top secret or secret inventories, and receipting and storage. These cost data become increasingly important these days in assisting us to develop new programs where we can present a rationale such as "If you adopt this particular procedure, you can effect cost avoidance savings." But the hard,

factual data to support this rationale are not readily available. So I appeal to all present here that if you have any cost data along the lines that I have just mentioned I would very much appreciate being informed. Send it directly in to our office. Thank you.

F. X. JAHN: This is in answer to some of the questions by Mr. Boberg as to how some of the classified document inventory can be reduced and controlled. We have in our plant no automatic distribution on classified documents. We have a six-month follow-up on every accountable document. If it's not charged out in six months, the person responsible for the document must certify in writing that it is to be used. We will then hold it an additional six months. If it is not used for one year it requires a memorandum from a manager to continue to hold the document. We have no classified reproduction except through central repro. On all of our machines around the plant there is a very strict statement on the machine that it must not be used for any classified reproduction. So all reproduction of classified documents has to go through the central organization. Anybody can put in a request for reproduction but he can only get it out through security, because all classified repros go from reproduction to security for release. We have a rule that you cannot make in excess of ten copies of a classified document unless it is a contract requirement. If you need something in excess of ten copies you have to get permission from security.

KENNETH WILSON: I think, George, in Dick's comment about these markings and some of the effects they are having, there is one that's brought on a cost real fast, by probably the human reaction to it. That is the recent change whereby you mark the back with the classification of the front if it's higher, etcetera, etcetera. I can name at least three companies in the New England area whose reaction to that has been to discontinue printing on other than one side of a page. This obviously doubles everything, cost and everything else. They feel that this is really easier than trying to explain, implement and enforce the multiple classification approach. I can see the desirability of it, and I understand all of the reasoning behind it. But when you try to write an instruction that explains this, you get into a lot of words and at least three companies—my company hasn't decided yet—have gone flatly to one side printing. This may not be the right answer but it is a case where our marking situation is getting into some bad reactions.

THOMAS GRADY: I would like to underscore Dick's remarks about additional markings. I know of one project that requires, beside "secret," thirteen DoD markings. There is hardly room for the title. This is not in the manual, and it's not in the contract instrument. Procurement put it into the 254, which is an improper use of it. I would like to see some thinking in that area. Thank you.

ROBERT BECKNER: This may answer Don Garrett's question on time elements and problems in getting answers to our classification

questions. Our program is Lunar Excursion Module Descent Engine, which we are subcontracted to by Grumann, who in turn is contracted by NASA here. We have a problem on our injector that is classified confidential. We go back to Grumann to help us answer this question and they in turn go back to NASA at Houston, who gives an answer, sends it back to Grumann who sends it back to TRW. And the thing is all wrong, in our opinion. So we confront them again by five or six other letters back and forth and we still get the wrong answer, because in the interim, our scientists and technical people know that this answer is wrong and that the injector hardware should be unclassified because they have old us at NASA headquarters that it should be—but not in writing, only verbally. So we go back again to them—and this is going on for about three years. We have gotten answers, it's true, but they are wrong answers. We know what the right answer is but we can't get it in writing. This is one of the dilemmas that you get into on trying to get fast answers. Thank you.